USD(R&E)

Trustworthiness and Assurance

As a function of system design

SE Role for Engineering Secure and Resilient Systems
IAW DoDI 5000.83 Section 3.3.c.(2)

Presented to NDIA Systems and Mission Engineering Conference
Norfolk, Virginia
October 2023

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

Michael McEvilley
System Assurance Lead
The MITRE Corporation

Need for Assurance gaining increased attention

Assurance, as for a variety of attributes such as safety, security, and dependability, is often required. Stakeholder concerns include achieving justified confidence that the system, while achieving its intent, does not also provide unintended behavior or produce unintended outcomes. A claims-oriented approach to assurance serves to address the concerns that are not typically captured within the requirements that focus on intended behavior. --- ISO/IEC/IEEE 15288:2023 Clause 5.10

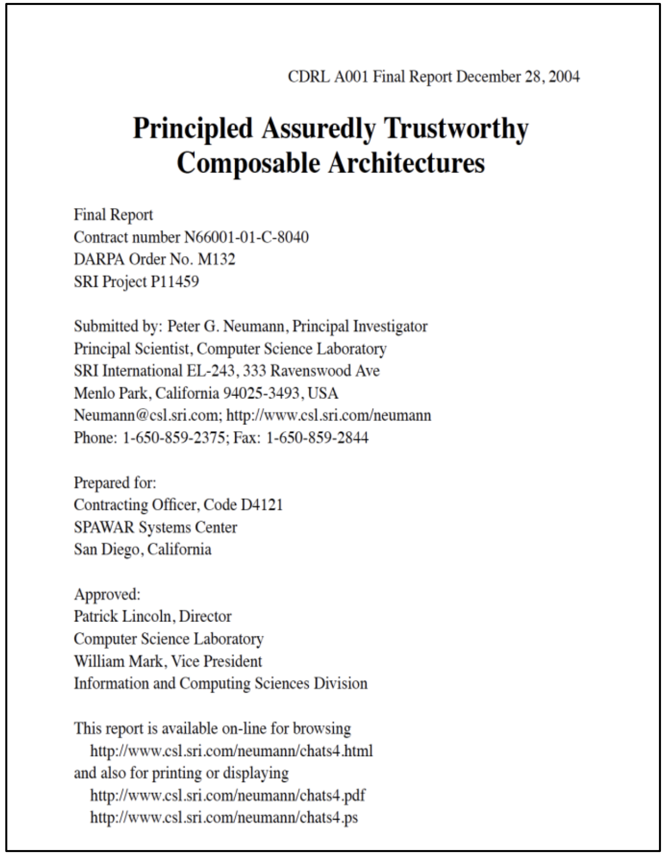
Comment on Trustworthiness “Principled Assuredly Trustworthy Composable Architectures” – Peter G. Neumann, SRI International, Principal Scientist

“We make a careful distinction throughout this report between *trust* and *trustworthiness*.”

“Trustworthiness implies that something is worthy of being trusted.”

**“Trust merely implies that you trust something whether it is trustworthy or not,
perhaps because you have no alternative, or because you are naive,
or perhaps because you do not even realize that trustworthiness is necessary,
or because of some other reason.”**
[Text in Chapter 1 – The Foundations of this Report]

**“As noted above, trustworthiness is a concept that encompasses being worthy of trust with
respect to whatever critical requirements are in effect,
often relating to security, reliability, guarantees of real-time performance
and resource availability, survivability in spite of a wide range of adversities, and so on.”**
[Text in Chapter 2.2 – Risks Resulting from Untrustworthiness]



CDRL A001 Final Report December 28, 2004

**Principled Assuredly Trustworthy
Composable Architectures**

Final Report
Contract number N66001-01-C-8040
DARPA Order No. M132
SRI Project P11459

Submitted by: Peter G. Neumann, Principal Investigator
Principal Scientist, Computer Science Laboratory
SRI International EL-243, 333 Ravenswood Ave
Menlo Park, California 94025-3493, USA
Neumann@csl.sri.com; http://www.csl.sri.com/neumann
Phone: 1-650-859-2375; Fax: 1-650-859-2844

Prepared for:
Contracting Officer, Code D4121
SPAWAR Systems Center
San Diego, California

Approved:
Patrick Lincoln, Director
Computer Science Laboratory
William Mark, Vice President
Information and Computing Sciences Division

This report is available on-line for browsing
http://www.csl.sri.com/neumann/chats4.html
and also for printing or displaying
http://www.csl.sri.com/neumann/chats4.pdf
http://www.csl.sri.com/neumann/chats4.ps

Comment on Trustworthiness and Assurance "Engineering Trustworthy Systems" - O. Sami Saydjari

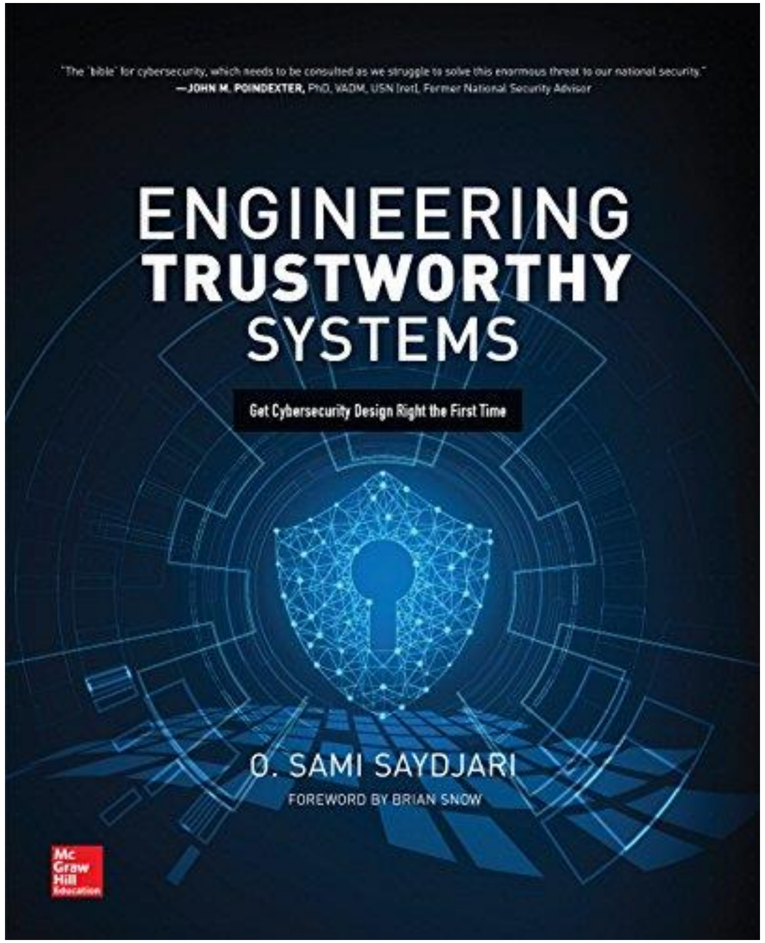
"Cybersecurity functionality is important to overall system trustworthiness; but without assurance, functionality could detract from system cybersecurity."

"Cybersecurity functionality without assurance is harmful"

"Cybersecurity functionality without assurance is called *veneer security* and can increase risk rather than decrease it."

"Veneer cybersecurity leads to increased risk"

[Text in Chapter 21.1 – Cybersecurity functionality without assurance is insecure]


"The 'bible' for cybersecurity, which needs to be consulted as we struggle to solve this enormous threat to our national security."
—JOHN M. POINDEXTER, PhD, VADM, USN [ret], Former National Security Advisor
ENGINEERING TRUSTWORTHY SYSTEMS
Get Cybersecurity Design Right the First Time
O. SAMI SAYDJARI
FOREWORD BY BRIAN SNOW
Mc Graw Hill Education

Applying the Reasoning – Comment on Trustworthiness and Assurance to Resilience

- **Cyber resilient functionality is important to overall system trustworthiness; but without assurance, cyber resilient functionality could detract from system cyber resilience**
- **Cyber resilient functionality without assurance is harmful**
- **Cyber resilient functionality without assurance can be referred to as *veneer resilience* and can increase risk rather than decrease it**

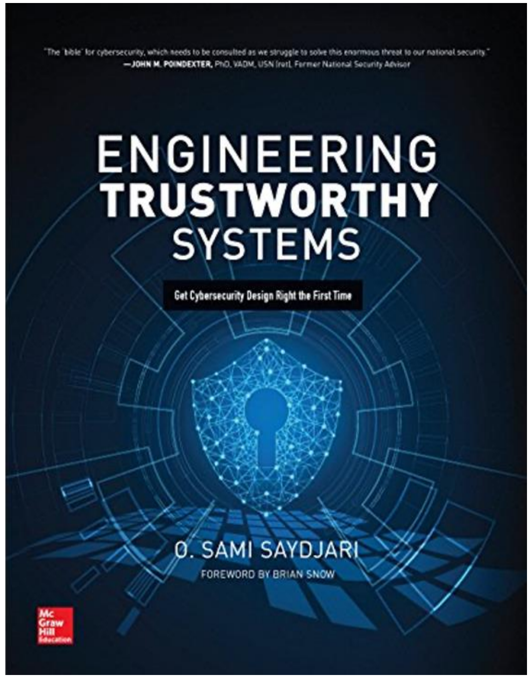
"Cybersecurity functionality is important to overall system trustworthiness; but without assurance, functionality could detract from system cybersecurity."

"Cybersecurity functionality without assurance is harmful"

"Cybersecurity functionality without assurance is called *veneer security* and can increase risk rather than decrease it."

"Veneer cybersecurity leads to increased risk"

[Text in Chapter 21.1 – Cybersecurity functionality without assurance is insecure]


"The 'bible' for cybersecurity, which needs to be consulted as we struggle to solve this enormous threat to our national security."
—JOHN M. POINDEXTER, PhD, VADM, USN (ret), Former National Security Advisor
ENGINEERING TRUSTWORTHY SYSTEMS
Get Cybersecurity Design Right the First Time
O. SAMI SAYDJARI
FOREWORD BY BRIAN SNOW
Mc Graw Hill Education

- **Veneer cyber resilience leads to increased risk**

Distribution Statement A: Approved for public release. DOPSR case #23-S-3528 applies. Distribution is unlimited.

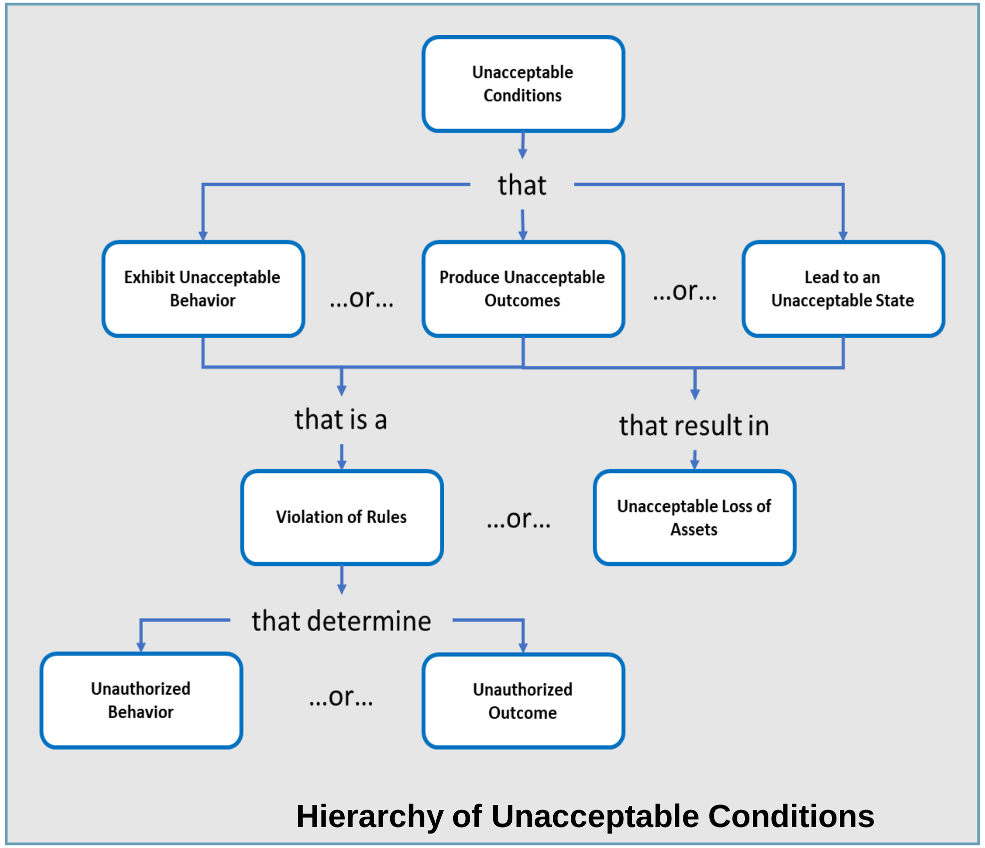
Why is this important to engineering practice IAW DoDI 5000.83 Section 3.3.c.(2)?

- The need for assured trustworthy systems derives from the nature of the consequences of the failure of systems to behave and produce outcomes as intended
  - Security, like safety, requires assurance about a negative/what is not to happen
- Engineering has responsibility to produce the design-related evidence to provide assurance that serves as a basis for trustworthiness judgments
- Insufficient assurance – an assurance deficit – is a risk driver
  - DoD Standard Practice for System Safety (MIL-STD-882E) explicitly addresses assurance about software contribution to hazards, mishaps, and the resultant risk
- Assurance varies as a function of rigor and therefore is a trade space and a driver of cost

“Shifting left for Systems Engineering”
Requires designing an inherently assured trustworthy secure and resilient system
thereby optimizing cost-effectiveness in protection capability and cost, performance, and schedule

Security is About Assuring a Negative

- Security: the **expectation that a system does not**, under defined conditions, exhibit behavior, produce outcomes, or lead to a state: [adapted from IEEE 12207 for safety]
  - that is in violation of rules that determine authorized and intended behaviors and outcomes
  - that causes an unacceptable loss of assets
  - that constitutes an unacceptable loss of assets
- Unacceptable conditions to be avoided are a common attribute of safety and security
  - The unacceptable conditions are controlled to the extent possible to prevent loss and to limit the extent of loss
  - A *hierarchy of unacceptable conditions* can drive engineering activities



Hierarchy of Unacceptable Conditions

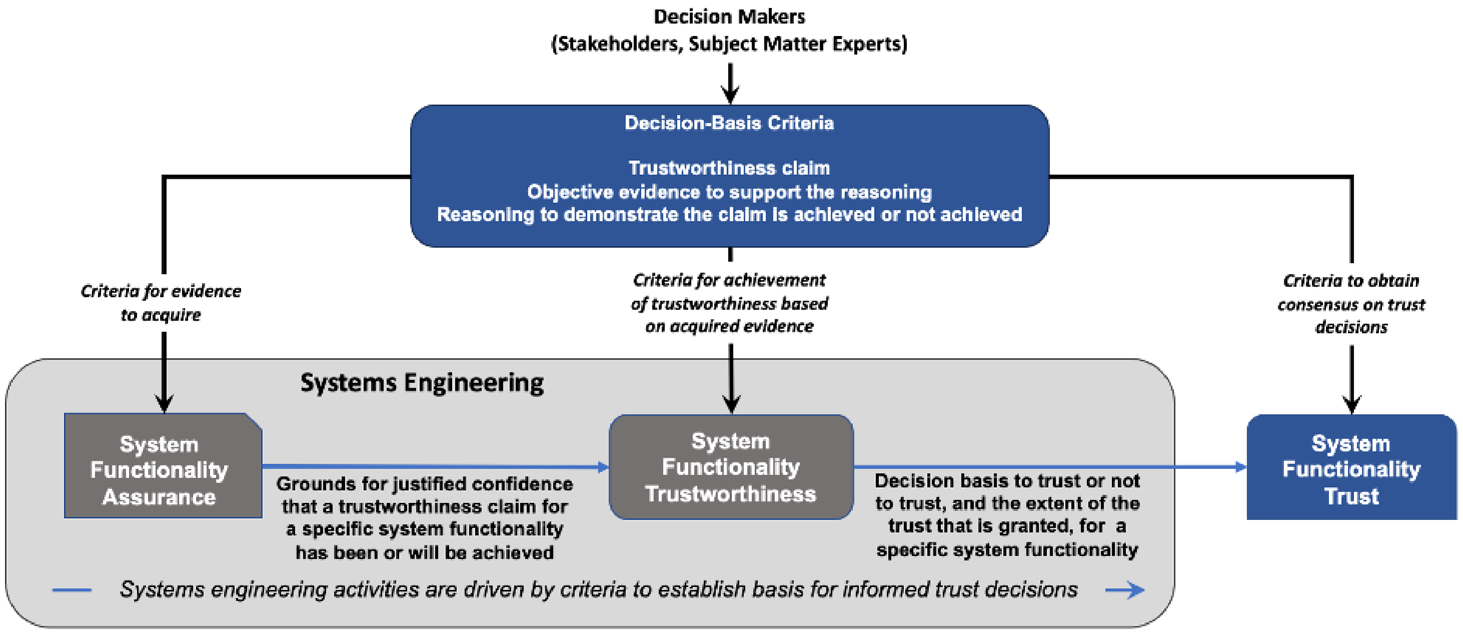
Safety [IEEE 12207]: the expectation that a system does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered.

- Human life, health property, and the environment are types of assets
- Security scope includes all types of assets

Distribution Statement A: Approved for public release. DOPSR case #23-S-3528 applies. Distribution is unlimited.

Assurance, Trustworthiness, Trust

- **Since**
  - Trust is a belief that may or may not be based on trustworthiness
- **It follows that**
  - Trust granted in the absence of sufficient trustworthiness is problematic
- **Therefore**
  - The extent of trust to be granted should be explicitly stated



Decision Makers
(Stakeholders, Subject Matter Experts)

Decision-Basis Criteria

Trustworthiness claim
Objective evidence to support the reasoning
Reasoning to demonstrate the claim is achieved or not achieved

Criteria for evidence to acquire

Criteria for achievement of trustworthiness based on acquired evidence

Criteria to obtain consensus on trust decisions

Systems Engineering

System Functionality Assurance

Grounds for justified confidence that a trustworthiness claim for a specific system functionality has been or will be achieved

System Functionality Trustworthiness

Decision basis to trust or not to trust, and the extent of the trust that is granted, for a specific system functionality

System Functionality Trust

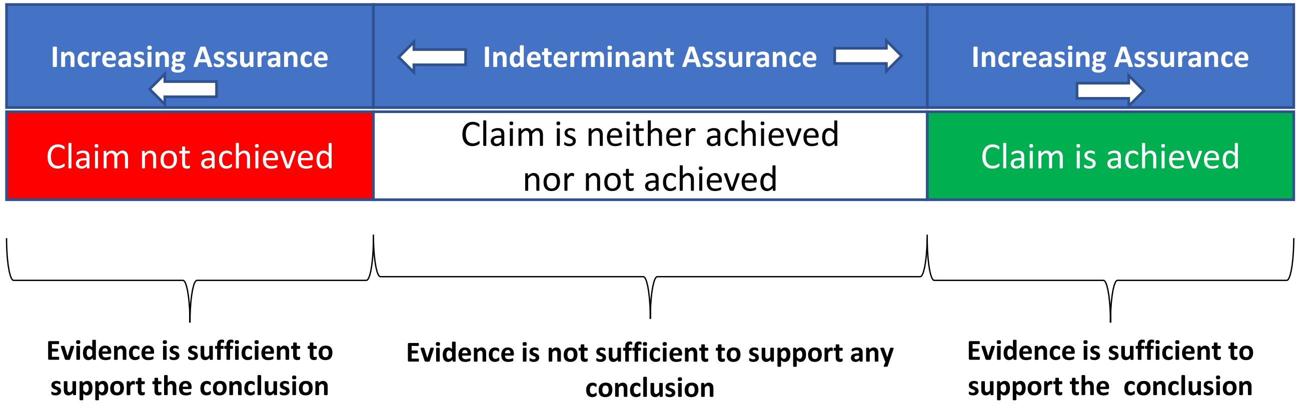
Systems engineering activities are driven by criteria to establish basis for informed trust decisions

- **To enable**
  - Engineering to provide the design-based assurance for the trustworthiness required to support the extent of trust to be granted

Distribution Statement A: Approved for public release. DOPSR case #23-S-3528 applies. Distribution is unlimited.

Assurance

- Assurance is grounds for justified confidence that a claim has been or will be achieved [IEEE 15026]
  - “grounds for justified confidence” implies the combination of **quality evidence** and **expertise**



Increasing Assurance ⟵	⟵ Indeterminant Assurance ⟶	Increasing Assurance ⟶
Claim not achieved	Claim is neither achieved nor not achieved	Claim is achieved
Evidence is sufficient to support the conclusion	**Evidence is not sufficient to support any conclusion**	**Evidence is sufficient to support the conclusion**

Assurance is defined in the positive but translates to three possibilities

- Sufficient grounds for justified confidence that a claim is achieved
- Sufficient grounds for justified confidence that a claim is not achieved
- Insufficient grounds for justified confidence to support any conclusion about a claim

Quality Evidence and Expertise

Quality Evidence

- Attributes include
  - Accuracy
  - Credibility
  - Precision
  - Relevance
  - Quantity (e.g., sample size)
- Note that other factors affect *application* of the evidence but not the *quality* of the evidence
  - Accessibility
  - Timeliness

Expertise

- To confirm the veracity of the approach and to provide the assurance
  - Claim characteristics
    - What is being substantiated?
  - Evidence characteristics
    - What is necessary to substantiate the claim?
  - Evidence generation characteristics
    - What methods, tools, competency is required?
  - Reasoning characteristics
    - What constitutes a valid, logical, compelling argument?

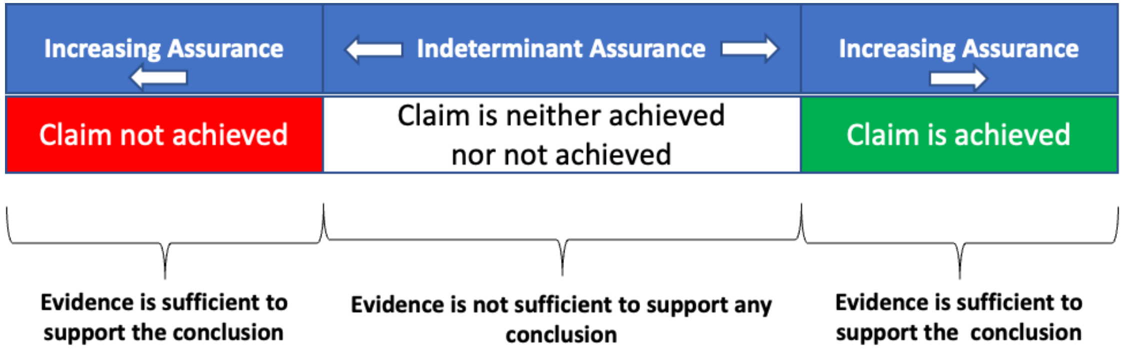
Approaches to Assurance

Appendix A "Approaches to Assurance" [DSB 2017]

- AXIOMATIC – Assertion
  - Assurance is based on beliefs that have been accepted on faith.
  - This provides the weakest form of assurance.
- ANALYTIC – Test and Analysis
  - Assurance is based on testing or reasoning to justify conclusions about properties of interest.
  - Assurance derives from methods of analysis, limited by assumptions underlying the analysis.
- SYNTHETIC – Compositional Reasoning
  - Assurance of the whole derives from assurance of the parts and how they compose.
  - Assurance must be a consideration at every step of design and implementation, from the smallest components to final subsystem realization.
  - Axiomatic and analytic approaches can be used in the synthetic approach to assurance.

Basis of the Grounds for Justified Confidence

- What is done
  - Activity planning and execution
- How it is done – selection and use of
  - Individuals
  - Methods, materials, processes, approaches
  - Tools, techniques
- The result of what is done and how it is done
  - Adequacy, sufficiency, completeness, comprehensiveness
  - Validated and unvalidated assumptions



Increasing Assurance ←	← Indeterminant Assurance →	Increasing Assurance →
Claim not achieved	Claim is neither achieved nor not achieved	Claim is achieved
Evidence is sufficient to support the conclusion	Evidence is not sufficient to support any conclusion	Evidence is sufficient to support the conclusion

Rigor

- Rigor is the formality, thoroughness, accuracy, and precision used in conducting assurance activities
- Rigor factors include
  - Personnel expertise and competency
  - The selection and execution of methods, techniques, and tools
  - Compatibility between personnel and methods, techniques, and tools employed
- Rigor is a trade space that determines the level/strength of assurance

Examples of Rigor Relating to Evidence and Confidence

System Analysis [IEEE 15288:2023]

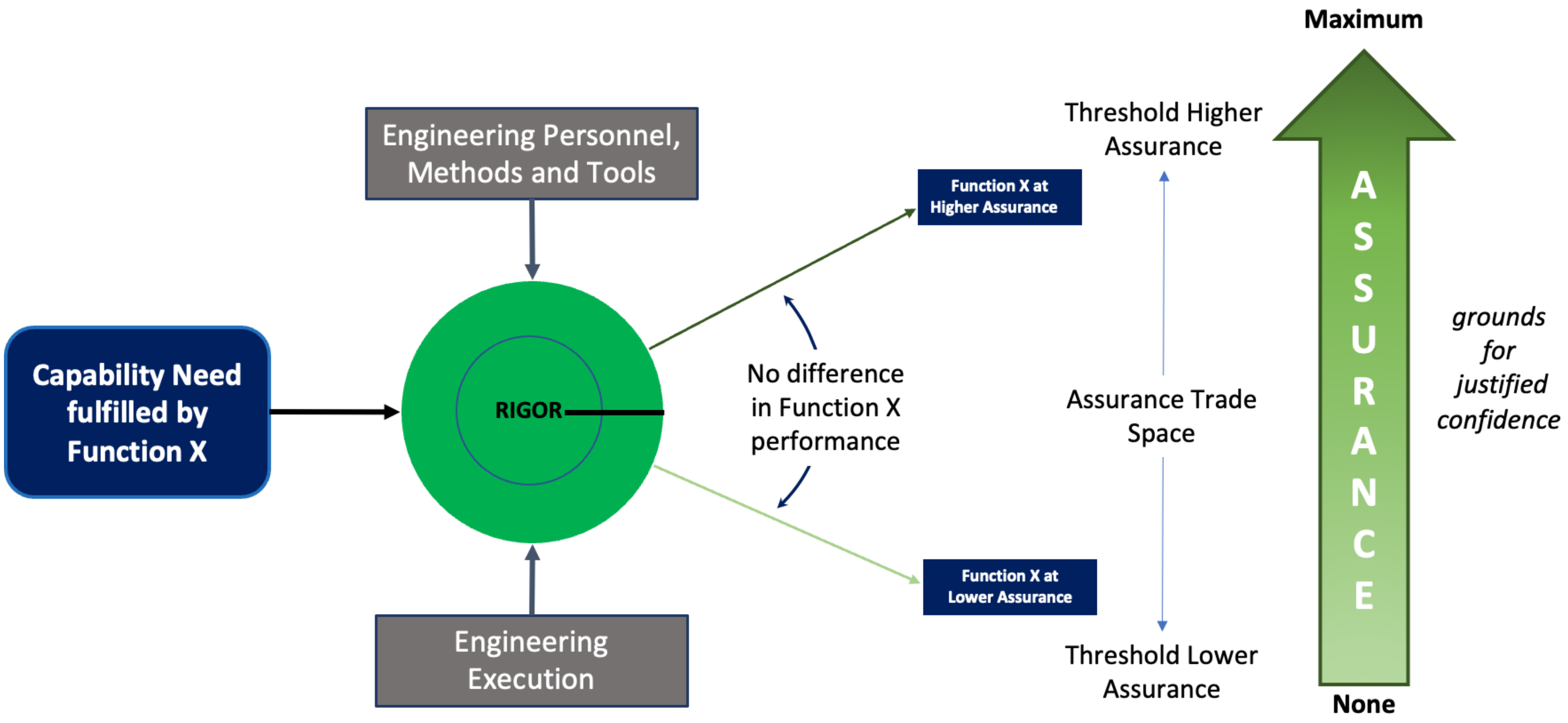
- Analysis methods have a wide range of levels of rigor and expert judgment
- Provides confidence in the outcomes of analysis
- The formality and rigor in analysis will depend on the nature of the evidence need

Level of Rigor (LOR) [DoD 2012]

- The depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required
- Tasks provide confidence to address uncertainty about the software performing as specified

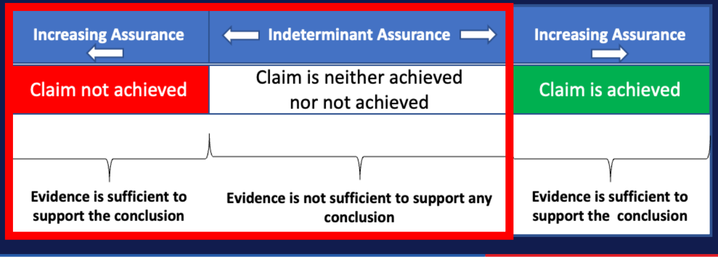
Rigor Drives the Assurance Trade Space

The capability need should be specified in terms of both the trade space of functional performance and the trade space of assurance


Maximum
Threshold Higher Assurance
Engineering Personnel, Methods and Tools
Function X at Higher Assurance
A S S U R A N C E
grounds for justified confidence
Capability Need fulfilled by Function X
RIGOR
No difference in Function X performance
Assurance Trade Space
Function X at Lower Assurance
Engineering Execution
Threshold Lower Assurance
None

Distribution Statement A: Approved for public release. DOPSR case #23-S-3528 applies. Distribution is unlimited.

Assurance Deficit

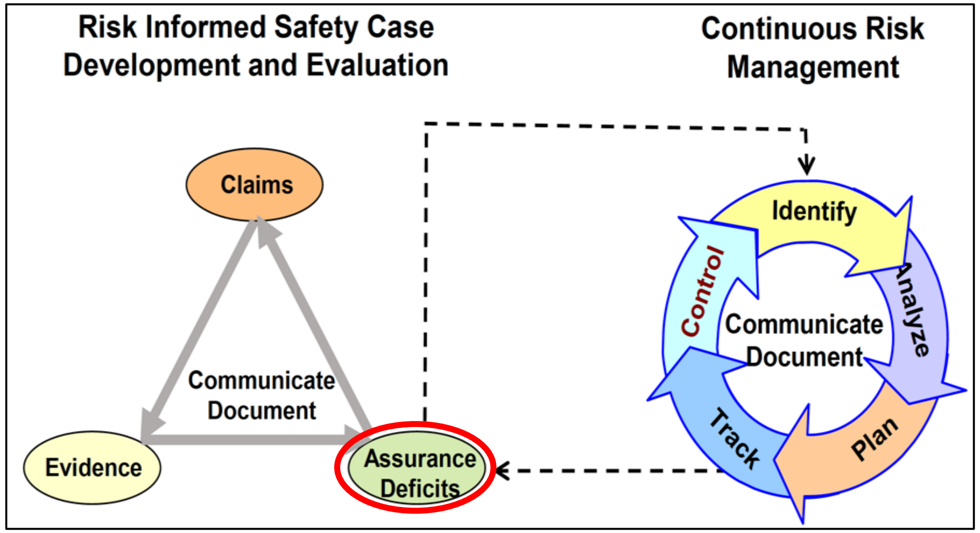


Increasing Assurance | Indeterminant Assurance | Increasing Assurance

Claim not achieved | Claim is neither achieved nor not achieved | Claim is achieved

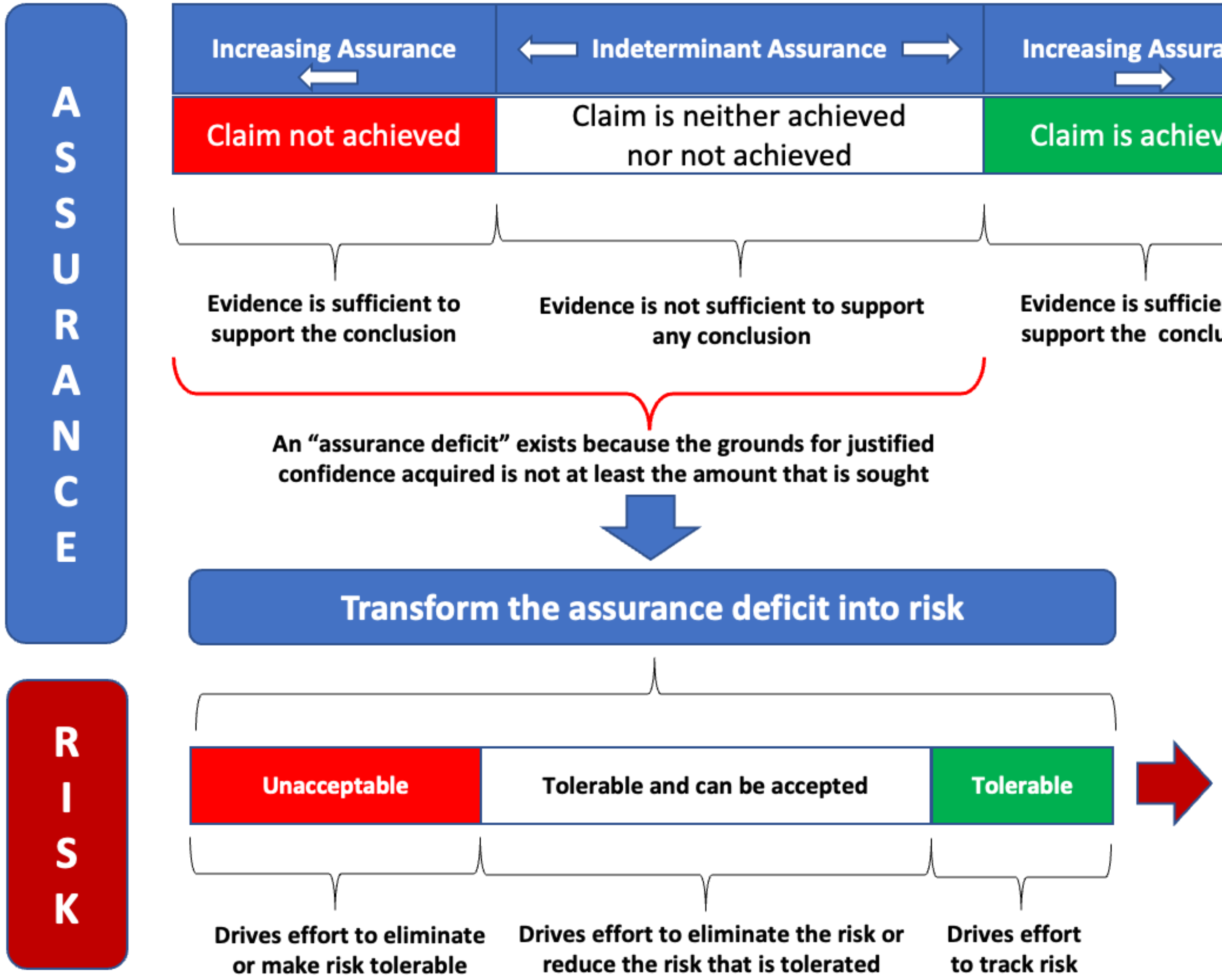
Evidence is sufficient to support the conclusion | Evidence is not sufficient to support any conclusion | Evidence is sufficient to support the conclusion

- Assurance helps determine the limits of certainty
  - Insufficient assurance has uncertainty with risk ramifications
- Assurance Deficit [NASA 2014]
  - Any knowledge gap that prohibits perfect (total) confidence
  - Assurance deficits are managed by the risk management process
- Level of Rigor (LOR) – [DoD 2012]
  - LOR tasks increase confidence that the software will perform as specified while reducing the number of contributors to hazards that may exist in the system.
  - Results of the LOR tasks shall be included in the risk management process
  - The system risk(s) contributions associated with LOR tasks that are not specified, performed, or incomplete shall be documented.
    - Causal factors and hazards that may require mitigation



Assurance Deficit Drives Risk Management Activity [NASA 2014]

Assurance Deficit (Insufficient Confidence) and Risk



ASSURANCE

Increasing Assurance

Indeterminant Assurance

Increasing Assurance

Claim not achieved

Claim is neither achieved nor not achieved

Claim is achieved

Evidence is sufficient to support the conclusion

Evidence is not sufficient to support any conclusion

Evidence is sufficient to support the conclusion

An "assurance deficit" exists because the grounds for justified confidence acquired is not at least the amount that is sought

Transform the assurance deficit into risk

RISK

Unacceptable

Tolerable and can be accepted

Tolerable

Drives effort to eliminate or make risk tolerable

Drives effort to eliminate the risk or reduce the risk that is tolerated

Drives effort to track risk

Assurance Activities

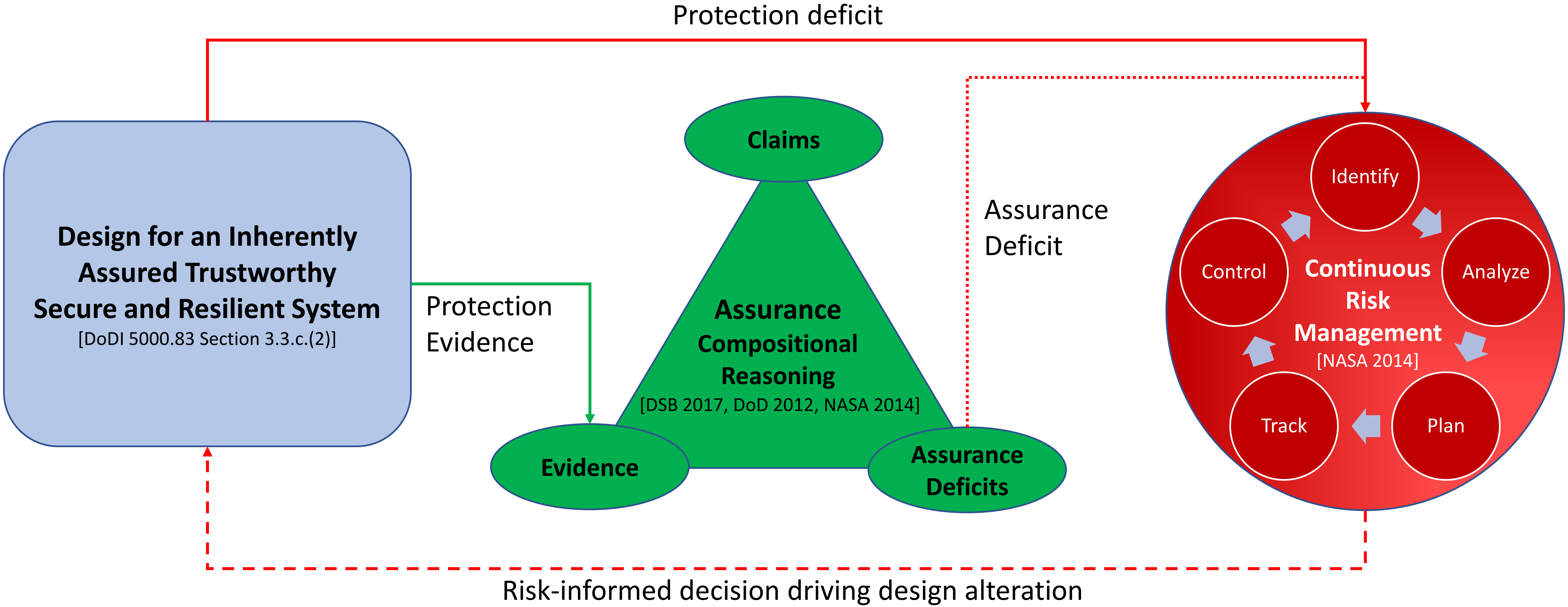
1. Determine the confidence need
2. Acquire the confidence
3. IF
   (a) The confidence need is met by the confidence acquired, THEN Done
   (b) The confidence need is not met by the confidence acquired, THEN either
      (1) Acquire the confidence
      (2) Address the deficit as risk

Risk Management Activities

1. Identify and assess the risk driven by assurance deficit
2. Make decision about the risk
- Unacceptable
- Tolerable/acceptable
- Of no consequence

3. IF risk is unacceptable, THEN determine the appropriate action that either eliminates the risk or makes the risk tolerable/acceptable

Notional Framework that Relates Design, Assurance, Risk Management

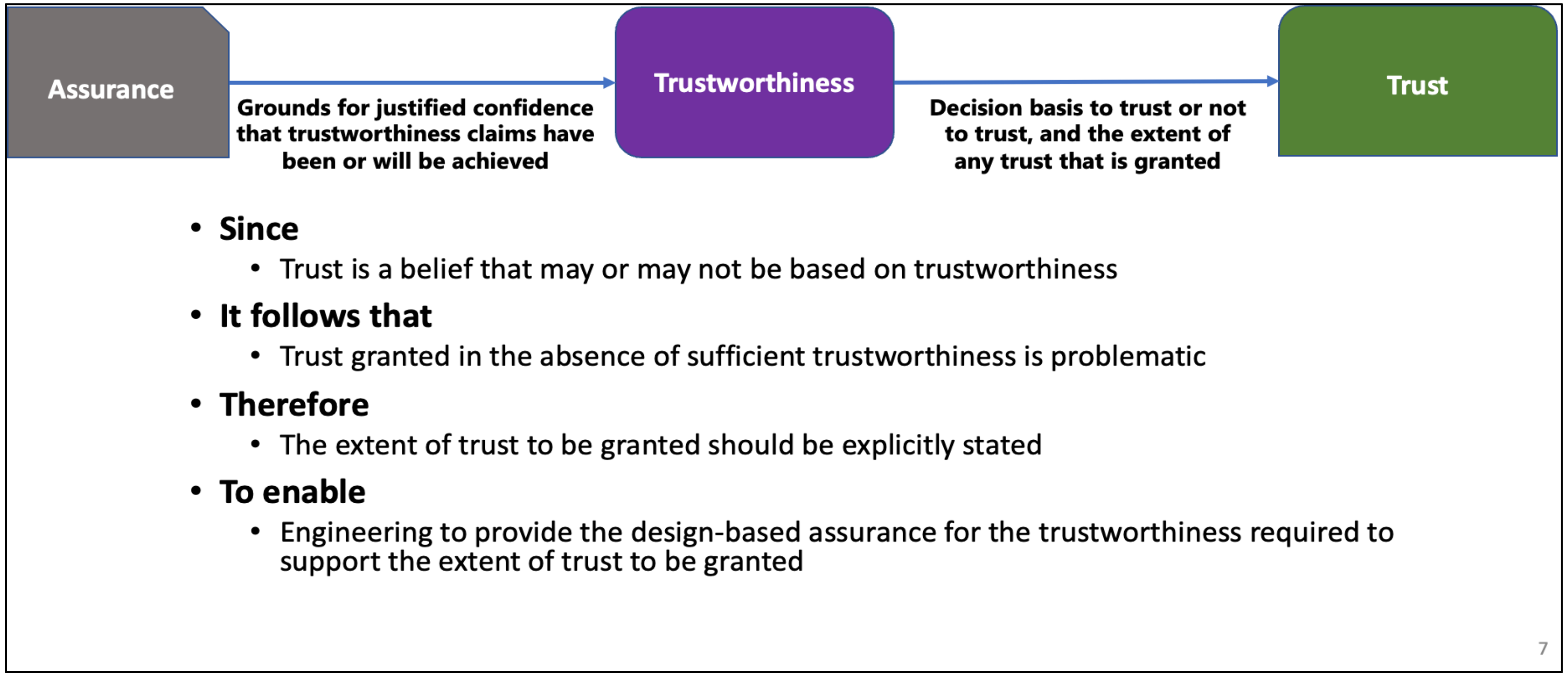

Protection deficit
Design for an Inherently Assured Trustworthy Secure and Resilient System
[DoDI 5000.83 Section 3.3.c.(2)]
Protection Evidence
Claims
Assurance Compositional Reasoning
[DSB 2017, DoD 2012, NASA 2014]
Evidence
Assurance Deficits
Assurance Deficit
Identify
Analyze
Plan
Track
Control
Continuous Risk Management
[NASA 2014]
Risk-informed decision driving design alteration

An inherently assured trustworthy secure and resilient design reduces the number of iterations of risk management activities

Distribution Statement A: Approved for public release. DOPSR case #23-S-3528 applies. Distribution is unlimited.

Concluding Thoughts

- Assurance
  - informs trustworthiness
  - is a trade space
  - is a driver of cost
- Assurance deficit
  - is a driver of risk



Assurance
Grounds for justified confidence that trustworthiness claims have been or will be achieved
Trustworthiness
Decision basis to trust or not to trust, and the extent of any trust that is granted
Trust

- **Since**
  - Trust is a belief that may or may not be based on trustworthiness
- **It follows that**
  - Trust granted in the absence of sufficient trustworthiness is problematic
- **Therefore**
  - The extent of trust to be granted should be explicitly stated
- **To enable**
  - Engineering to provide the design-based assurance for the trustworthiness required to support the extent of trust to be granted

7

- Level/degree/amount of assurance is a function of criticality
  - Higher criticality (consequence/ramification/effect of failure) demands higher assurance
- Use of criticality should not be limited to determining where to expend resources

Key Definitions

- **Assurance**: grounds for justified confidence that a claim has been or will be achieved [IEEE 15026]
- **Claim:** true-false statement about the limitations on the values of an unambiguously defined property — called the claim's property — and limitations on the uncertainty of the property’s values falling within these limitations during the claim's duration of applicability under stated conditions the limitations [IEEE 15026]
- **Trust**: belief that an entity can be relied upon to fulfill certain expectations [Neumann 2004, revised*]
- **Trustworthy**: worthy of being trusted to fulfill certain expectations. [Neumann 2004, revised*]
- **Trustworthiness**: a well-founded assessment of the extent to which an entity is demonstrated to fulfill certain expectations [Neumann 2004, revised*]

*Revision to Neumann definitions because those definitions were provided in the narrative of the report. Any revisions made were for consistency in terms and phrasing (e.g., fulfill certain expectations).

Contextual Definitions

- **Inherently secure**: a design, that avoids susceptibility, vulnerability, and hazard rather than controlling them [Heikkilä 2004]
  - Provides an optimized basis of assured trustworthy protection capability that enforces a set of rules governing behavior and outcomes and that protects against loss
  - Reduces the number iterations for subsequent alteration and employment of engineered features and devices to control susceptibility, vulnerability, and hazards that could not be avoided
- **Risk:** the effect of uncertainty on objectives [ISO 73]
  - Typically-used risk definitions constrain the scope of risk to types of effects, types of uncertainty, and types of or presumed objectives
- **Security:** the expectation that a system does not, under defined conditions, exhibit behavior, produce outcomes, or lead to a state [adapted from IEEE 12207 definition of safety]:
  - that is in violation of rules that determine authorized and intended behaviors and outcomes
  - that causes an unacceptable loss of assets
  - that constitutes an unacceptable loss of assets

References

- [DoD 2012] Department of Defense Standard Practice: System Safety MIL STD 882E, May 2012
- [DSB 2017] Report of the Defense Science Board on Cyber Supply Chain, March 2017
- [Heikkilä, Anna-Mari, Inherent safety in process plant design. An index-based approach. Espoo 1999, Technical Research Centre of Finland, VTT Publications 384 2004]
- [INCOSE SEBoK] INCOSE, System Resilience, Online: http://sebokwiki.org/wiki/System_Resilience, Accessed 6 Feb 2023
- [ISO 73] ISO Guide 73:2009, Risk Management – Vocabulary, 2009
- [ISO 12207] ISO/IEC/IEEE 12207:2017, Systems and software engineering – Software life cycle processes
- [ISO 15026-1] ISO/IEC/IEEE 15026:2019, Systems and Software Engineering – Systems and Software Assurance - Part 1: Concepts and Vocabulary, 2019
- [ISO 15288] ISO/IEC/IEEE 15288:2023, Systems and software engineering —Systems life cycle processes, May 2023
- [NASA 2014] NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples, NASA/SP-2014-612, Version 1.0, November 2014
- [Neumann 2004] Neumann, Peter G., Principled Assuredly Trustworthy Composable Architectures, SRI International, December 2004
- [NRC 2007] Committee on Certifiably Dependable Software Systems, Software for Dependable Systems: Sufficient Evidence?, National Research Council, 2007

Zero Trust

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

- A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy

Responsibility spans those that design, build, operate, and sustain

- Eliminates implicit trust

Applies to machine and human entities attempting to perform an operation –
Does not apply to human and machine entities making and enforcing response decisions

- Requires continuous verification of the operational picture to determine access and other system responses.

Situational awareness of self and environment

- Constantly limits access to only what is needed and looks for anomalous or malicious activity.

Continuous least-privilege access mediation and continuous anomaly detection

- Allows concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Continuous protection in form of least-privilege access mediation

Historical reference: J.H. Saltzer, M.D. Schroeder. The protection of information in computer systems. Proceedings of the IEEE, 63(9):1278–1308, September 1975.
This work established mediated access and the Principle of Least Privilege (PoLP), among several others, as principles for secure system design.