International Council on Systems Engineering
A better world through a systems approach

When Assurance Cases Are Needed For Security

Mark Winstead PhD CSEP

Dr. Mark Winstead

Email mark@markwinstead.net
or mwinstead@mitre.org

Mark serves as The MITRE Corporation's Systems Security Engineering Department Chief Engineer and works with various MITRE sponsors on practice standardization efforts, including co-authoring NIST SP 800-160 Volume 1 Revision 1 *Engineering Trustworthy Secure Systems* with Ron Ross and MITRE's Michael McEvilley.

With INCOSE, Mark is co-chair of the Systems Security Engineering Working Group and cochair and security advocate on the Loss Driven Systems Engineering project. He also participates in other groups, such the FuSE Vision and Roadmap Workstream and the Resilient Systems Working group.

Mark is a graduate of the University of Virginia (PhD, Mathematics) and Florida State University (BS & MS, Mathematics). He resides in Colorado Springs, CO.

Mark is currently looking forward to a career next phase. In addition to remaining "on-call" with MITRE, Mark will continue work with Cal Tech's Center for Technology and Management Education, plans to increase volunteer work with INCOSE, and consult from time to time.

Roadmap

1) Quick Assurance 101
2) When Assurance Cases Work discussion
3) If goal-oriented, what should the goals look like?
4) Shifting Policy coming?

Assurance

Grounds for justified confidence that a claim has been or will be achieved

This confidence is achieved by applying applicable system life cycle activities, which include a planned, systematic approach with acceptable measures of system assurance and risk management of exploitable vulnerabilities … A claims-oriented approach to assurance serves to address the concerns that are not typically captured within the requirements that focus on intended behavior [e.g., safety, security]

ISO/IEC/IEEE 15288 Clause 5.10

Different ways to classify assurance

Weak

Strong

AXIOMATIC Assertion	• assurance by unsubstantiated or weakly substantiated declaration
ANALYTIC Test and Analysis	• assurance from accumulated evidence
SYNTHETIC Assurance Case	• assurance from reasoned and compelling evidence-based arguments

NIST SP 800-160 Volume 1 Revision 1

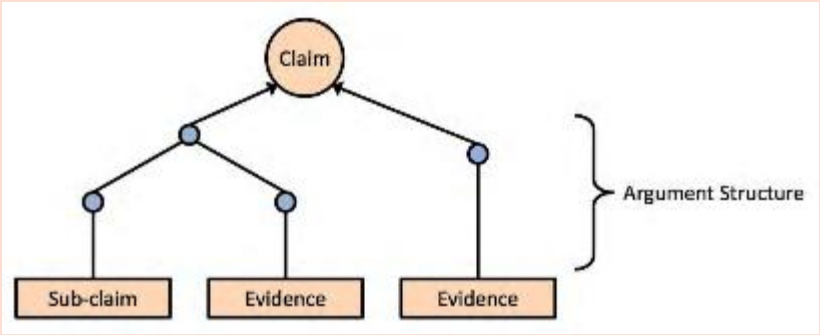
Axiomatic & Analytic → Prescriptive
Synthetic → Goal-Oriented & Blended

Prescriptive	• Assurance by adherence to process or test-driven governance or demonstrating compliance • "one size fits all"
Goal Oriented	• Assurance by adaptable outcome-driven governance, whereby goals or claims are established, and explicit argumentation is made that goals are met
Blended	• Assurance by mixing prescriptive and goal-oriented approaches

Rinehart, Knight, and Rowanhll, **Understanding What it Means for Assurance Cases to "Work"** (2017)

Assurance Case

Structured argument, supported by a body of evidence, that provides a compelling, comprehensible, and valid case that the stated claims for a system are achieved within a set of accepted constraints



Contrasts with Axiomatic (follow a process) and Analytics

Employs the 3 Es

Explicit Claims

- Assertions: What do you seek to achieve?

Evidence

- Quality of data: accuracy, credibility, relevance, sufficiency

Expertise

- Competency: About the subject addressed by the claim and in all supporting evidence

versus

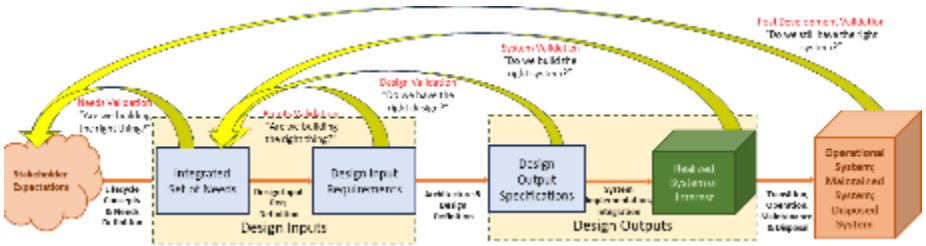
Some Assurance Case Advantages

"An assurance case can identify gaps in requirements coverage and inform the development of derived requirements to address those gaps" ISO/IEC/IEEE 15288:2023 Clause 5.10

"Construction of an assurance case can be helpful to provide insight for verification activities and to present verification results 15288 Clause 6.4.9

"Construction of an assurance case can be helpful to provide insight for validation activities and to present validation results" 15288 Clause 6.4.11

"Establishing an assurance case can be applied to guide quality assurance activities and to help ensure critical quality characteristics are considered" 15288 Clause 6.3.8

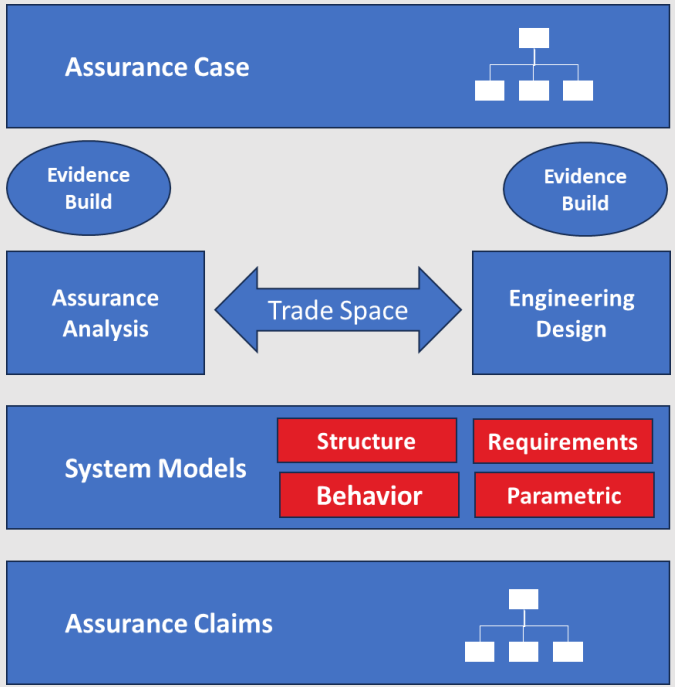


The assurance case is the enabling mechanism to show that the system will meet its prioritized requirements, and that it will operate as intended in the operational environment, minimizing the risk of being exploited through weaknesses and vulnerabilities …

the assurance case is a critical mechanism for supporting the risk management process …

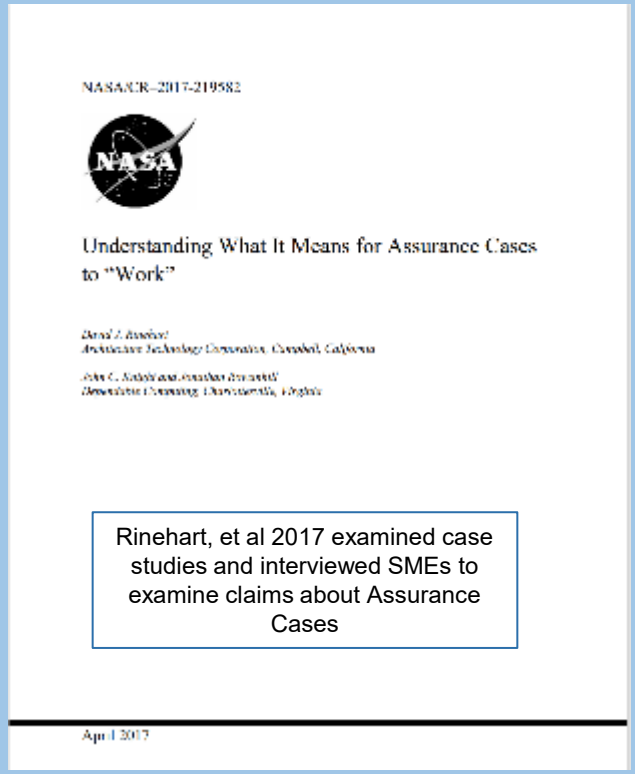
In systems engineering, the activities for developing and maintaining the assurance case enable rational decision making, so that only the actions necessary to provide adequate justification (arguments and evidence) are performed.

- NATO Standard AEP-67 Engineering for System Assurance in NATO Programmes'
Executive Summary



Adaptation of NASA's Model Based Mission Assurance Vision

When Do Assurance Cases Work?


NASA/CR–2017-219582

Understanding What It Means for Assurance Cases to "Work"

April 2017

Rinehart, et al 2017 examined case studies and interviewed SMEs to examine claims about Assurance Cases

Claim	Result
Fundamental: Assurance cases (ACs) are successful where suitable	Well-founded historically and by expert consensus
Benefit: ACs are more comprehensive than conventional methods alone	Easily substantiated
Benefit: ACs improve the allocation of responsibility over prior norms	Appears well backed
Benefit: ACs organize information more effectively than conventional methods	True with caveats. The notional rigor often needed impedes accessibility
Benefit: ACs address modern certification challenges	Largely well-supported, especially for complexity and technical innovation
Benefit: ACs offer an efficient certification path compared to other approaches	Maybe, once an organization has experience
Benefit: ACs provide a practical, robust way to establish due diligence	Appears well-founded

Prescriptive vs Goal-Oriented

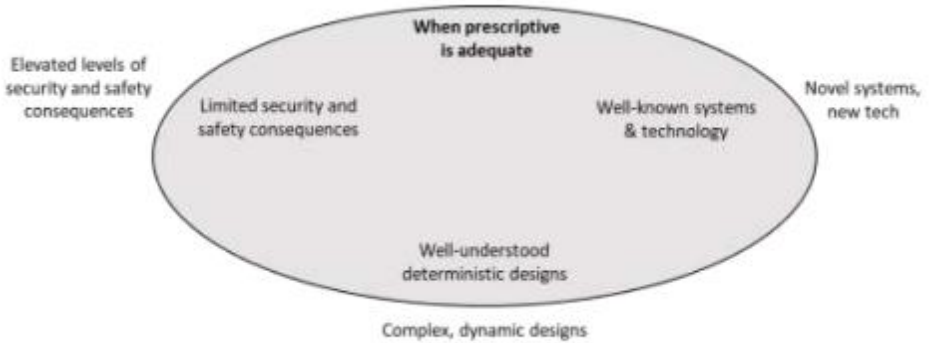
Or

Adherence to process, tests, or compliance vs. Assurance by adaptable outcome-driven governance

Prescriptive is preferable ***when adequate*** due to its "complete the checklist" approaches that enable high confidence in completing authorizations on time

Prescriptive adequate when	Goal-oriented/blended[1] necessary when
Using well-established technology	Using novel systems and innovative technology
Using straightforward and predictable design (simple design)	Systems have complex and non-intuitive design
Safety and security consequences are limited due to low level of safety/security responsibilities	Systems have elevated security and safety responsibilities with elevated failure consequences (safety/security-critical)

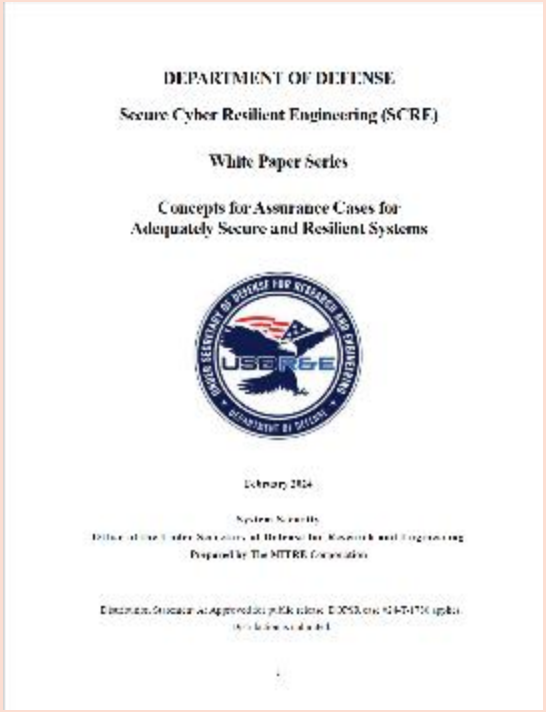
[1]Blended *may* suffice when subsystems or elements satisfy prescriptive adequacy properties



Adapted from

Challenges with Defense (and other) Systems and Prescriptive Approaches

- Use of emerging technologies and technologies often developed for limited use (e.g., military), such technologies are often new and innovative.
  - True for space systems, other unique mission systems
- Complexity, especially for those purposes unique to the community (e.g., military in nature)
  - Not unique to defense
- Needs to preserve technology secrecy further complicates a system.
  - Commercial interests may have intellectual property interests to protect
- Needs to protect the means and methods used to acquire information that inform development of the technology and the use of the system.
- The intended use and opposition to that use often mean the systems have severe security-related consequences including those associated with failures and erroneous behaviors and outcomes.
  - Often true for cyber physical systems controlling large force/energy (critical infrastructure)
- Having a "by design" destructive intent, making it necessary to ensure the destructive capability is used only for the intended manner and results in intended destruction.
- Prevent the exposure of technology that provides combative advantages.
  - Commercial interests have concerns about competitive advantages


DEPARTMENT OF DEFENSE

Secure Cyber Resilient Engineering (SCRE)

White Paper Series

Concepts for Assurance Cases for Adequately Secure and Resilient Systems

February 2024

Complex, innovative, and security-critical

If goal-oriented, what should the goals be?

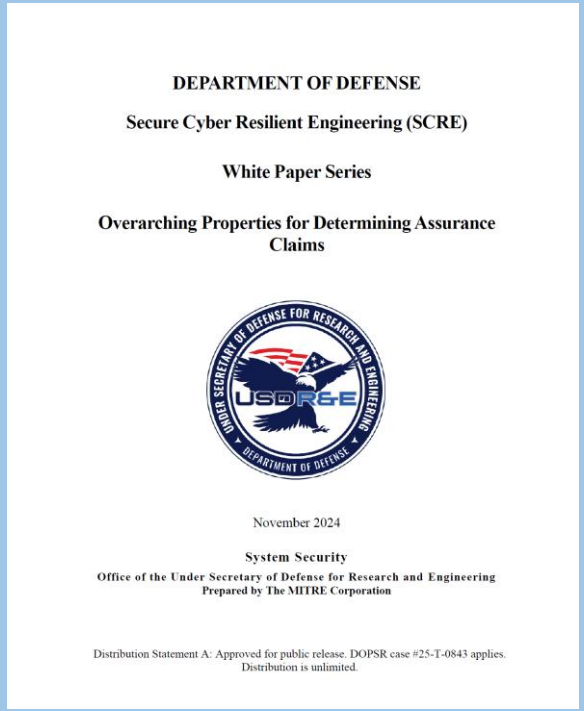
NIST SP 800-160 Vol 1 Rev1 identified three essential items that characterize an ideally secure system:

- Delivering required system capability despite adversity (i.e., negative influences) within foreseeable operating conditions.
- Ensuring that the intended and only the intended behaviors and outcomes occur.
- Ensuring only authorized interactions and operations of the system occur, initiated by authorized entities either outside or inside the system.
    - In other words, the system enforces complete mediated access.

Overarching Properties

Intent, Correctness, Innocuity, and Evolvability

- Claims are about properties
- Borrowing from work involving NASA and FAA, four overarching properties to make claims about are recommended
  - **Intent (specification of intended behavior):** The defined intended behavior is correct and complete with respect to the desired behavior *for authorized entities*.
  - **Correctness (implementation of correct behavior):** The implementation is correct with respect to its defined intended behavior, under foreseeable operating conditions.
  - **Innocuity (security of the unintended behavior):** Any part of the implementation that the defined intended behavior does not require has no unacceptable impact and only authorized entities invoke such implementation.
  - **Evolvable:** The design and implementation enable modifications and other changes in a manner that achieves intent, correctness, and innocuity at comparable levels of assurance across the lifecycle.



DEPARTMENT OF DEFENSE

Secure Cyber Resilient Engineering (SCRE)

White Paper Series

Overarching Properties for Determining Assurance Claims

November 2024

System Security

Office of the Under Secretary of Defense for Research and Engineering
Prepared by The MITRE Corporation

Distribution Statement A: Approved for public release. DOPSR case #25-T-0843 applies.
Distribution is unlimited.

C. M. Holloway, "Understanding the Overarching Properties NASA/TM–2019–220292," National Aeronautics and Space Administration, Hampton VA, 2019.

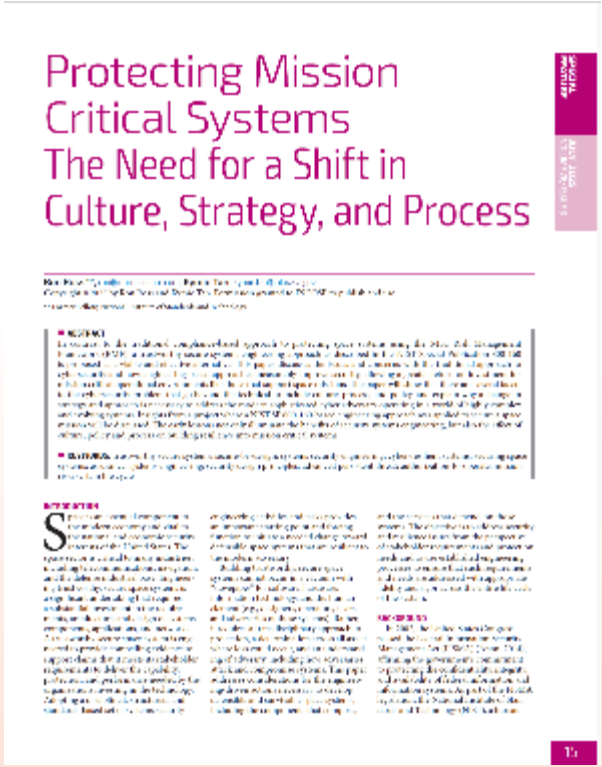
Z. Daw, S. Beecher, M. Holloway and M. Graydon, "Overarching Properties as means of compliance: An industrial case study," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference*, San Antonio TX USA, 2021.

What's Next?

Briefly on movement to change "tradition"

Courtesy of Ron Ross

Current Prescriptive Means Are Known to be Inadequate


Protecting Mission Critical Systems
The Need for a Shift in Culture, Strategy, and Process

the NASA's space systems. This problem has been exacerbated by the convergence of cyber and physical systems and the emergence of artificial intelligence (AI) and robotics technologies. In addition to the above, cybersecurity has largely been implemented as a separate and disconnected process for the past four decades creating several institutional and generations problems. These include:

- Insufficient alignment with the systems engineering life cycle of complex systems, creating a disconnected process
- Insufficient attention to risks involving cyber-physical assets (e.g., application specific intergrated circuits, FPGAs, programmable logic controllers, robotic actuators, sensors)
- Inadequate integration of cybersecurity risks into the established framework for overall project risks (e.g., safety, reliability)
- Inadequate conversion of current threat intelligence into actionable items by systems engineers
- Questionable protection, ambiguous return on investment (e.g., unknown confidence or assurance against a range of specified threats)
- Inadequate visibility into the underlying system design resulting in insufficient trust and assurance in the system capability
- Ineffective for emerging technologies like AI, autonomy, and cloud-based ground stations, insufficient guidance is provided on how to secure these cutting-edge systems effectively or in a timely fashion.

To address these problems, NIST developed a set of systems security engineering (SSE) tools and approaches to help organizations developing systems for their critical missions. The SSE guidance is contained in NIST SP 800-160, Vols. 1 and 2 (Ross, Winstead, and McEvilley 2022; and Ross, et al. 2021). The engineering-based security approach was designed to help organiza-

Ron Ross and Kymie Tan, **Protecting Mission Critical Systems**

Moving Forward

NIST SP 800-160 Vol 1 Rev 1, a systems engineering approach, focuses on evidence-based assurance (i.e., assurance case)

Figure 1 illustrates the 6 key pillars of the TSSE ecosystem.

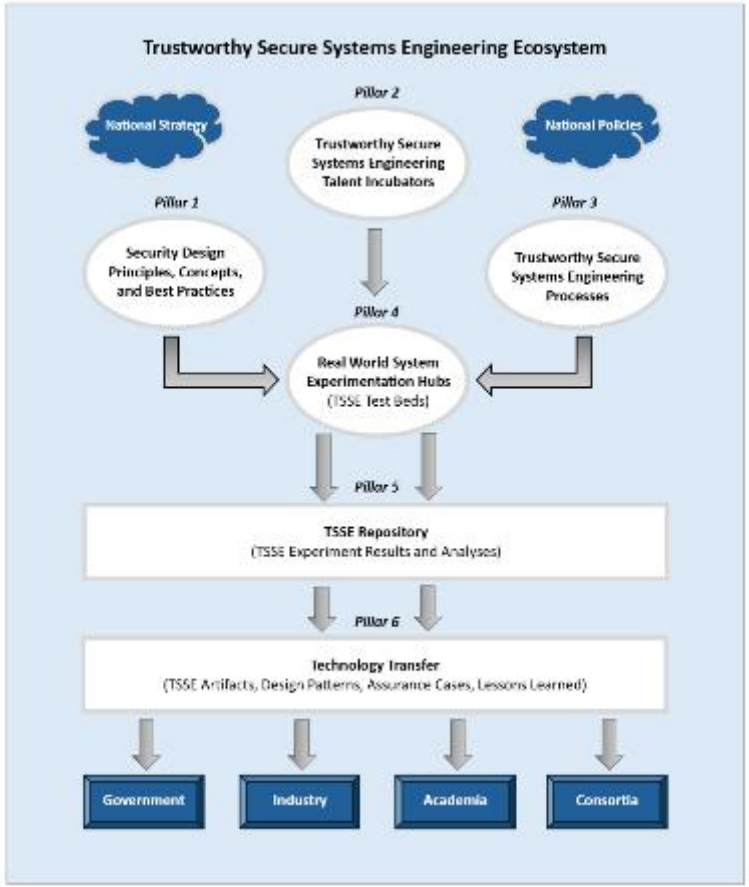


Figure. 1

Questions/Discussion