Developing Requirements for Secure System Function

NDIA 20th Annual Systems Engineering Conference
October 23-26, 2017
Springfield VA

Michael McEvilley
Max Allway
Alvi Lim

The MITRE Corporation
Systems Engineering Technical Center
mcevilley@mitre.org
703.472.5409

Approved for Public Release; Distribution Unlimited. Case Number 17-3190

The authors affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the authors.

MITRE

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Basis for Effort

- **Integrating SSE into SE across multiple sponsor organizations and foci:**
  - AFLCMC/EZC Cyber Systems Engineering Division
  - Systems Mission Assurance Working Group (SMAWG)
  - PEO-BM process improvements to Anti-Tamper
  - Cyber Resiliency Steering Group (CRSG)
  - AF Cyber Campaign Plan

- **Recognition of the need for foundational requirements-oriented considerations informed by results of Program Protection pathfinders for CPI and CC identification**
  - Security requirements elicitation, analysis, and negotiation activities to identify, establish valuation of, and prioritize assets

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)
© 2017 The MITRE Corporation. All Rights Reserved.

Motivation for this Effort

- **Lack of foundational material in a form that is suitable to build application guidance for system security**
  - There is no security equivalent to MIL-STD-882E (2012), Department of Defense Standard Practice, System Safety
  - MIL-STD-1785 Systems Security Engineering (1989) was recast and remains validated as MIL-HDBK-1785 (1995/2014)
- **Computer security foundational materials date back to the 1970's – but have not been interpreted for "system context" application**
  - Ware, Anderson, Saltzer and derivative works
  - Developed to target "design for" and not "demonstrate compliance to" objectives

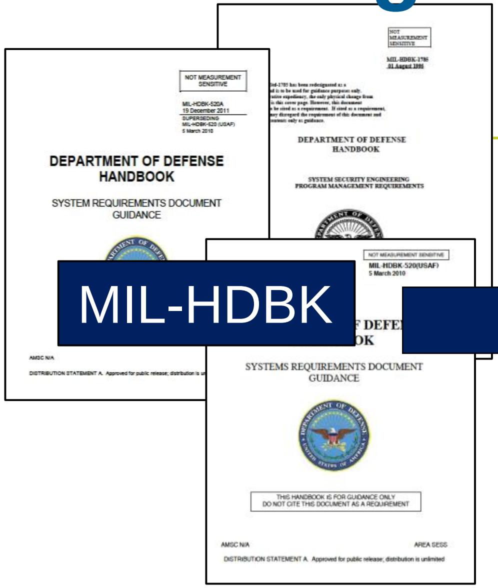
❖ **W. Ware**, et al, "Security Controls for Computer Systems," Report of the Defense Science Board Task Force on Computer Security, February 1970.

❖ **J. Anderson**, et al., "Computer Security Technology Planning Study," Technical Report ESD-TR-73- 51, Air Force Electronic Systems Division, Hanscom AFB, October 1972.

❖ **J. Saltzer**, M. Schroeder, "The Protection of Information in Computer Systems," Proceedings of the IEEE, September 1975, 1278–1308.

© 2017 The MITRE Corporation. All Rights Reserved.

Informing Aspects to the Effort



NOT MEASUREMENT SENSITIVE

MIL-HDBK-520A
19 December 2011
SUPERSEDING
MIL-HDBK-520 (USAF)
5 March 2010

DEPARTMENT OF DEFENSE HANDBOOK

SYSTEM REQUIREMENTS DOCUMENT GUIDANCE

AMSC N/A

DISTRIBUTION STATEMENT A. Approved for public release; distribution is un

NOT MEASUREMENT SENSITIVE

MIL-HDBK-1785
01 August 1995

Std-1785 has been redesignated as a … and is to be used for guidance purposes only. … administrative expediency, the only physical change from … is this cover page. However, this document … be cited as a requirement. If cited as a requirement, … may disregard the requirement of this document and … content only as guidance.

DEPARTMENT OF DEFENSE HANDBOOK

SYSTEM SECURITY ENGINEERING PROGRAM MANAGEMENT REQUIREMENTS

NOT MEASUREMENT SENSITIVE

MIL-HDBK-520(USAF)
5 March 2010

F DEFE… OK

SYSTEMS REQUIREMENTS DOCUMENT GUIDANCE

THIS HANDBOOK IS FOR GUIDANCE ONLY
DO NOT CITE THIS DOCUMENT AS A REQUIREMENT

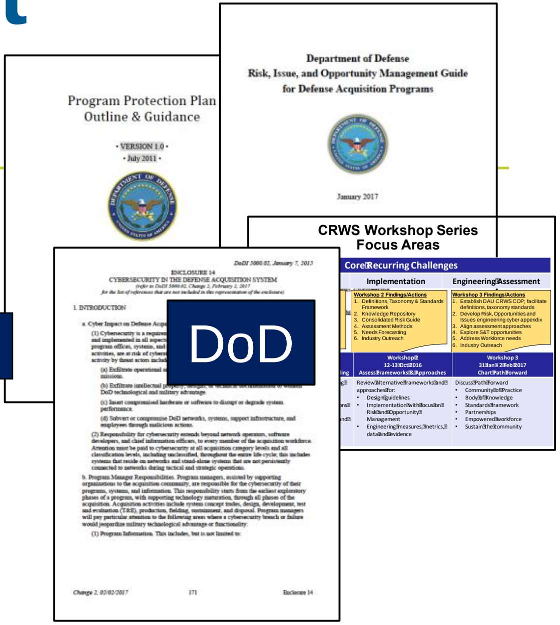
AMSC N/A

AREA SESS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

MIL-HDBK

Developing Requirements for Secure System Function: Foundation, Method, and Supporting Considerations



Department of Defense
Risk, Issue, and Opportunity Management Guide
for Defense Acquisition Programs

January 2017

Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

DoDI 5000.02, January 7, 2015

ENCLOSURE 14
CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM
(refer to DoDI 5000.02, Change 2, February 2, 2017
for the list of references that are not included in this representation of the enclosure)

1. INTRODUCTION

a. Cyber Impact on Defense Acqu…

Change 2, 02/02/2017 171 Enclosure 14

CRWS Workshop Series
Focus Areas

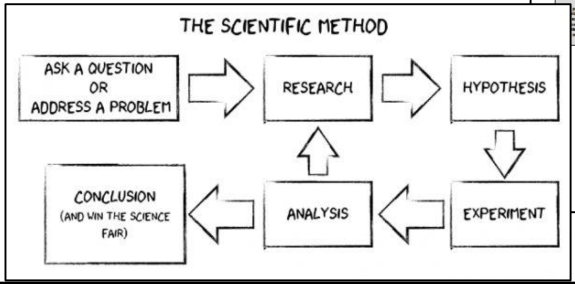
Core Recurring Challenges

Implementation	Engineering Assessment
Workshop 2 Findings/Actions 1. Definitions, Taxonomy & Standards Framework 2. Knowledge Repository 3. Consolidated Risk Guide 4. Assessment Methods 5. Needs Forecasting 6. Industry Outreach	**Workshop 3 Findings/Actions** 1. Establish DAU CRWS COP; facilitate definitions, taxonomy standards 2. Develop Risk, Opportunities and Issues engineering cyber appendix 3. Align assessment approaches 4. Explore S&T opportunities 5. Address Workforce needs 6. Industry Outreach
Workshop 2 12-13 Oct 2016 Assess Frameworks & Approaches	Workshop 3 31 Jan – 2 Feb 2017 Chart Path Forward
Review alternative frameworks and approaches for: • Design guidelines • Implementation with focus on Risk and Opportunity Management • Engineering measures, metrics, data and evidence	Discuss Path Forward • Community of Practice • Body of Knowledge • Standards framework • Partnerships • Empowered workforce • Sustain the community

DoD

AF Support

- CPI Identification
- CC Identification
- Integrated CPI and CC Identification
- Program and SRD Analysis


THE SCIENTIFIC METHOD
ASK A QUESTION OR ADDRESS A PROBLEM
RESEARCH
HYPOTHESIS
EXPERIMENT
ANALYSIS
CONCLUSION (AND WIN THE SCIENCE FAIR)

The Protection of Information in Computer Systems

…OR MEMBER, IEEE, AND …ER, MEMBER, IEEE

SECURITY CONTROLS FOR COMPUTER SYSTEMS (U)

…nce Board

…ublication 800-160

Systems Security …
Considerations for a Multidisci…
Engineering of Trust…

ISI-TR-nnn
NPS-CS-08-001

SecureCore

Trustworthy Commodity Computation and Communication

SecureCore Technica…

NASA/SP-2010-580
Version 1.0
November 2011

NASA System Safety Handbook

Volume 1, System Safety Framework and Concepts for Implementation

Government, Industry, Academia

Comprehensive multidisciplinary and system-oriented considerations to incorporate security in Capability, Requirements, and Performance artifacts

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

MITRE

Discussion Topics

- **Section 1**
  - Challenges to engineering dependably secure systems
- **Section 2**
  - Concept and principle base
- **Section 3**
  - Method to drive requirements elicitation, analysis, negotiation
- **Section 4**
  - Viewpoint-driven considerations

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013) **© 2017 The MITRE Corporation. All Rights Reserved.**

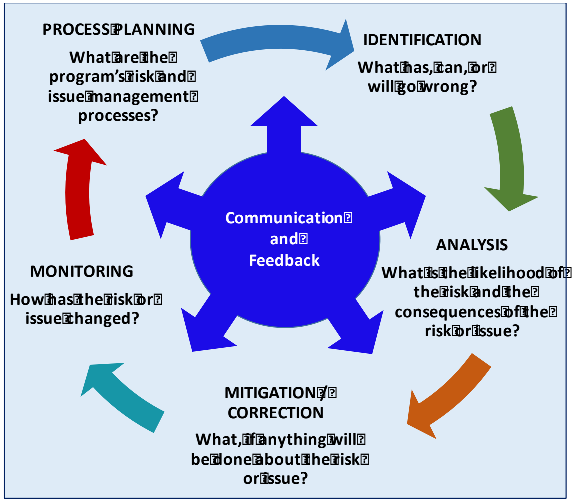
Section 1 – Challenges

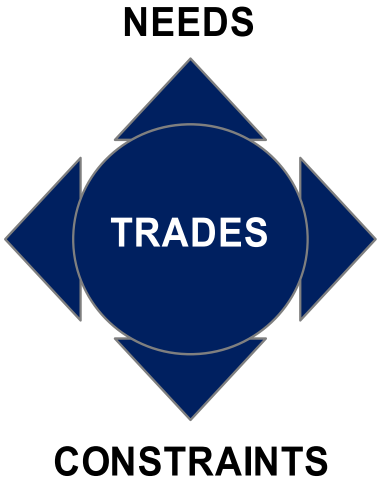
This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)
© 2017 The MITRE Corporation. All Rights Reserved.

Challenges to the Effective Engineering of Dependably Secure Systems

- Absence of system perspective
- Accurately framing the problem
- Need for requirements-based risk management
- Level-of-Rigor (LoR) and evidence-based system security
- Dependably secure system function
- Uncertainty and the limits in understanding technology

Systems Engineering Need


PROCESS PLANNING
What are the program's risk and issue management processes?
IDENTIFICATION
What has, can, or will go wrong?
Communication and Feedback
ANALYSIS
What is the likelihood of the risk and the consequences of the risk or issue?
MITIGATION / CORRECTION
What, if anything will be done about the risk or issue?
MONITORING
How has the risk or issue changed?



- Security of the Intended System Function
- Security Function of the System
- Security of Life Cycle Assets

While processes help, the quality and effectiveness of risk mitigation planning, judgement, "What we call 'requirements' determines a great deal – almost everything – about the risks we need to manage" ~ AT&L Memorandum, Jan 2017

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

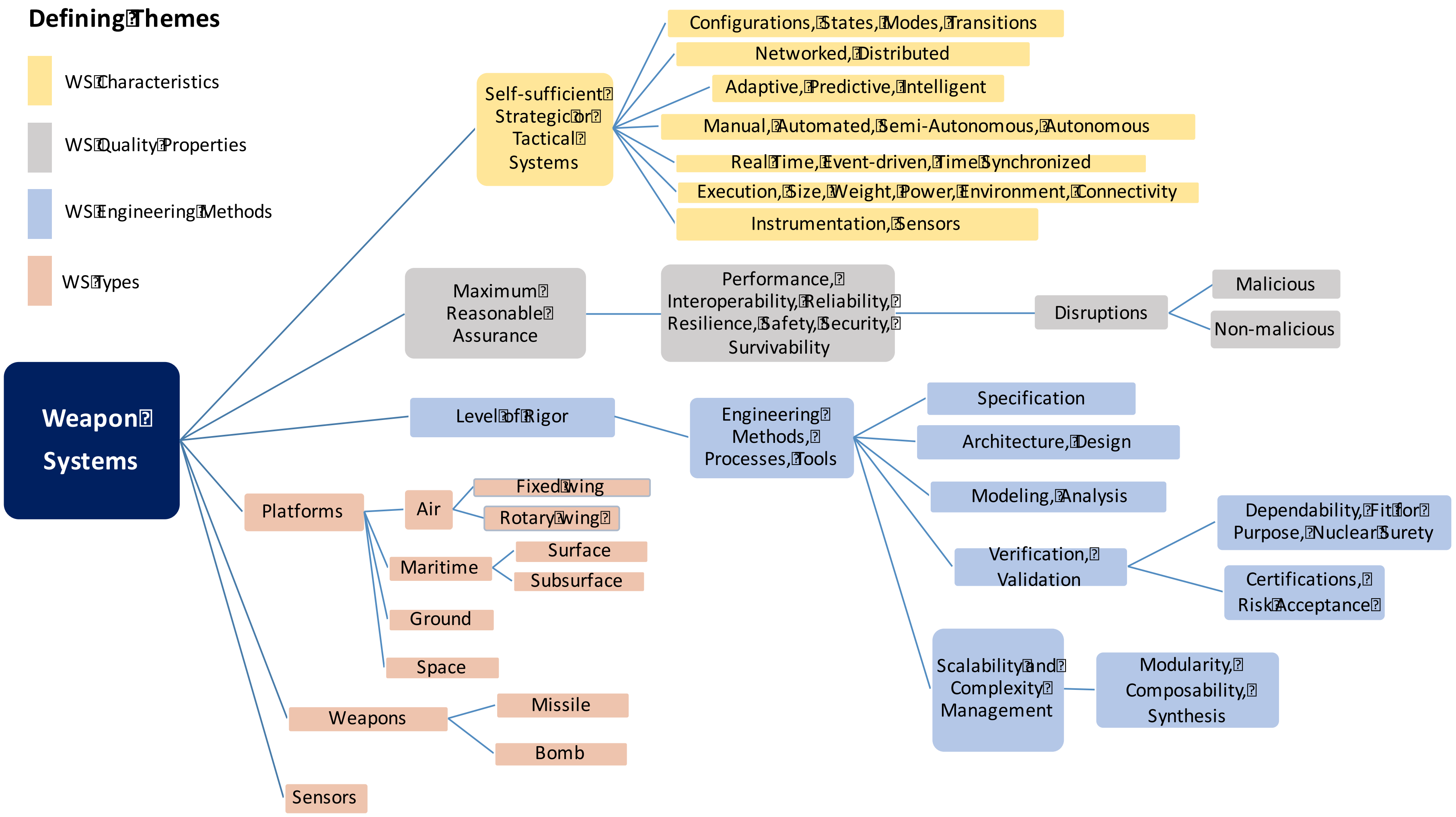
Section 2 – Concept and Principle Base

MITRE

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)
© 2017 The MITRE Corporation. All Rights Reserved.

Weapon Systems Characterization

Intentionally destructive delivery of lethal force



Defining Themes

- WS Characteristics
- WS Quality Properties
- WS Engineering Methods
- WS Types

- Weapon Systems
  - Self-sufficient Strategic or Tactical Systems
    - Configurations, States, Modes, Transitions
    - Networked, Distributed
    - Adaptive, Predictive, Intelligent
    - Manual, Automated, Semi-Autonomous, Autonomous
    - Real Time, Event-driven, Time Synchronized
    - Execution, Size, Weight, Power, Environment, Connectivity
    - Instrumentation, Sensors
  - Maximum Reasonable Assurance
    - Performance, Interoperability, Reliability, Resilience, Safety, Security, Survivability
      - Disruptions
        - Malicious
        - Non-malicious
  - Level of Rigor
    - Engineering Methods, Processes, Tools
      - Specification
      - Architecture, Design
      - Modeling, Analysis
      - Verification, Validation
        - Dependability, Fit for Purpose, Nuclear Surety
        - Certifications, Risk Acceptance
      - Scalability and Complexity Management
        - Modularity, Composability, Synthesis
  - Platforms
    - Air
      - Fixed wing
      - Rotary wing
    - Maritime
      - Surface
      - Subsurface
    - Ground
    - Space
  - Weapons
    - Missile
    - Bomb
  - Sensors

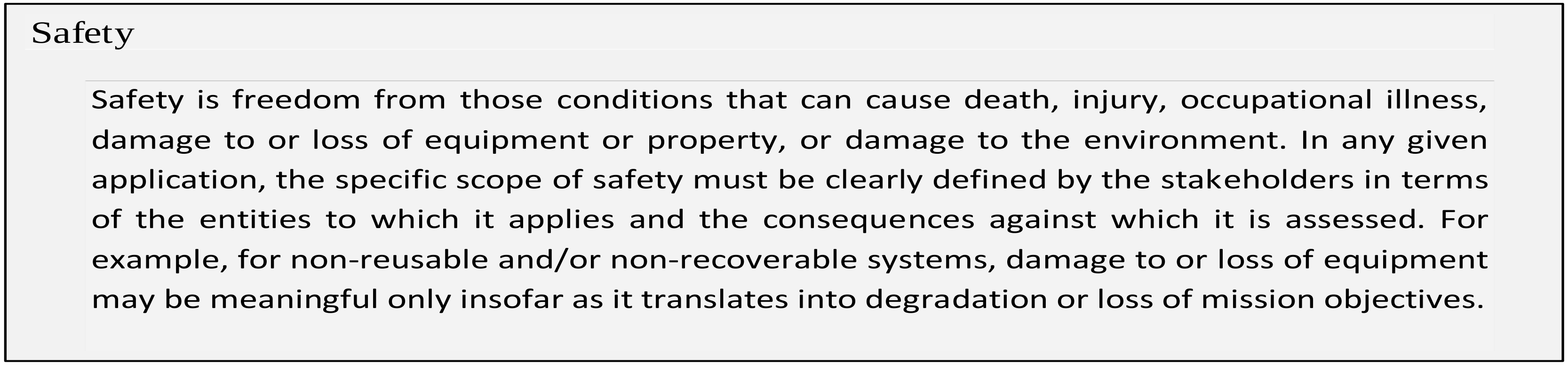
This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Security
Working Definitions

Each adapted from NASA (NASA System Safety Handbook VOL1, 2011)

- **Security**
  - – Freedom from those conditions that can cause loss of assets with unacceptable consequences
    - Stakeholder judgement
- **Secure System**
  - – A system that for all states, modes, and transitions is deemed adequately secure
    - i.e., demonstrates “freedom from those conditions ...”
- **Adequate Security**
  - – Meets the minimum tolerable level of security performance
  - – Maximizes security performance relative to the impact of commitments that must be made and/or degradation of system performance



Safety

Safety is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. In any given application, the specific scope of safety must be clearly defined by the stakeholders in terms of the entities to which it applies and the consequences against which it is assessed. For example, for non-reusable and/or non-recoverable systems, damage to or loss of equipment may be meaningful only insofar as it translates into degradation or loss of mission objectives.

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Predominant Views of System Security

- **Security of the Intended System Function**
  - Security-driven constraints on all system functions
    - Avoid, eliminate, tolerate, forecast
      - defects, exposure, flaws, weaknesses

- **Security Function of the System**
  - Security functions that provide system protection capability
    - Mechanisms that constitute controls, countermeasures, features, inhibits, overrides, safeguards

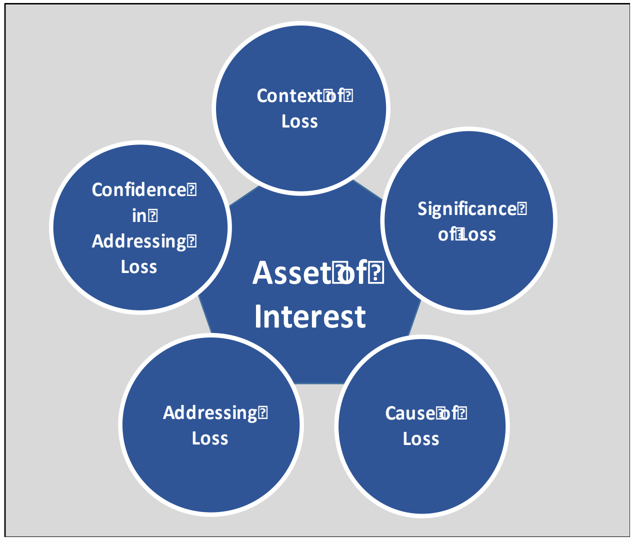
- **Security of Life Cycle Assets**
  - Security for data, information, technology, methods, and other assets associated with the system throughout its life cycle

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013) © 2017 The MITRE Corporation. All Rights Reserved.

Concept and Principle Coverage

- System, security, and adequate security
- Assets and reasoning about asset loss
- Secure system function
- Strategy for secure system function
- Risk, issue, and opportunity management

Ultimately – system security is about assets and the effect of their loss relative to the system-of-interest ands its enabling and supporting systems



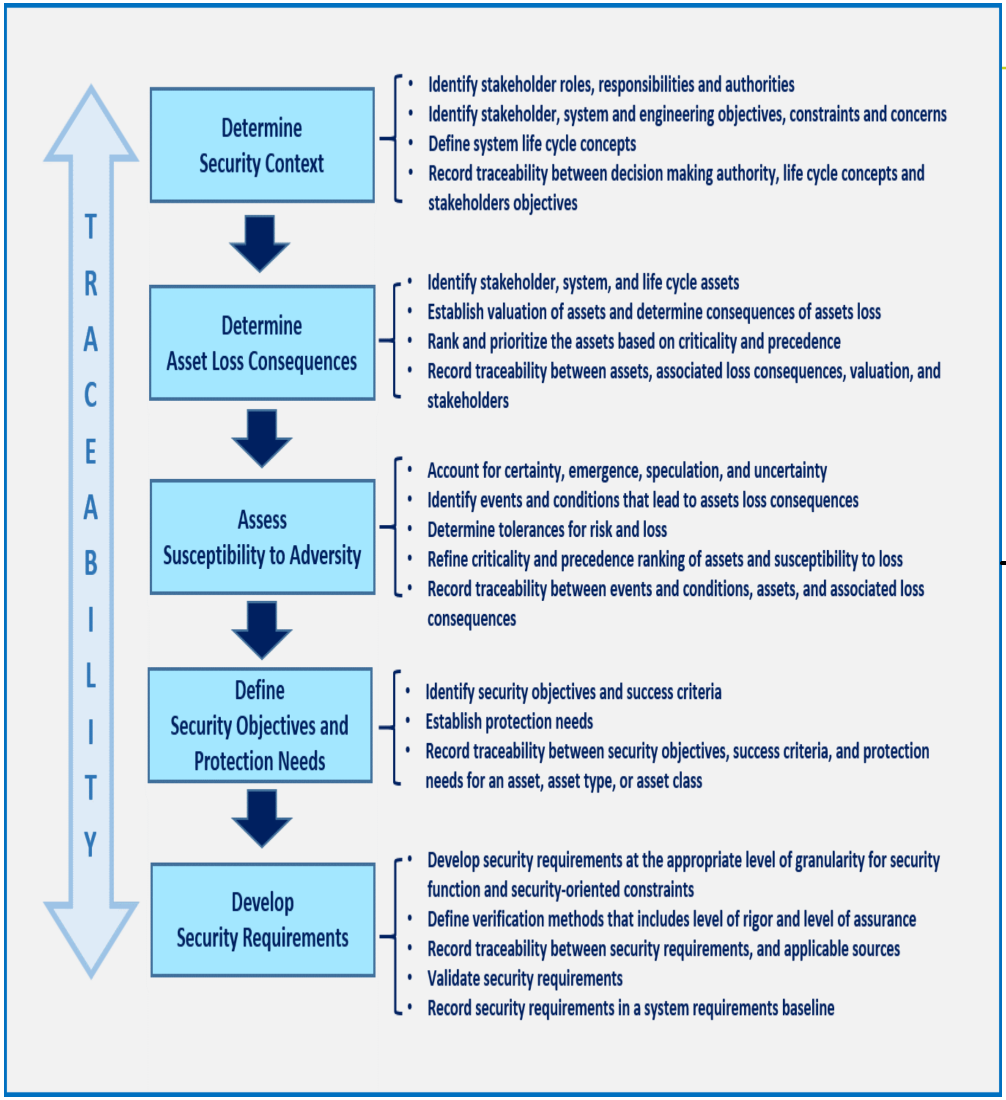
This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Section 3 – Method

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)
© 2017 The MITRE Corporation. All Rights Reserved.

Generalized Security Requirements Elicitation, Analysis, Negotiation Method



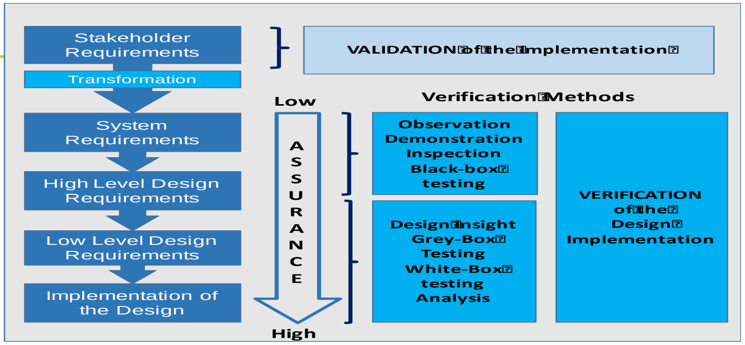
Determine Security Context
- Identify stakeholder roles, responsibilities and authorities
- Identify stakeholder, system and engineering objectives, constraints and concerns
- Define system life cycle concepts
- Record traceability between decision making authority, life cycle concepts and stakeholders objectives

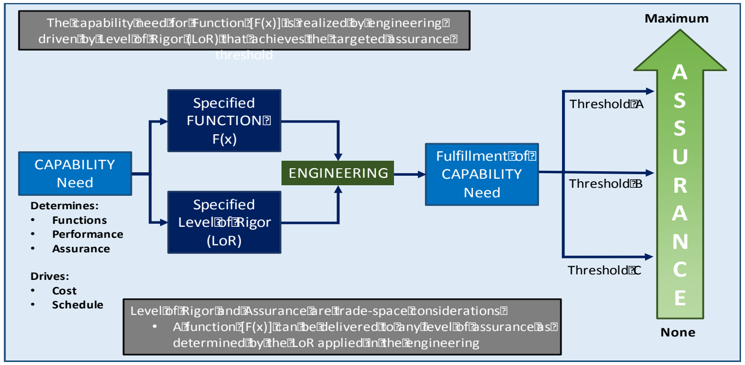
Determine Asset Loss Consequences
- Identify stakeholder, system, and life cycle assets
- Establish valuation of assets and determine consequences of assets loss
- Rank and prioritize the assets based on criticality and precedence
- Record traceability between assets, associated loss consequences, valuation, and stakeholders

Assess Susceptibility to Adversity
- Account for certainty, emergence, speculation, and uncertainty
- Identify events and conditions that lead to assets loss consequences
- Determine tolerances for risk and loss
- Refine criticality and precedence ranking of assets and susceptibility to loss
- Record traceability between events and conditions, assets, and associated loss consequences

Define Security Objectives and Protection Needs
- Identify security objectives and success criteria
- Establish protection needs
- Record traceability between security objectives, success criteria, and protection needs for an asset, asset type, or asset class

Develop Security Requirements
- Develop security requirements at the appropriate level of granularity for security function and security-oriented constraints
- Define verification methods that includes level of rigor and level of assurance
- Record traceability between security requirements, and applicable sources
- Validate security requirements
- Record security requirements in a system requirements baseline


Stakeholder Requirements
Transformation
System Requirements
High Level Design Requirements
Low Level Design Requirements
Implementation of the Design
VALIDATION of the Implementation
Low
ASSURANCE
High
Verification Methods
Observation Demonstration Inspection Black-box testing
Design Insight Grey-Box Testing White-Box testing Analysis
VERIFICATION of the Design Implementation

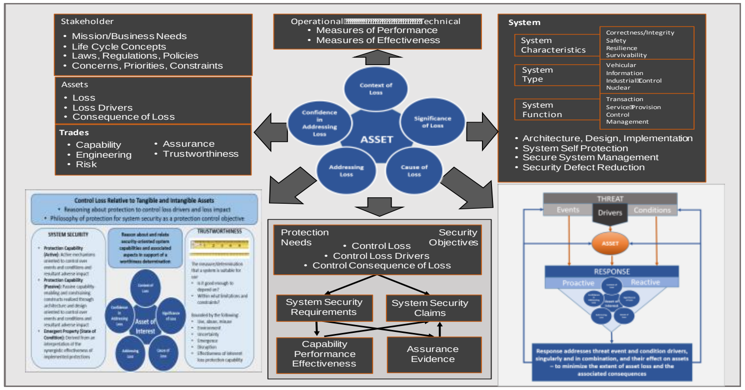


The capability need for Function [F(x)] is realized by engineering driven by Level of Rigor (LoR) that achieves the targeted assurance threshold

Determines:
- Functions
- Performance
- Assurance

Drives:
- Cost
- Schedule

Level of Rigor and Assurance are trade-space considerations
- A function [F(x)] can be delivered to any level of assurance as determined by the LoR applied in the engineering


Context of Loss
Confidence in Addressing Loss
Significance of Loss
ASSET
Addressing Loss
Cause of Loss
Control Loss Relative to Tangible and Intangible Assets
Reasoning about protection to control loss drivers and loss impact
Philosophy of protection for system security as a protection control objective
SYSTEM SECURITY
TRUSTWORTHINESS
Asset of Interest
THREAT
Events
Drivers
Conditions
ASSET
RESPONSE
Proactive
Reactive
Response addresses threat event and condition drivers, singularly and in combination, and their effect on assets – to minimize the extent of asset loss and the associated consequences

Stakeholder
- Mission/Business Needs
- Life Cycle Concepts
- Laws, Regulations, Policies
- Concerns, Priorities, Constraints

Assets
- Loss
- Loss Drivers
- Consequence of Loss

Trades
- Capability
- Engineering
- Risk
- Assurance
- Trustworthiness

Operational Technical
- Measures of Performance
- Measures of Effectiveness

System

System Characteristics	Correctness/Integrity Safety Resilience Survivability
System Type	Vehicular Information Industrial Control Nuclear
System Function	Transaction Service Provision Control Management

- Architecture, Design, Implementation
- System Self Protection
- Secure System Management
- Security Defect Reduction

Protection Needs
Security Objectives
- Control Loss
- Control Loss Drivers
- Control Consequence of Loss

System Security Requirements
System Security Claims
Capability Performance Effectiveness
Assurance Evidence

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

MITRE

Section 4 – Viewpoint Considerations

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

System Requirements “Viewpoints”

MIL-HDBK-520A – System Requirements Document (SRD) Guidance

A.3 System or Subsystem Requirements

A.3.1 Required states and modes

A.3.2 System or subsystem functional requirements

A.3.3 System external interface requirements

A.3.4 System internal interface requirements

A.3.5 System internal data requirements

A.3.6 Adaptation requirements

A.3.7 Environmental, Safety, and Operational Health (ESOH) requirements

A.3.8 Security and privacy requirements

A.3.9 System environment requirements

A.3.10 Computer resource requirements

A.3.11 System quality factors

A.3.12 Design and construction constraints

A.3.13 Personnel-related requirements

A.3.14 Training-related requirements

A.3.15 Logistics-related requirements

A.3.16 Other requirements

A.3.17 Packaging requirements

A.3.18 Statutory, regulatory, and certification requirements

A.3.19 Precedence and criticality of requirements

A.3.20 Demilitarization and disposal

A.4 VERIFICATION PROVISIONS

A.4.1 Verification methods

A.5 REQUIREMENTS TRACEABILITY

A.5.1 Traceability to capability document or system specification

A.5.2 Traceability to subsystems requirements

Although security requirements are explicitly called out in A.3.8, security-driven concerns regarding *Security of the Intended System Function* affect content throughout A.3, A.4, A.5

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Revised Viewpoints

4. Secure System Function Requirements Considerations

4.1 System States and Modes
4.2 System Functions
4.3 Communication
4.4 System Interfaces
4.5 Design and Construction Constraints
4.6 Safety
4.7 System Environment
4.8 System Configuration and Adaptation
4.9 Computing
4.10 System Quality Factors
4.11 Maintenance
4.12 Logistics
4.13 Packaging, Labeling, and Handling
4.14 Personnel
4.15 Training
4.16 Statutory, Regulatory, and Certification
4.17 Retirement and Disposal
4.18 Priority and Criticality of Requirements
4.19 Other Requirements
4.20 Verification
4.21 Traceability

- **Each viewpoint provides a “lens” into the system to provide an explicit statement of a need to be met**
  - **Proactive**
  - **Reactive**
  - **Constraining**

- **The requirements for secure system function have two generic forms**
  - **Explicit function**
  - **Explicit constraint**

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.

Conclusion

- **SSE and what it represents as a necessary part of SE remains an open-ended question**
  - We continue to evolve our thinking towards an optimal end state

- **Challenges remain and are primarily rooted in**
  - Absence of system-oriented security perspective
  - Viewing security through an operations, organizational, and IT lens
  - Insufficient leveraging from other disciplines

- **This work is oriented to closing the gap between SE and SSE with focus limited to requirements elicitation, analysis, and negotiation for secure system function**

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013) © 2017 The MITRE Corporation. All Rights Reserved.

Future Work

- **Explicitly bring in resilience considerations**
- **Add depth to Section 4 viewpoint considerations**
- **Elaborate on the tasks in each of the activities presented in the Section 3 generalized method**
- **Explore other specialties and disciplines and incorporate their concepts, principles, and methods to more effectively achieve secure system function when operating in contested cyberspace**
  - System safety
  - Fault tolerance
  - Reliability

This technical data was produced for the U. S. Government under Contract No. FA8702-17-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

© 2017 The MITRE Corporation. All Rights Reserved.