Concepts for Assurance of Adequately Secure and Resilient Systems

Secure Cyber Resilient Engineering Practice

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

Presented to NDIA
Systems and Mission
Engineering Conference
Norfolk, VA
October 2024

CRWS 13 Assurance Thru Engineering

Cyber Resilient Weapon Systems Workshop 11 (CRWS 11) planted a seed on trustworthiness and assurance, which took some roots at CRWS 12 discussions of secure design – specifically the question of assurance of design and system realization. CRWS 13 dived into assurance through engineering with the help of National Nuclear Security Administration (NNSA), Sandia, DARPA, NIST, and others.

Mission Statement

The CRWS Workshop forum provides a venue for enabling the military systems community (government agencies, the Services, the defense industrial base, and academia) and other extreme consequence systems communities (e.g., NASA, NNSA, NRC) to collaboratively address

1) secure cyber resilient engineering technical challenges and
2) secure cyber resilient engineering workforce competency,

for the fulfillment of the engineering roles and responsibilities stated in DoDI 5000.83.

Vision for Secure Cyber Resilient Engineering (SCRE)

- Secure cyber resilient engineered systems that embody a system-centric and effects-oriented perspective to address the ubiquitous nature of security concerns associated with the design, development, fielding and sustainment of military systems.
- The approach seeks to establish and maintain a strategic, principled, and effective engineering capability for delivery of cost-effective secure cyber resilient engineered weapon systems to the warfighter

Assurance

Grounds for justified confidence that a claim has been or will be achieved ISO/IEC/IEEE 15026-1

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

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

Appendix A "Approaches to Assurance" in [DSB 2017]

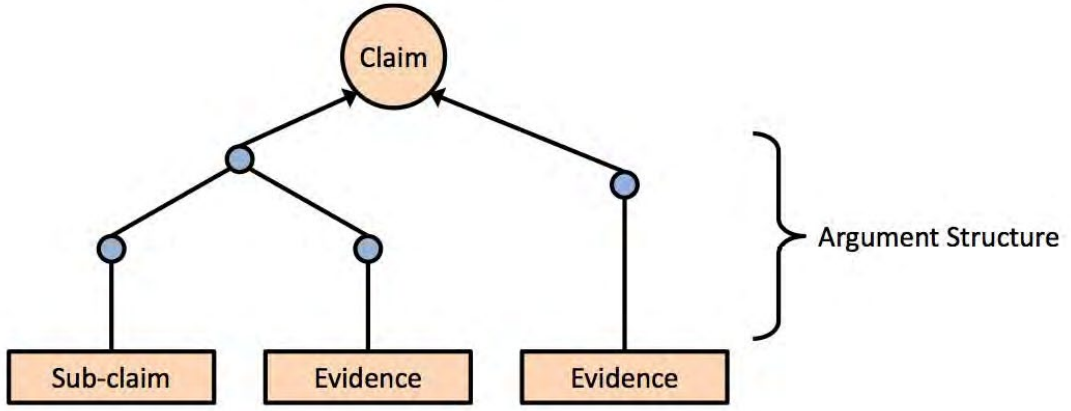
Prescriptive	• Assurance by adherence to process or test-driven governance or demonstrating compliance • "one size fits all"
Goal Oriented	• Assurance by adaptable outcome-driven governance, whereby goals or claims are established and explicit argumentation is made that goals are met
Blended	• Assurance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

Rinehart, et al 2017

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

Assurance Case (Synthetic)

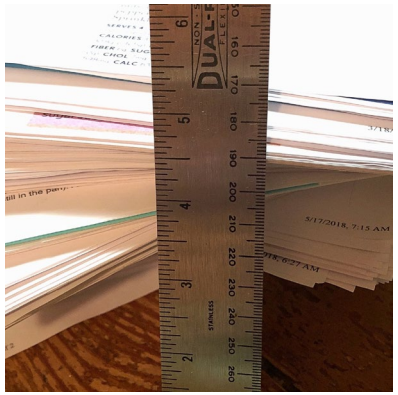
- Structured argument, supported by a body of evidence, that provides a compelling, comprehensible, and valid case that the stated claims for a system are achieved within a set of accepted constraints



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

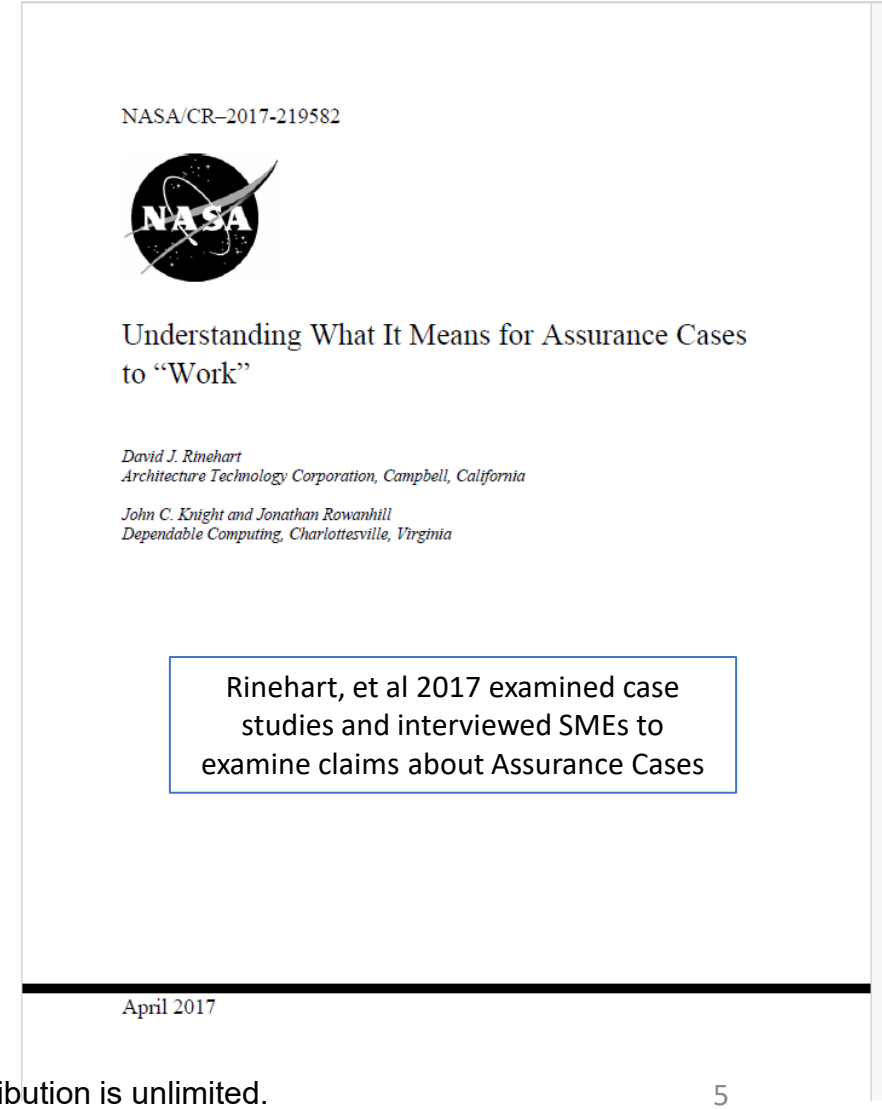
Contrasts with Axiomatic (follow a process) and Analytics



When Assurance Cases Work

Examined Claims and Results

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. 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



NASA/CR–2017-219582

Understanding What It Means for Assurance Cases to "Work"

David J. Rinehart
Architecture Technology Corporation, Campbell, California

John C. Knight and Jonathan Rowanhill
Dependable Computing, Charlottesville, Virginia

April 2017

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

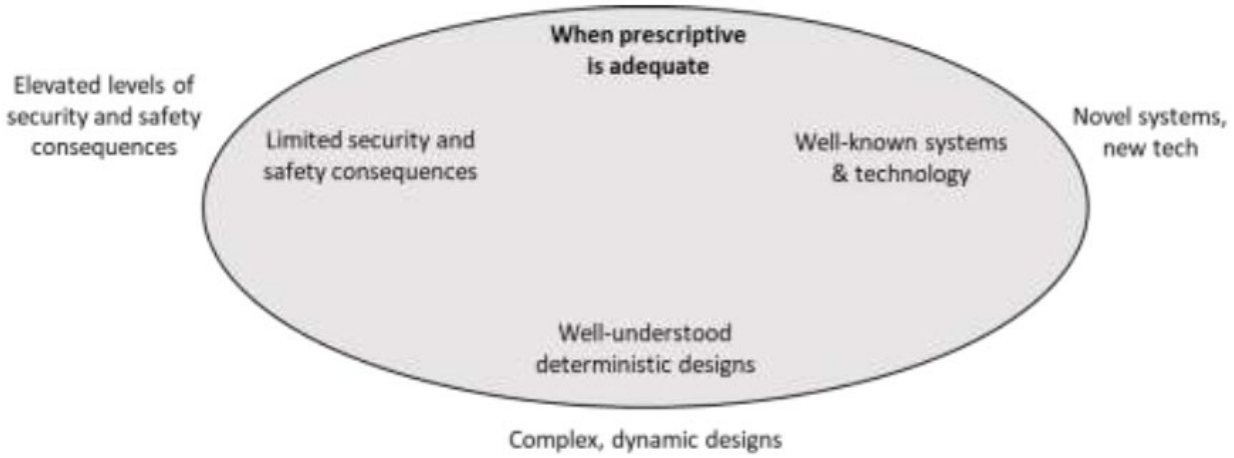
Prescriptive vs Goal-Oriented

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

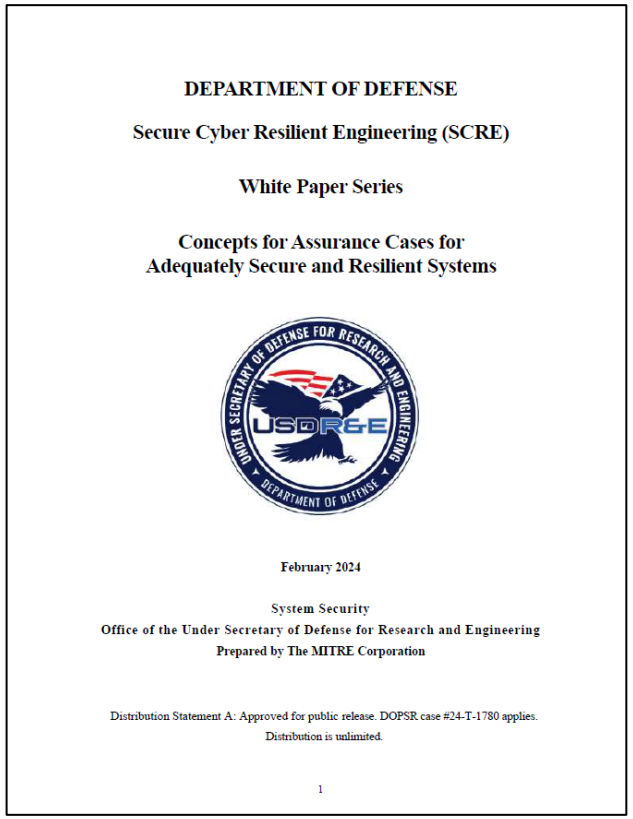
Prescriptive adequate when	Goal-oriented/blended[1] necessary when
Using well-established technology	Using novel systems and innovative technology
Using straightforward and predictable design (simple design)	Systems have complex and non-intuitive design
Safety and security consequences are limited due 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

Challenges with Defense 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.
- Complexity, especially for those purposes unique to the community (e.g., military in nature)
- Needs to preserve technology secrecy further complicates a system.
- 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.
- 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.



DEPARTMENT OF DEFENSE

Secure Cyber Resilient Engineering (SCRE)

White Paper Series

Concepts for Assurance Cases for
Adequately Secure and Resilient Systems

February 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 #24-T-1780 applies.
Distribution is unlimited.

1

Complex, innovative, and security-critical

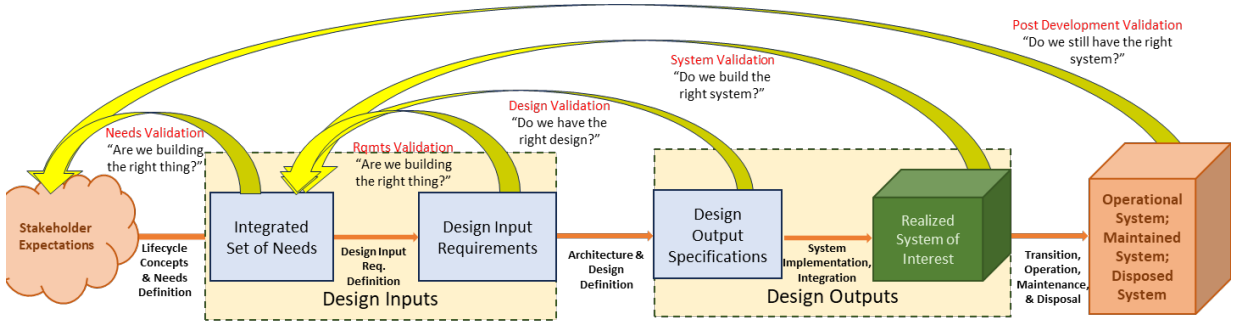
More on Assurance Case Advantages

"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" ISO/IEC/IEEE 15288:2023 Clause 6.4.9

"Construction of an assurance case can be helpful to provide insight for validation activities and to present validation results" ISO/IEC/IEEE 15288:2023 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" ISO/IEC/IEEE 15288:2023 Clause 6.3.8



When Assurance Cases Work Redux

Examined Claims and Results

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. 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

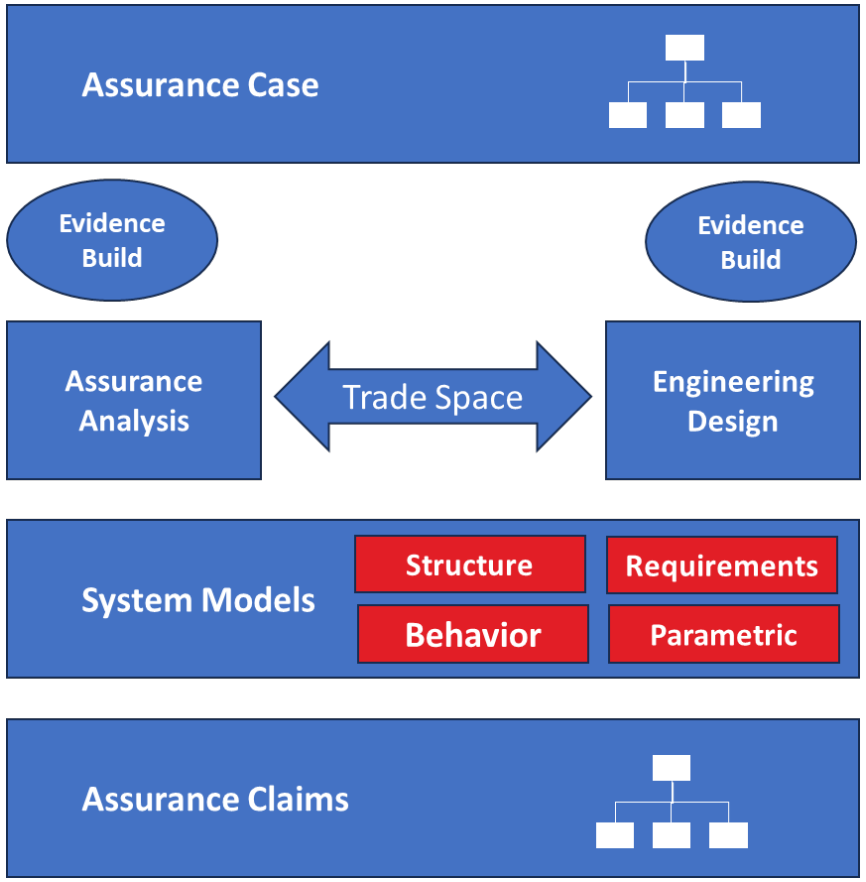
The assurance case is the enabling mechanism to show that the system will meet its prioritized requirements, and that it will operate as intended in the operational environment, minimizing the risk of being exploited through weaknesses and vulnerabilities …

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.

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

Conclusion



When used, assurance cases can show meeting prioritized mission requirements as intended and only as intended and justify systems engineering decisions.

Questions/Discussion

Mark Winstead ***mwinstead@mitre.org***