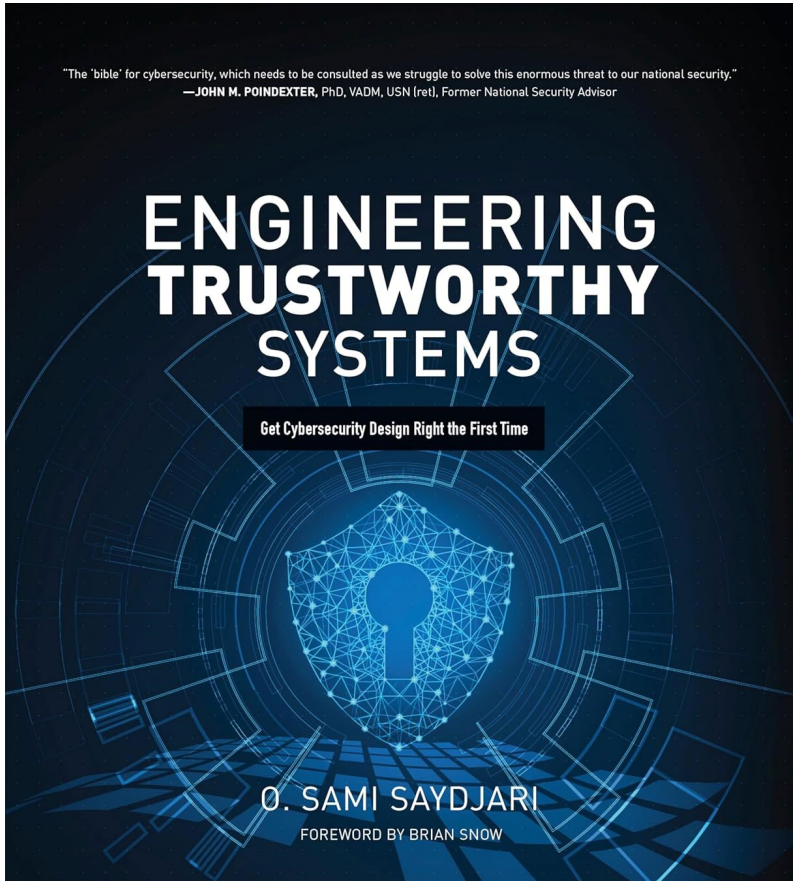
Secure Cyber Resilient Engineering (SCRE) Practice

Assurance-Informed Engineering Perspective

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

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

Fundamental Need for Assurance



Security functionality without assurance is veneer

– Sami Saydjari, Engineering Trustworthy Systems

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)

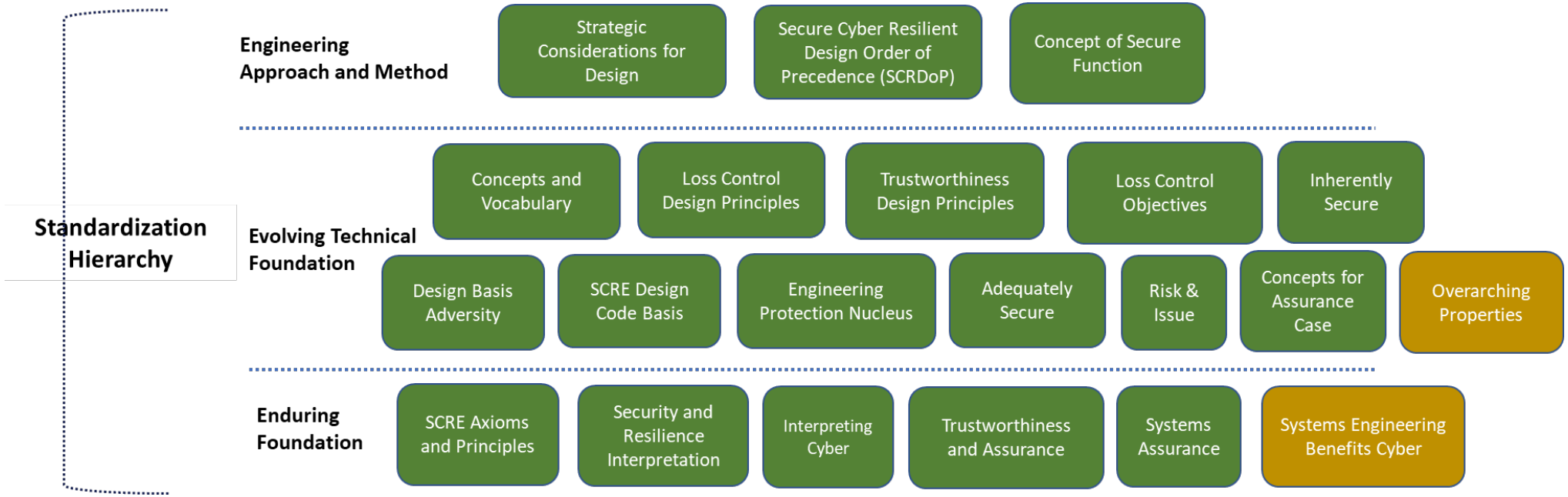
- Secure cyber resilient engineered systems that embody a system-centric and effects-oriented perspective to address the ubiquitous nature of security concerns associated with the design, development, fielding and sustainment of military systems.
- The approach seeks to establish and maintain a strategic,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

SCRE: Technical Whitepapers

Released DoD Distro A

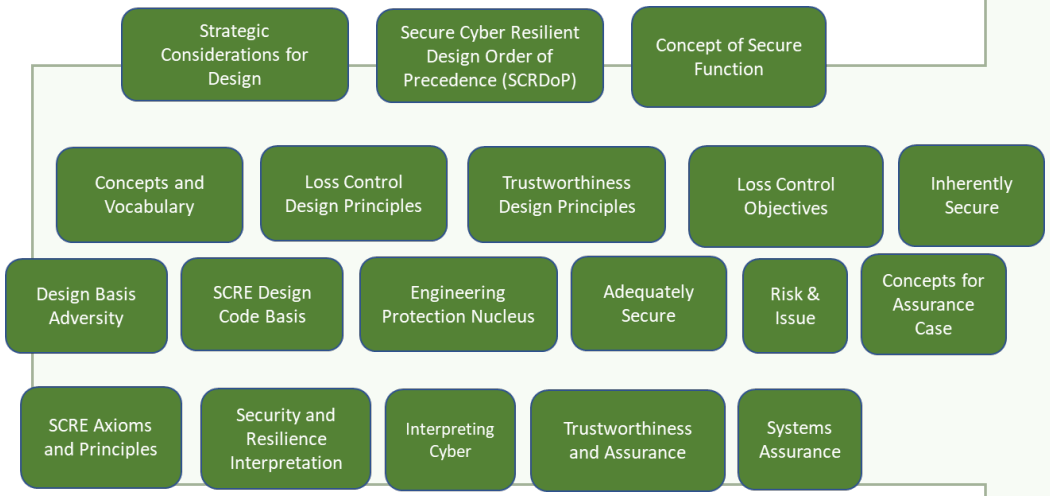
Currently DoD Distro C

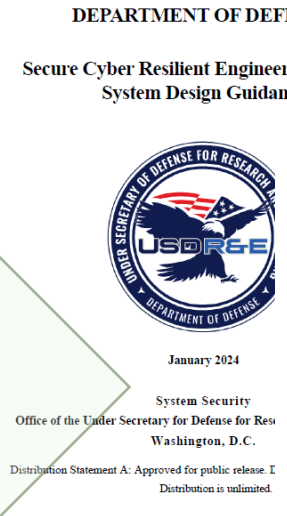
The companion white paper series launched with CRWS 10 discussed assurance within or as a main topic to them. Many of those focused to design or other topics often approached the topic with a supporting theme of generating evidence that provide confidence about system claims



Guidance

To support CRWS 13, the assurance topics were pulled together, and dots connected, for the assurance guidance





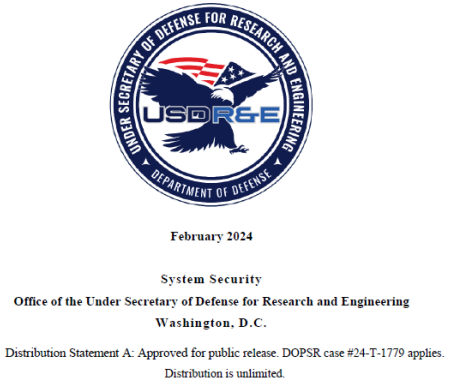
DEPARTMENT OF DEFENSE

Secure Cyber Resilient Engineering (SCRE)
System Design Guidance

January 2024

System Security
Office of the Under Secretary for Defense for Res
Washington, D.C.

Distribution Statement A: Approved for public release. I
Distribution is unlimited.



DEPARTMENT OF DEFENSE

Secure Cyber Resilient Engineering (SCRE)
System Assurance Guidance

February 2024

System Security
Office of the Under Secretary of Defense for Research and Engineering
Washington, D.C.

Distribution Statement A: Approved for public release. DOPSR case #24-T-1779 applies.
Distribution is unlimited.

Pulling it together

Approaches to Assurance

Appendix A "Approaches to Assurance" in [DSB 2017]; Rinehart, et al 2017

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

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

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

Prescriptive vs Goal-Oriented

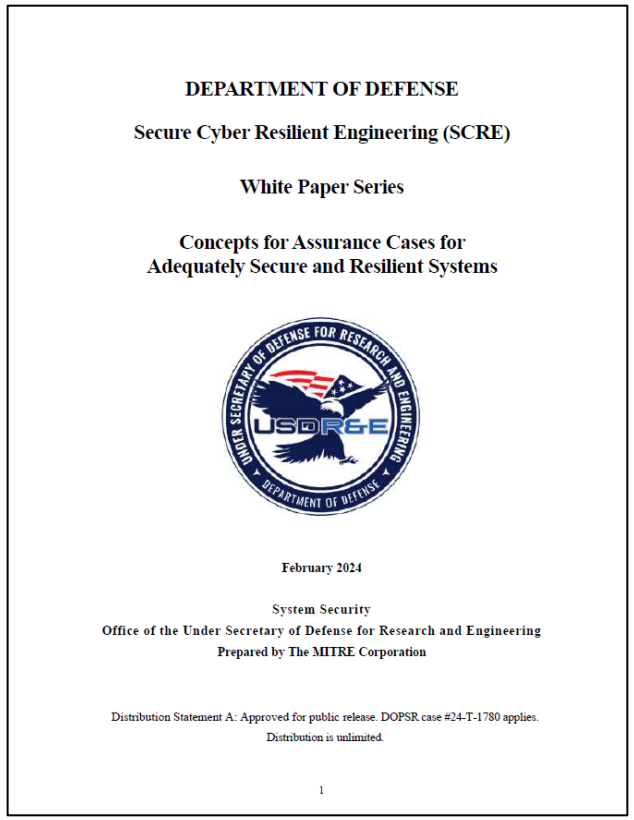
Or

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 is adequate when	Goal-oriented (or blended[1]) necessary when
Using well-established technology	Using novel systems and cutting-edge 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

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



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

SYNTHETIC – Assurance Case

Structured argumentation employing defensible logic

Assurance derives from “assurance components” synthesis

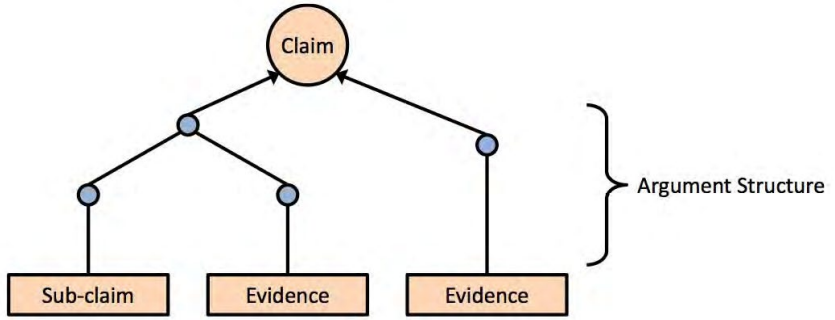
Assurance must be considered at every step of engineering, from the smallest components to final system realization

Assurance Case
Means to Demonstrate Trustworthiness

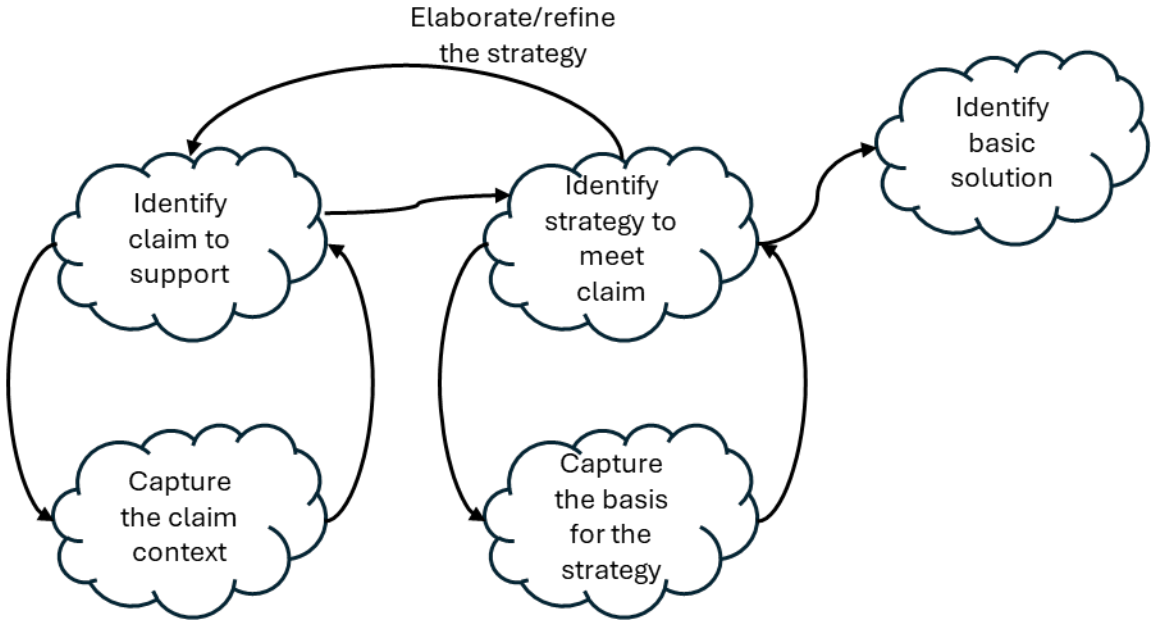
Structured argument, supported by a body of evidence, that provides a compelling, comprehensible, and valid case that the stated claims for a system are achieved within a set of accepted constraints

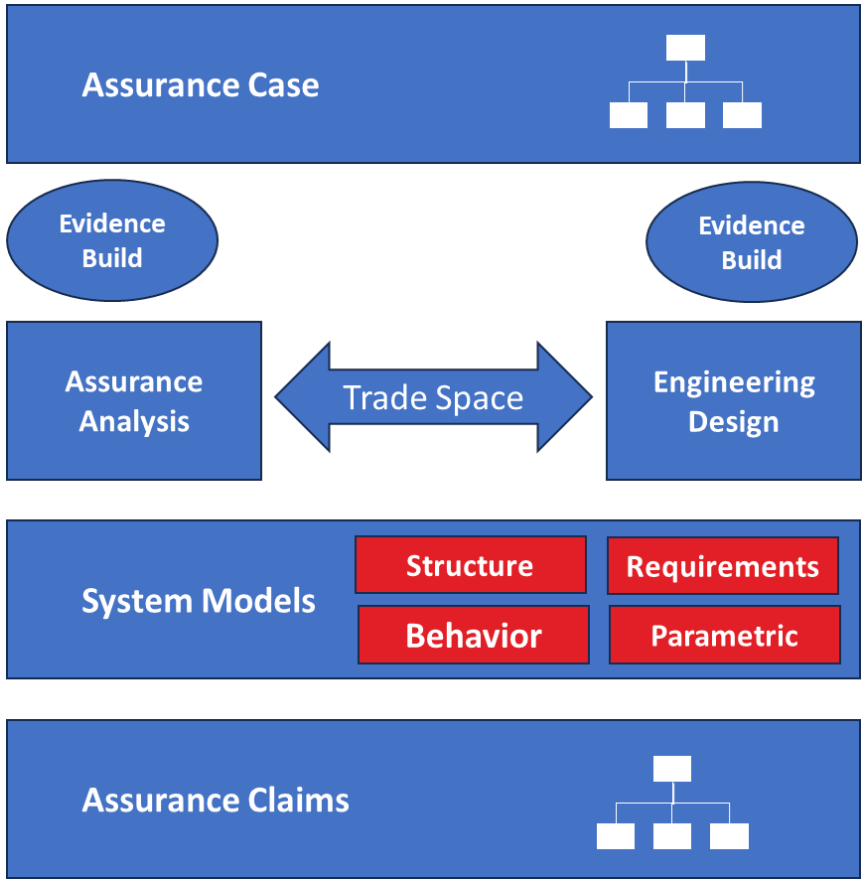
Employs the 3 Es

- **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



Integrating Assurance into Engineering





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. 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

Some CRWS 13 Questions Identified

- How to show assurance claims are sufficient (if met)?
- How to overcome cultural barriers?
- What guidance is needed for claims? What is the analogue for “SMART” for claims?
- What is the ontological language of the assurance case?
- How to integrate assurance case elements into DiDs, CDRLs, Sections L & M, and SOWs?

Closing Thoughts and Questions

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

SCRE Standardization Area


SD1

DEFENSE STANDARDIZATION PROGRAM

STANDARDIZATION DIRECTORY

(FSC CLASS AND AREA ASSIGNMENTS)

REVISED AS OF

1 July 2022

STDZ

SCRE Area Category

- Covers the ***integration of life cycle security and protection considerations*** in the requirements, design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems that operate in physical and cyberspace operational domains

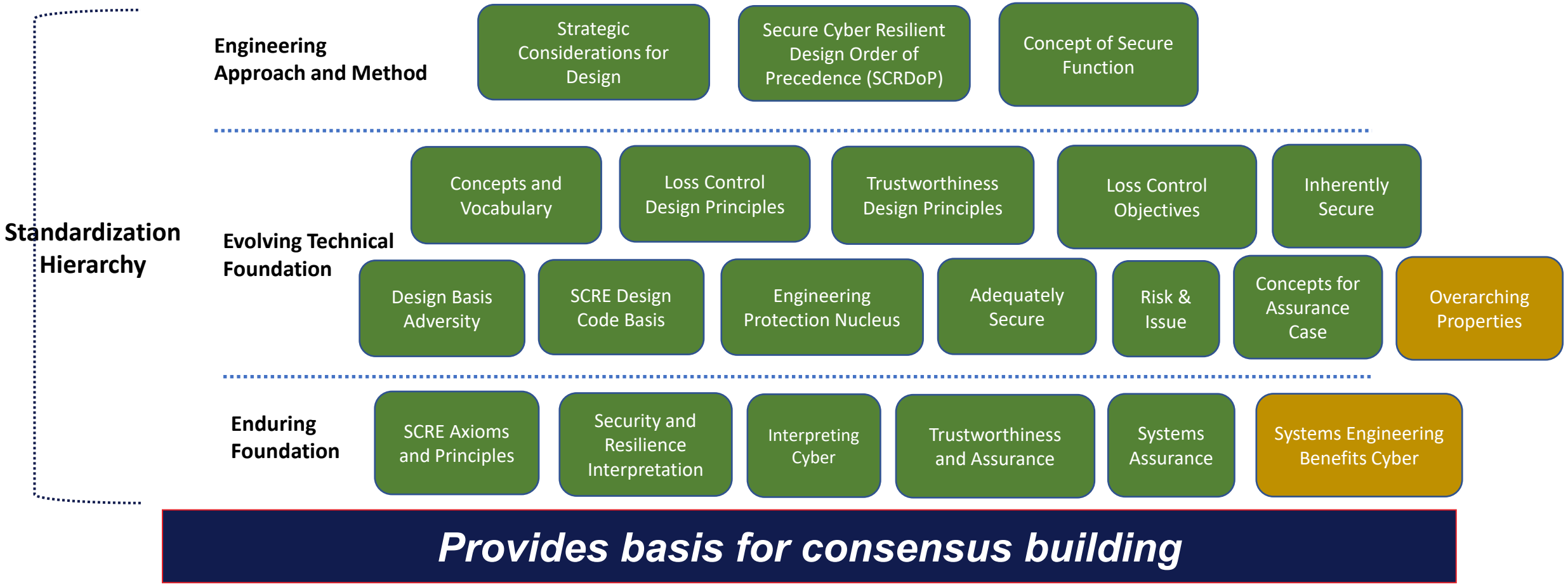
- Specifically encompasses the standards, specifications, methods, practices, techniques, and data requirements ***for the security aspects of systems engineering*** activities executed and artifacts produced, with explicit consideration of malicious and non-malicious adversity

Defense Standardization Program Standards Area for SCRE Engineering Technologies, Disciplines, and Practices

SCRE: Technical Whitepapers

Released DoD Distro A

Currently DoD Distro C



Provides basis for consensus building