USD(R&E)

SCRE Design Guidance

Foundation for a Secure System

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

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

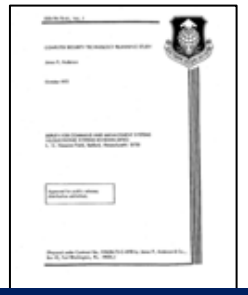
Michael McEvilley
Systems Assurance Lead
The MITRE Corporation

Agenda

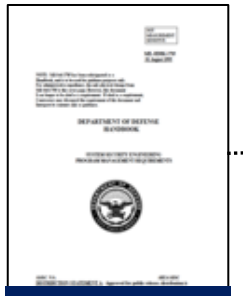
- **Background**
- **Purpose, Foundations, Desired Outcomes**
- **Approach to building**
- **Context**
- **Tasks guidance**
  - **Management**
  - **Analysis**
  - **System Definition**
- **Next Steps**

DoD-centric System Security Engineering Timeline

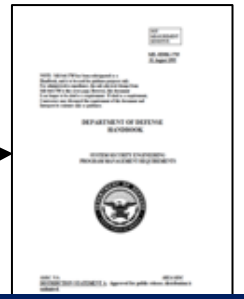
Problem: To increase effectiveness of systems security engineering, secure cyber-resilient engineering methods are needed that adapt to the cyber physical/physics characteristics of weapon



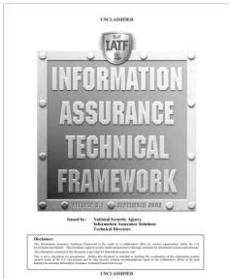
Computer Technology Planning Study "Anderson Report" Basis for Orange Book



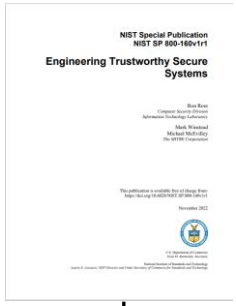
MIL-STD-1785 System Security Engineering



MIL-STD-1785 redesignated as a Handbook to be used for guidance purposes only



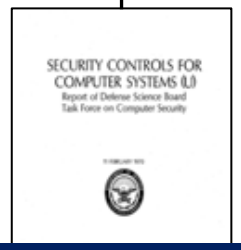
Last release of IATF from NSA



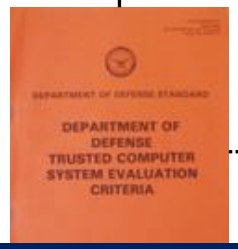
Gaps Caused by the Absence of Relevant Codified Engineering Practice

1970 1972 1985 1989 1992 1998 2002 2019 2022 2023>

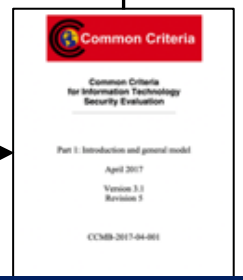
COMPUSEC COMSEC TRANSE | INFOSEC | Information Assurance (IA) | Cybersecurity (CS)



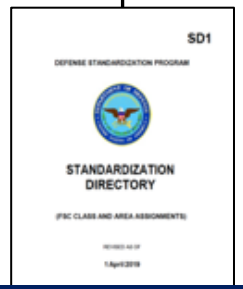
Defense Science Board Task Force Report to Director DR&E



DoD Std 5200.28 "Orange Book" Standard for Security Evaluation Criteria



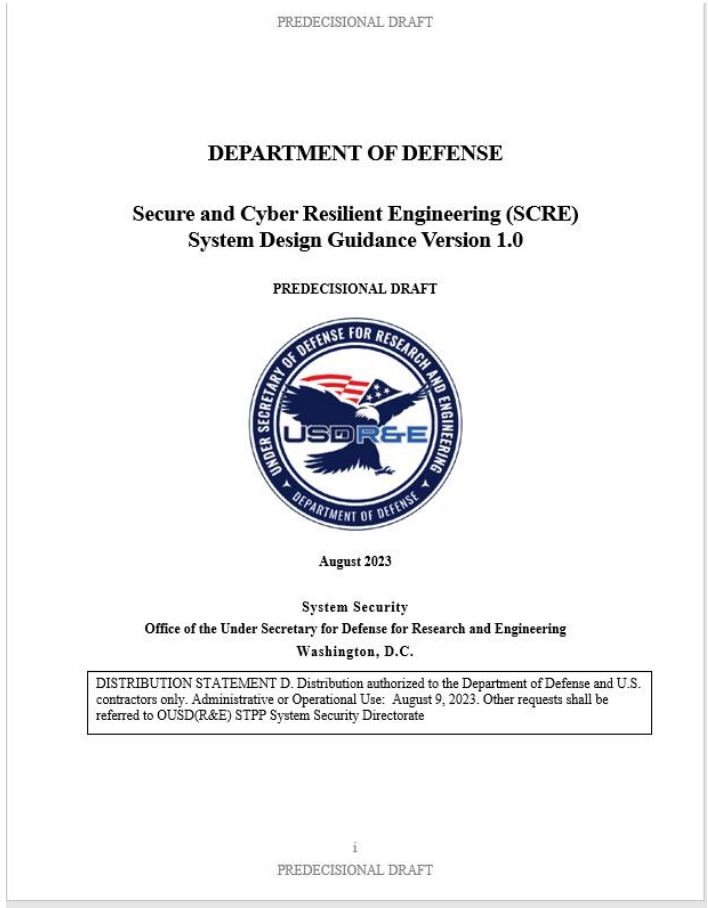
ISO/IEC Standard 15408 "Common Criteria" Replaces Orange Book



SCRE Standardization Area Established

Security as foundational to system design as safety and performance

Guidance Purpose



PREDECISIONAL DRAFT

DEPARTMENT OF DEFENSE

Secure and Cyber Resilient Engineering (SCRE)
System Design Guidance Version 1.0

PREDECISIONAL DRAFT

August 2023

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

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. contractors only. Administrative or Operational Use: August 9, 2023. Other requests shall be referred to OUSD(R&E) STPP System Security Directorate

i

PREDECISIONAL DRAFT

- For the role of the secure cyber resilient engineering practice ***as an element of*** Systems Engineering (SE) to establish and mature the design of trustworthy assured secure and resilient systems.
  - A trustworthy assured secure and resilient system has an evidence basis to support claims that the system can deliver required capability while limiting the adverse effects caused by intentional and unintentional forms of adversity found in the environment of the system and within the system itself

Foundations

- Conform to Department of Defense Instruction (DoDI) 5000.83, Design for Security and Cyber Resiliency
- Consistent with broad systems engineering community, e.g., as captured by ISO/IEC/IEEE 15288:2023
- Embrace a philosophy for a principled and strategic approach to design that is based on scientific and engineering concepts and principles.
  - The approach is effects-based to provide effective control over losses that may result from intentionally exploiting or unintentionally triggering susceptibility, vulnerability, and hazards.


INTERNATIONAL STANDARD

ISO/ IEC/IEEE 15288

Second edition 2023-05

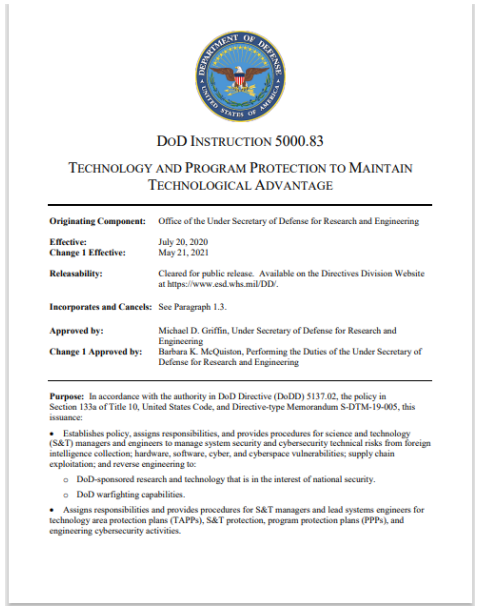
Systems and software engineering — System life cycle processes

Ingénierie des systèmes et du logiciel — Processus du cycle de vie du système

ISO IEC IEEE

Reference number ISO/IEC/IEEE 15288:2023(E)

© ISO/IEC 2023 © IEEE 2023


DoD INSTRUCTION 5000.83

TECHNOLOGY AND PROGRAM PROTECTION TO MAINTAIN TECHNOLOGICAL ADVANTAGE

Originating Component: Office of the Under Secretary of Defense for Research and Engineering

Effective: July 20, 2020
Change 1 Effective: May 21, 2021

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Incorporates and Cancels: See Paragraph 1.3.

Approved by: Michael D. Griffin, Under Secretary of Defense for Research and Engineering
Change 1 Approved by: Barbara K. McQuiston, Performing the Duties of the Under Secretary of Defense for Research and Engineering

Purpose: In accordance with the authority in DoD Directive (DoDD) 5137.02, the policy in Section 133a of Title 10, United States Code, and Directive-type Memorandum S-DTM-19-005, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for science and technology (S&T) managers and engineers to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to:
  - DoD-sponsored research and technology that is in the interest of national security.
  - DoD warfighting capabilities.
- Assigns responsibilities and provides procedures for S&T managers and lead systems engineers for technology area protection plans (TAPPs), S&T protection, program protection plans (PPPs), and engineering cybersecurity activities.

Desired Outcomes

- The principled and strategic approach provides an enduring foundation to be used to establish and mature an **inherently secure** system design as the basis to satisfy any functional, performance, certification, accreditation, authorization, or approval requirement or criteria.
  - Avoiding known susceptibility, vulnerability, and hazard to the extent practical as a by-product of the design and provide effective system protection control over those susceptibilities, vulnerabilities, and hazards that cannot be avoided
- Can be used to support engineering activities conducted as part of an integrated transdisciplinary SE process.
  - Transdisciplinary as optimization for one discipline may create susceptibilities, vulnerabilities, and hazards in other disciplines

Leverage SCRE Whitepapers -> Design Guidance (+ Future Products)

DoD Distro A Available @ CRWS-BoK

DoD Distro D, & on roadmap to A

Engineering Approach and Method

- Strategic Considerations for Design
- Secure Cyber Resilient Design Order of Precedence (SCRDoP)
- Concept of Secure Function

Evolving Technical Foundation

- Loss Control Design Principles
- Engineering Protection Nucleus
- Inherently Secure
- Concepts and Vocabulary
- SCRE Design Code Basis
- Loss Control Objectives
- Risk & Issue
- Design Basis Adversity
- Trustworthiness Design Principles
- Adequately Secure

Enduring Foundation

- SCRE Axioms and Principles
- Security and Resilience Interpretation
- Interpreting Cyber
- Trustworthiness and Assurance
- Systems Assurance

WPs summarized in and provided additional info to Sec 4

4 SECURE CYBER RESILIENT ENGINEERING SYSTEM DESIGN FOUNDATION 11
4.1 OVERVIEW OF THE SCRE PRACTICE 11
4.2 SCRE APPROACH TO DESIGN FOR ASSURED TRUSTWORTHY PROTECTION CONTROL 11
4.3 SYSTEMS ENGINEERING FRAMES SECURE CYBER RESILIENT ENGINEERING 13
4.4 SYSTEM PROTECTION CONTROL 15
4.4.1 Protection Control Constraint Enforcement Basis 15
4.4.2 Protection Control Scenario 16
4.4.3 Protection Control Design Objectives 19
4.5 SYSTEM FUNCTIONALITY 21
4.5.1 Intended System Functionality 21
4.5.2 Security Functionality 21
4.6 PROPERTIES OF INHERENTLY SECURE AND RESILIENT SYSTEM DESIGN AND FUNCTIONALITY 21
4.6.1 Secure and Resilient Protection Control Design 22
4.6.2 Secure and Resilient Protection Control Functionality 23
4.6.3 Design Order of Precedence for Secure and Resilient Systems 24
4.7 ASSURED SYSTEM TRUSTWORTHINESS 26
4.7.1 Assured Secure and Resilient System Trustworthiness 27
4.7.2 Assurance and Risk 28

WPs inform Sec 5

5 SECURE CYBER RESILIENT ENGINEERING SYSTEM DESIGN EXECUTION 29
5.1 INTRODUCTION 29
5.2 SYSTEM DEFINITION 30
5.3 TASKS OVERVIEW 33
5.3.1 Task Structure 33
5.4 MANAGEMENT TASKS 33
5.5 ANALYSIS TASKS 41
5.6 SYSTEM DEFINITION TASKS 44

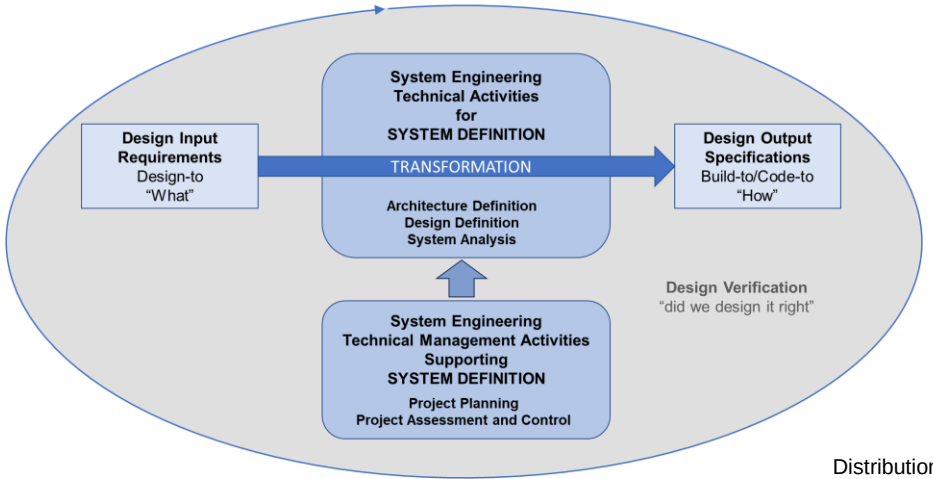
Approach …

Primary goal is control of the loss potential that is directly associated with the capabilities provided by the system and the intended use of those system capabilities

- Prevent the losses that can be prevented
- Limit to tolerable levels, the consequence, impact, and severity of adverse effects and loss that cannot be prevented

Secondary goal is control of the loss potential that is directly associated with the capabilities provided by the engineered protection control functionality and the intended use of those protection control capabilities

- Avoid introducing, enabling, or triggering loss scenarios and adverse effects due to the employment of specific protection control functionality
- Limit to tolerable levels the consequence, impact, and severity of adverse effects and loss that cannot be avoided when employing necessary protection control functionality that introduce, enable, or trigger loss scenarios and adverse effects



The design aspect of the practice is comprised of activities that are:

- **Principled:** Built upon concepts and principles for a system design with the protection control capability that is a necessary capability of any secure and resilient system.

  The characteristic of being a necessary capability means that the design approach is universally applicable to establish a basis fulfilling any specific protection requirement or acceptance criteria, and not based on countering any specific susceptibility, vulnerability, hazard, and associated threats.

- **Optimized protection effectiveness:** Seeks to produce a design that, to the extent practical, eliminates design-based susceptibility, vulnerability, and hazard, thereby reducing the presence of susceptibility, vulnerability, and hazard that must be controlled.

- **Effect-based and cause-informed:** Distinguishes cause and effect. Places emphasis on protection control of effects independent of cause.

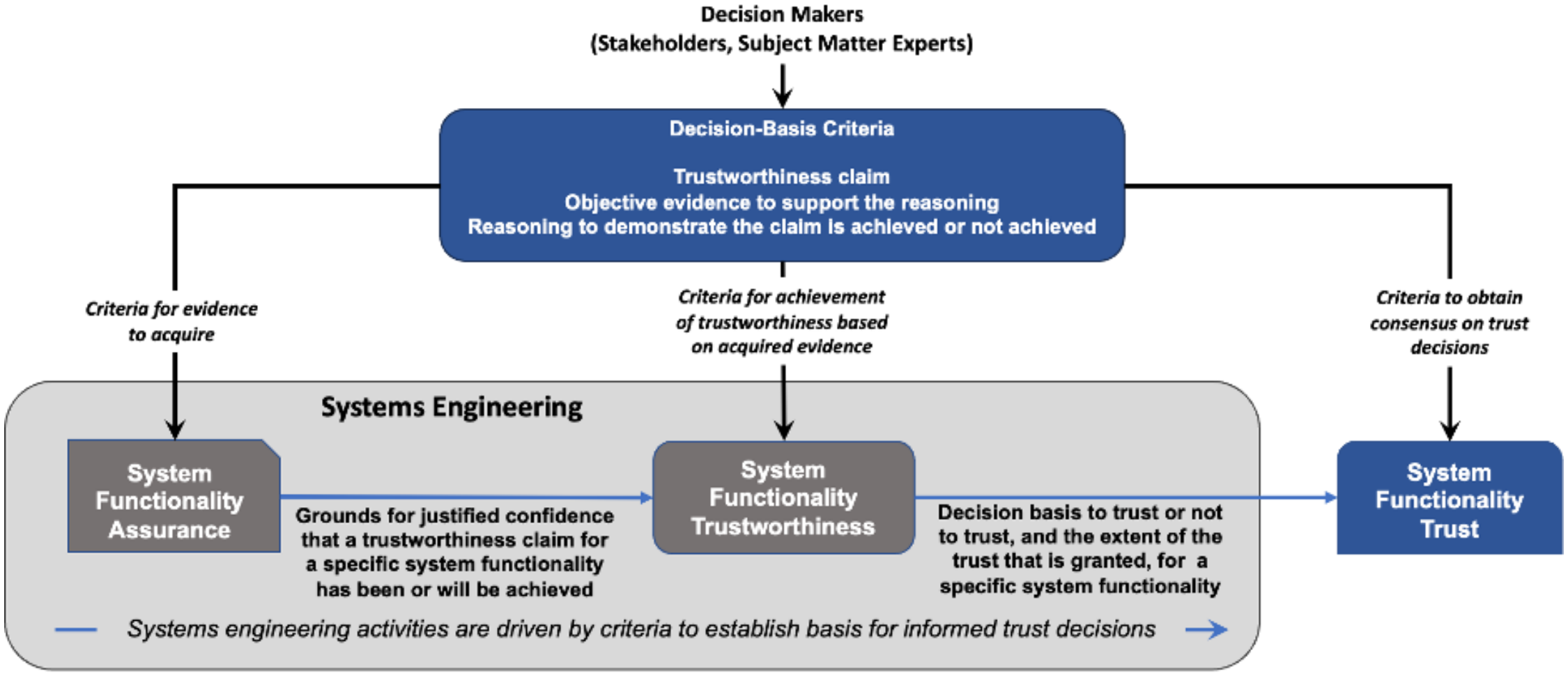
- **Effective against adversity across-the-board:** Recognizes that adversity is ever-present in all environments and exists in both malicious and non-malicious forms.

  - Adversity, regardless of the presence or absence of malicious or any intent, may result in unacceptable consequences and losses.

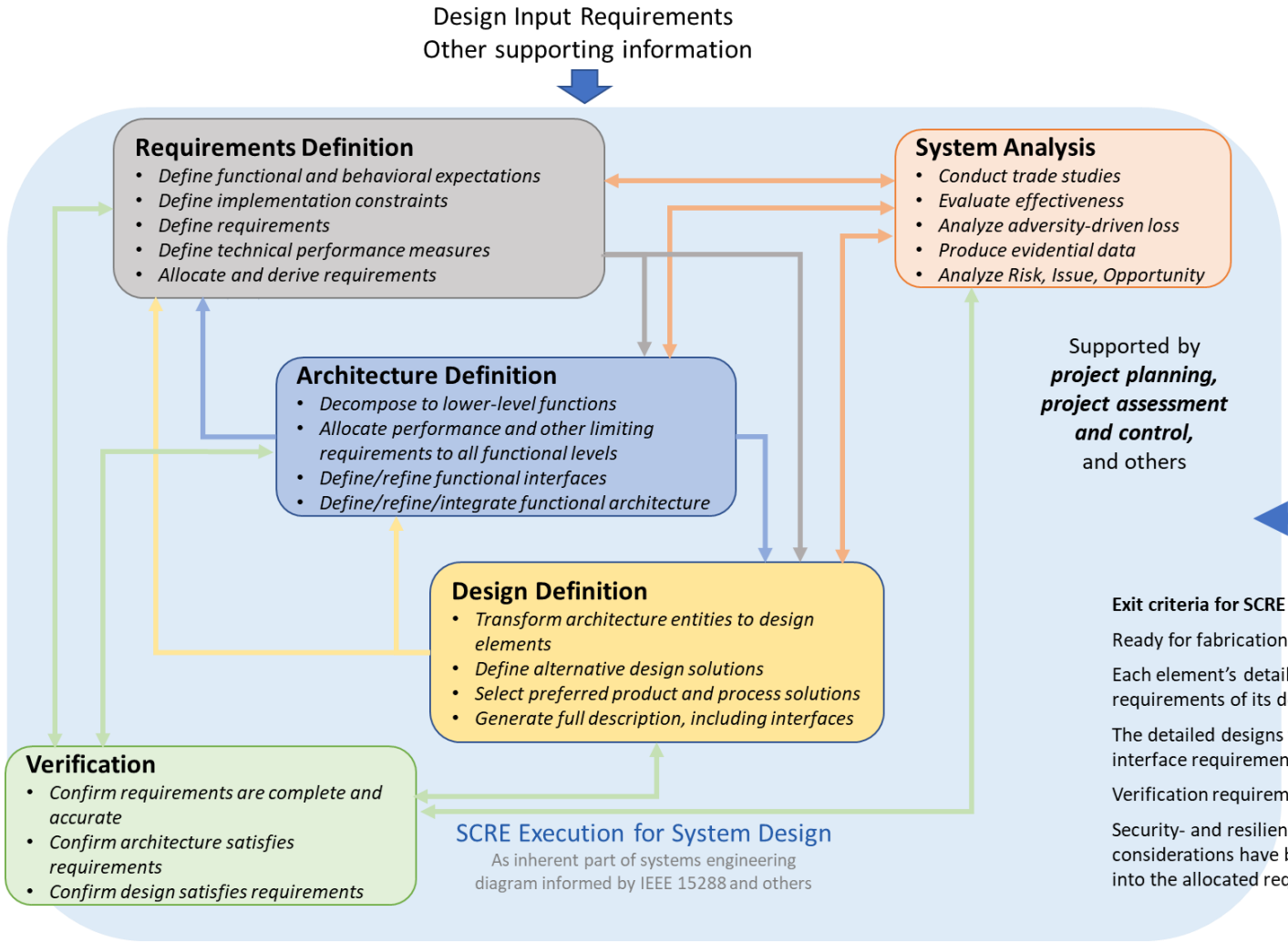
- **Assured trustworthiness:** Produces objective evidence used in reasoning about the fulfillment of trustworthiness claims..

- **Integrated into systems engineering**

… building assured system trustworthiness



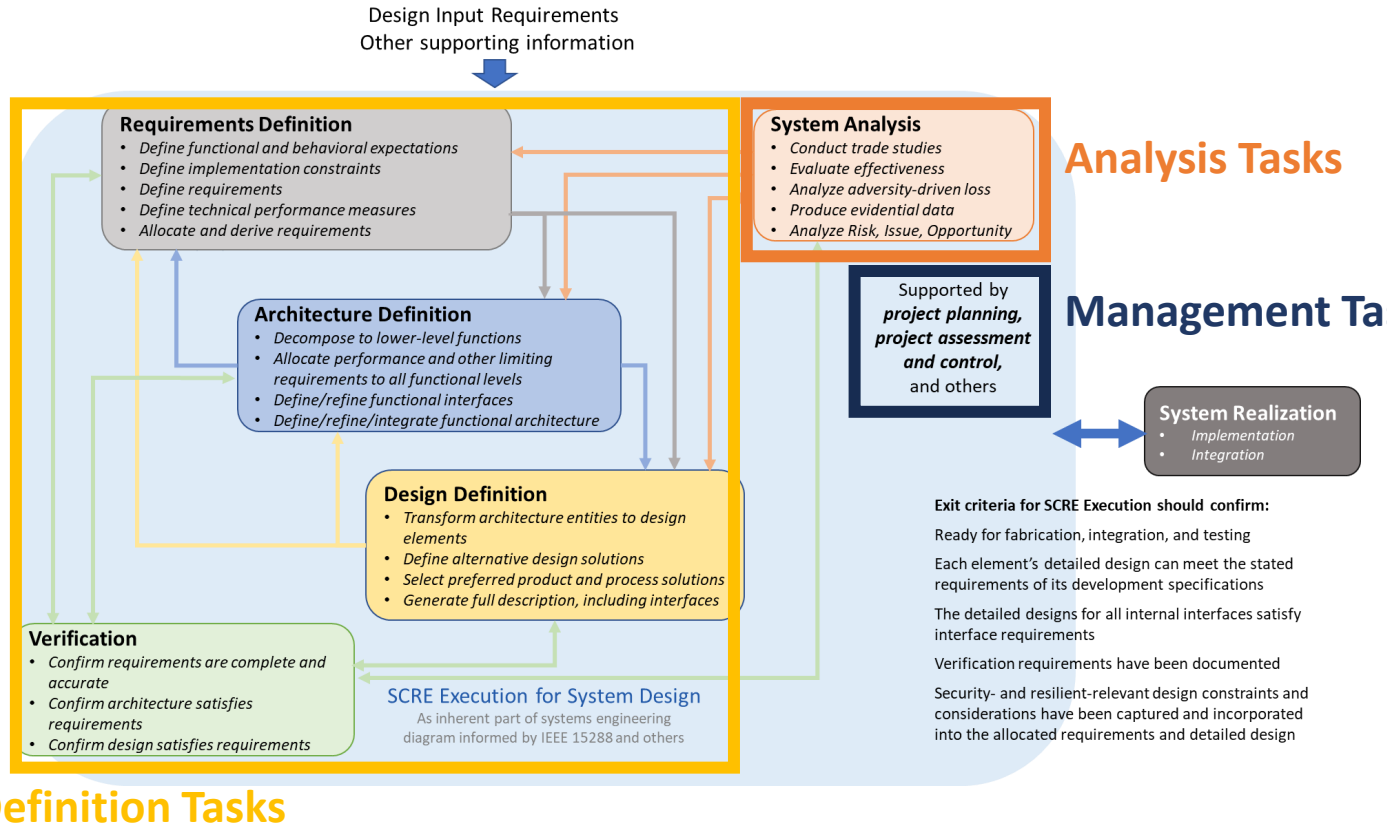
Context for SCRE Execution for System Design



Executed iteratively, recursively, and concurrently

Section 5 provides guidance on tasks

- Task structure
  - **Purpose** – what is to be accomplished
  - **Rationale** – explains why it is important
  - **Description** – needed results
- Divided to three categories
  - Management
  - Analysis
  - System Definition



Management Tasks

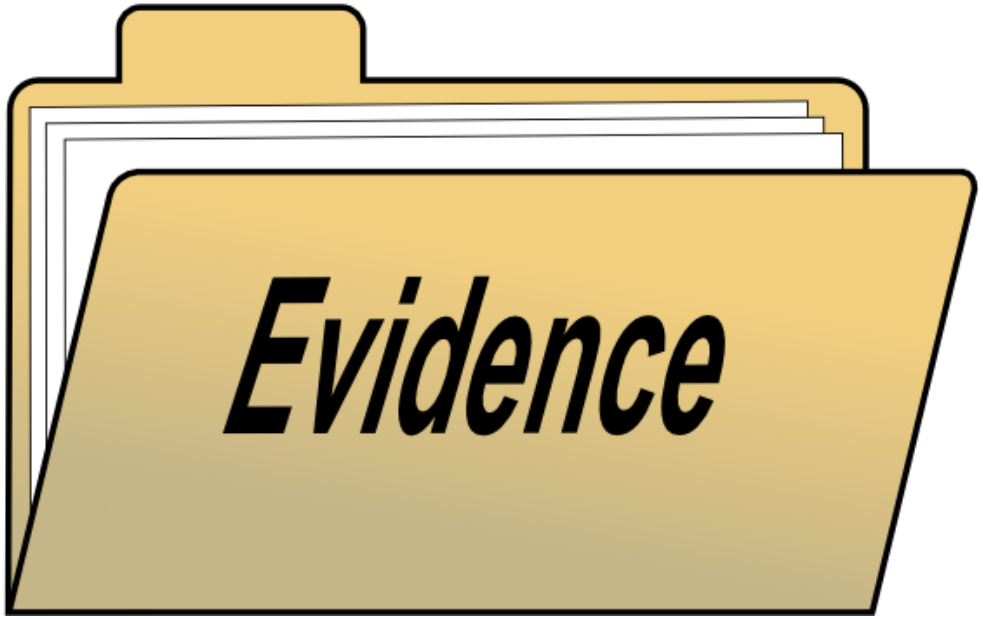
Tasks associated with project planning, project assessment and control, and other project management and execution activities

- Includes planning what systems engineering must do re: security and resilience
- Analogous to Management Tasks within **MIL STD 882E Systems Safety**

5.4 MANAGEMENT TASKS 33
5.4.1 SCRE Management Plan 33
5.4.3 Support of Government Reviews and Audits 36
5.4.4 Integrated Product Team and Working Group Support 36
5.4.5 Deficiencies Report 36
5.4.6 SCRE Progress Reports 37
5.4.7 System Security Concept 37
5.4.8 Assurance Body of Knowledge 38
5.4.9 Technology Assessments and Cost Studies 41
5.4.10 Logistics Support 41

Analysis Tasks

Tasks associated with various systems analyses which produce data that provides evidence for decision making and for assurance

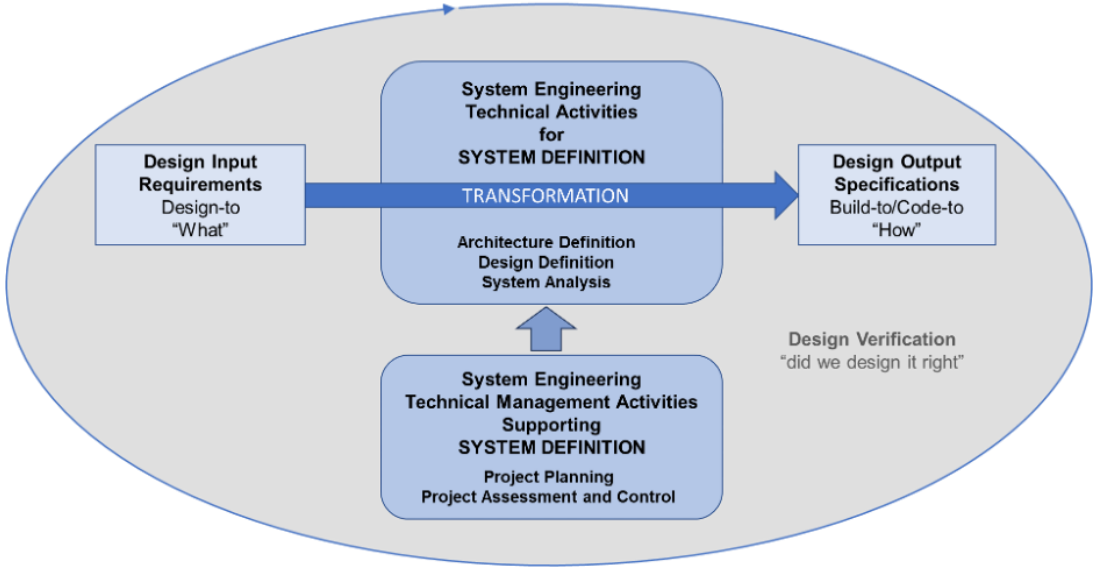


5.5 ANALYSIS TASKS 41
5.5.1 Analyze Adversity Uncertainty 41
5.5.2 Identify Product Susceptibility, Vulnerability, and Hazards 41
5.5.3 Analyze Protection Functions 42
5.5.4 Analyze Requirement Set 42
5.5.5 Analyze Constraint Options 43
5.5.6 Analyze Design Alteration Alternatives 43

Systems Definition Tasks

SE tasks to be conducted as an integrated part of SE

- These complement the systems engineering planning considerations for security and resilience within the SCRE Management Plan and Functional Assurance Plan



5.6 SYSTEM DEFINITION TASKS 44
5.6.1 Define Functional and Behavior Expectations 44
5.6.2 Identify Adversity 45
5.6.3 Define Architecture Criteria 45
5.6.4 Define Design Criteria 46
5.6.5 Alter Design 46
5.6.6 Define Performance Requirements 46

Next Steps

- Respond to feedback
  - Incorporate into guidance as appropriate
  - Develop products reflecting needs identified in feedback
  - Other in-depth guidance (candidate)
- Share in other formats
  - Advancing systems engineering is a partnership
    - Candidate – INCOSE

Questions?

References

- Department of Defense, “DoD Instruction 5000.83: Technology and Program Protection to Maintain Technological Advantage.” July 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

- ISO/IEC/IEEE 15288:2023, “Systems and software engineering —Systems life cycle processes”, May 2023

- Department of Defense Standard Practice: System Safety MIL STD 882E, May 2012