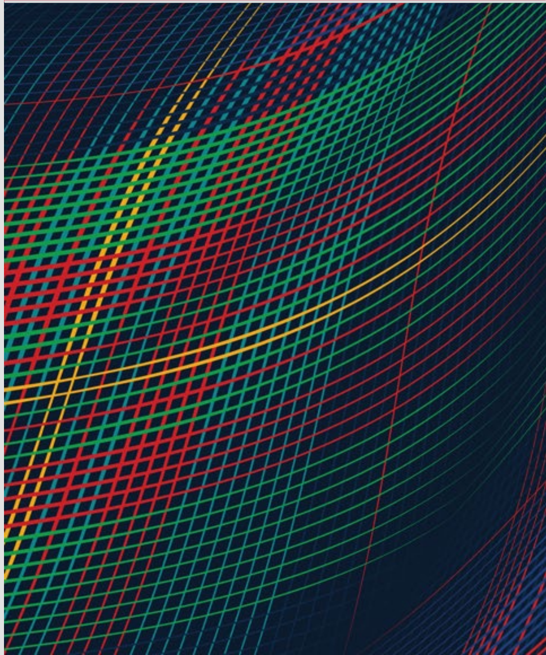
Carnegie Mellon University
Software Engineering Institute



An Approach Applying Zero Trust in Acquisition

JUNE 12, 2023

Tim Morrow
CMU/SEI CERT Situational Awareness Technical Manager

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

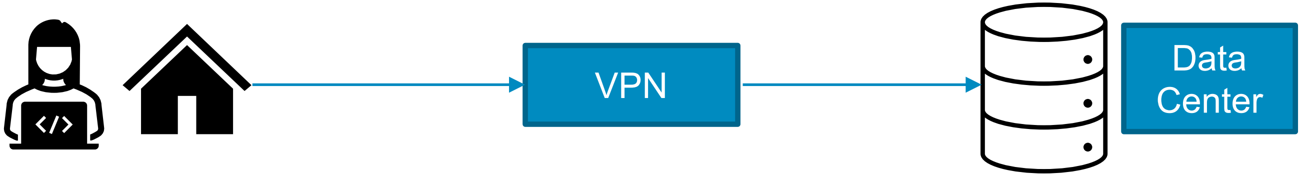
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM23-0553

Overview

Why apply a zero trust strategy for cybersecurity?



Zero trust is a security model that John Kindervag and his team from Forrester Research, Inc. developed in 2009.

Goals

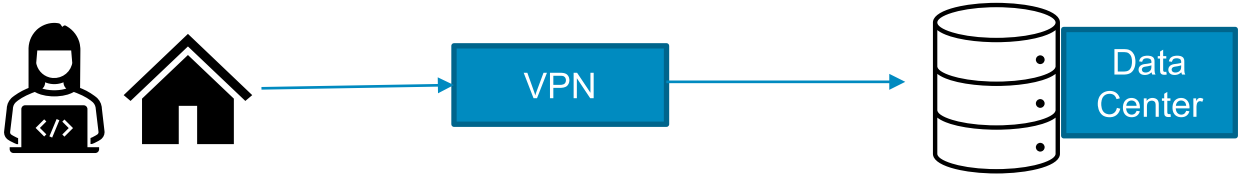
- Remove implicit trust. (*Zero trust* is the associated buzzword.)
- Move security from the network to users, applications, and workloads.

Food for Thought

- The zero trust strategy applies to personnel and physical security. The Department of Defense (DoD) has applied zero trust to these areas for years.

Principles

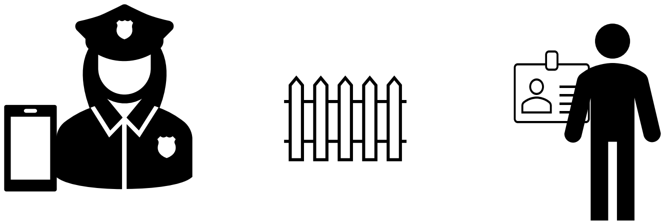
- Ensure all resources are accessed securely, regardless of location.
- Adopt a least privilege strategy and strictly enforce access control.
- Inspect and log traffic necessary to support continuous auditing.
- Ensure all components support application programming interfaces (APIs) for event and data exchange.
- Automate actions across environments and systems driven by context and events.



[Garbis 2021]

Working Definitions

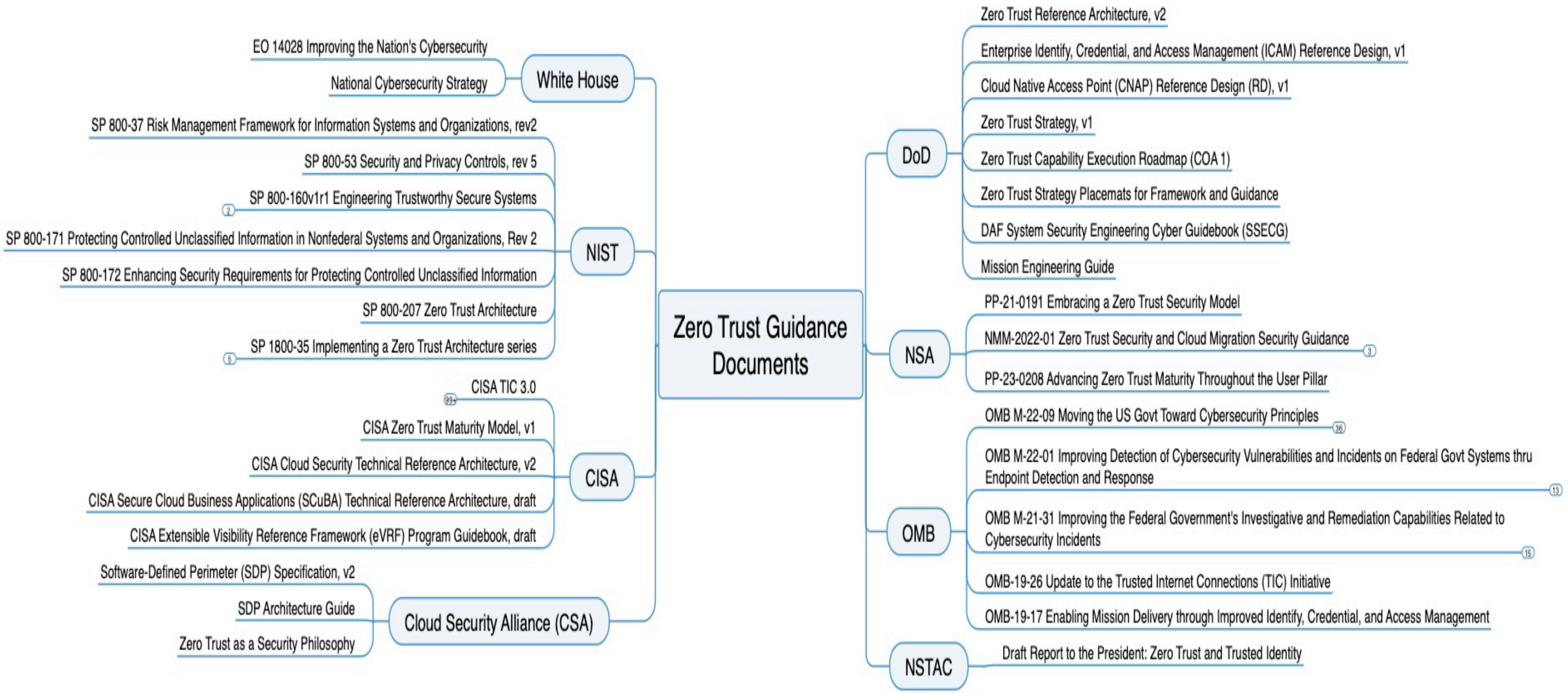
A zero trust system employs an *integrated security solution* that uses *contextual information* from (1) identity, security, and IT infrastructure and (2) risk analytics tools to inform and enable the *dynamic enforcement of security policies uniformly across the enterprise* [Garbis 2021].



Physical security analogy

Zero trust shifts security from an ineffective perimeter-centric model to a *resource- and identity-centric model*. As a result, organizations can continuously adapt access controls to a changing environment, resulting in improved security, reduced risk, simpler and more resilient operations, and increased business agility [Garbis 2021].

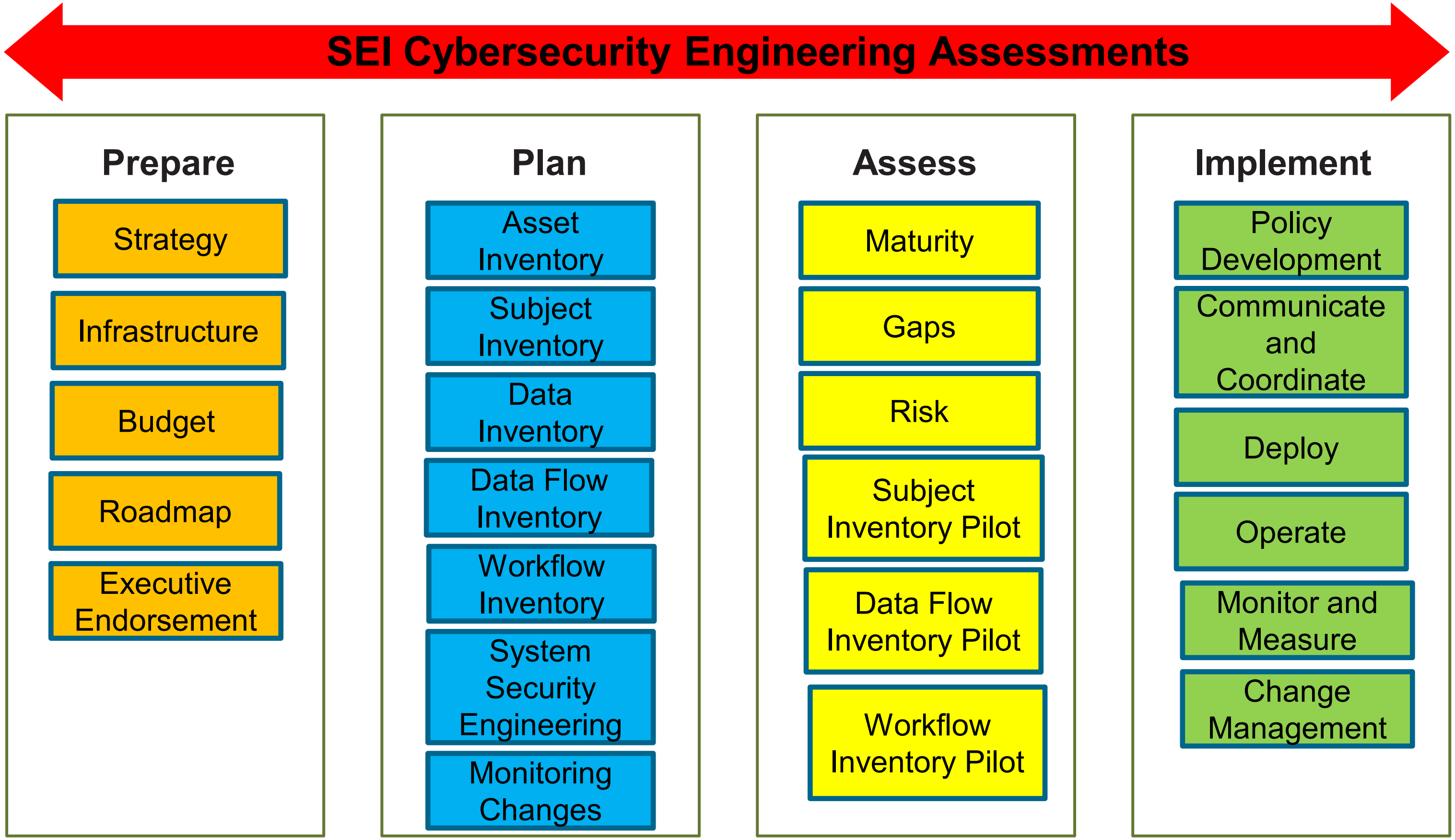
Guidance Documents When Considering a Zero Trust Implementation



- Zero Trust Guidance Documents
  - White House
    - EO 14028 Improving the Nation's Cybersecurity
    - National Cybersecurity Strategy
  - NIST
    - SP 800-37 Risk Management Framework for Information Systems and Organizations, rev2
    - SP 800-53 Security and Privacy Controls, rev 5
    - SP 800-160v1r1 Engineering Trustworthy Secure Systems
    - SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev 2
    - SP 800-172 Enhancing Security Requirements for Protecting Controlled Unclassified Information
    - SP 800-207 Zero Trust Architecture
    - SP 1800-35 Implementing a Zero Trust Architecture series
  - CISA
    - CISA TIC 3.0
    - CISA Zero Trust Maturity Model, v1
    - CISA Cloud Security Technical Reference Architecture, v2
    - CISA Secure Cloud Business Applications (SCuBA) Technical Reference Architecture, draft
    - CISA Extensible Visibility Reference Framework (eVRF) Program Guidebook, draft
  - Cloud Security Alliance (CSA)
    - Software-Defined Perimeter (SDP) Specification, v2
    - SDP Architecture Guide
    - Zero Trust as a Security Philosophy
  - DoD
    - Zero Trust Reference Architecture, v2
    - Enterprise Identify, Credential, and Access Management (ICAM) Reference Design, v1
    - Cloud Native Access Point (CNAP) Reference Design (RD), v1
    - Zero Trust Strategy, v1
    - Zero Trust Capability Execution Roadmap (COA 1)
    - Zero Trust Strategy Placemats for Framework and Guidance
    - DAF System Security Engineering Cyber Guidebook (SSECG)
    - Mission Engineering Guide
  - NSA
    - PP-21-0191 Embracing a Zero Trust Security Model
    - NMM-2022-01 Zero Trust Security and Cloud Migration Security Guidance
    - PP-23-0208 Advancing Zero Trust Maturity Throughout the User Pillar
  - OMB
    - OMB M-22-09 Moving the US Govt Toward Cybersecurity Principles
    - OMB M-22-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Govt Systems thru Endpoint Detection and Response
    - OMB M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
    - OMB-19-26 Update to the Trusted Internet Connections (TIC) Initiative
    - OMB-19-17 Enabling Mission Delivery through Improved Identify, Credential, and Access Management
  - NSTAC
    - Draft Report to the President: Zero Trust and Trusted Identity

DISTRIBUTION STATEMENT A This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Software Engineering Institute (SEI) Zero Trust Journey



SEI Cybersecurity Engineering Assessments

Prepare

- Strategy
- Infrastructure
- Budget
- Roadmap
- Executive Endorsement

Plan

- Asset Inventory
- Subject Inventory
- Data Inventory
- Data Flow Inventory
- Workflow Inventory
- System Security Engineering
- Monitoring Changes

Assess

- Maturity
- Gaps
- Risk
- Subject Inventory Pilot
- Data Flow Inventory Pilot
- Workflow Inventory Pilot

Implement

- Policy Development
- Communicate and Coordinate
- Deploy
- Operate
- Monitor and Measure
- Change Management

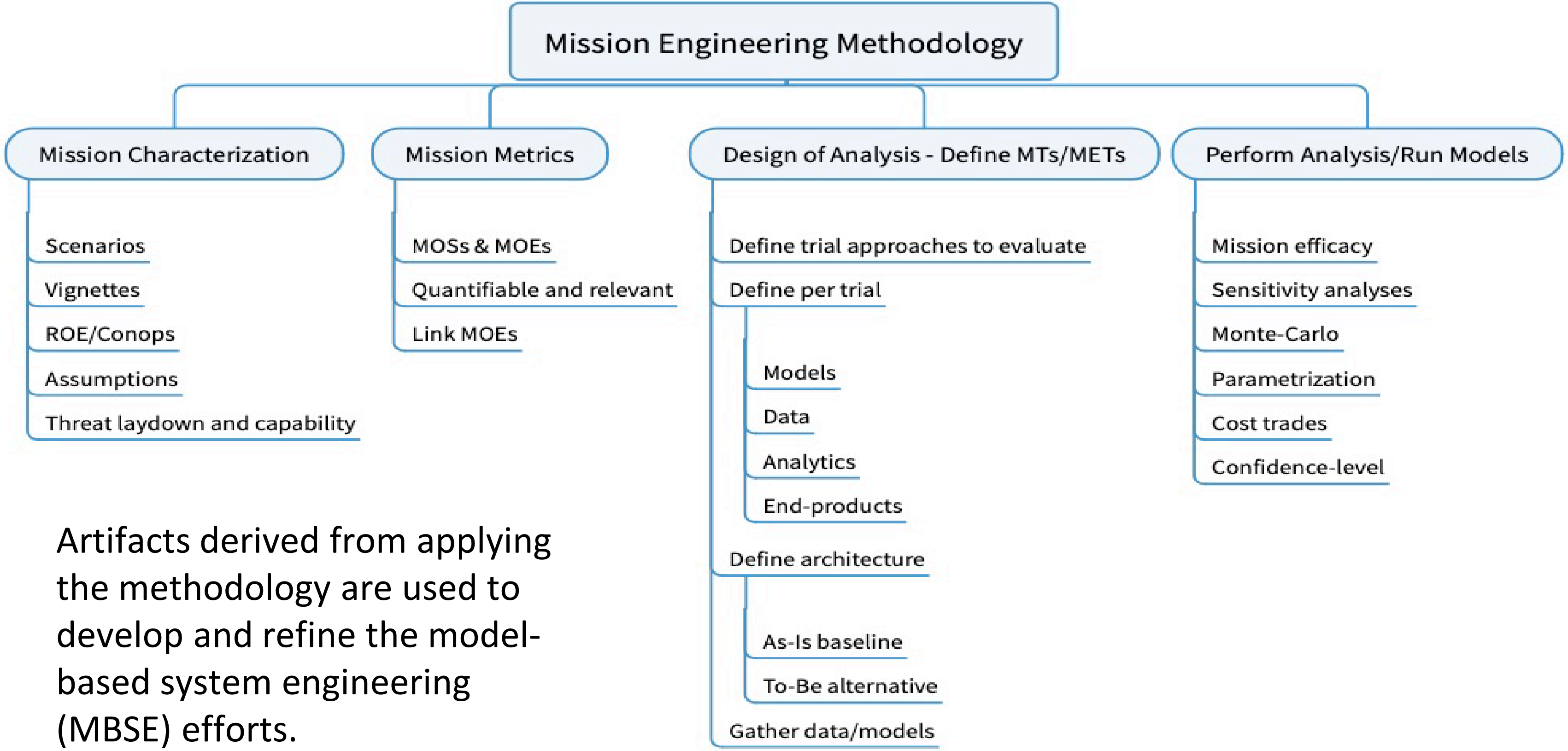
What’s Mission Engineering and its Objectives?

Mission Engineering (ME) is the planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.

Five Objectives

1. Enable mission-focused, threat-informed analysis.
2. Identify and address mission gaps.
3. Develop Government Reference Architectures (GRA) to guide development and prototypes.
4. Inform stakeholders how the architecture is envisioned to address/support the missions.
5. Generate and capture scenarios, assumptions, constraints, system attributes, and data for use during analysis.

Focused View of ME Methodology

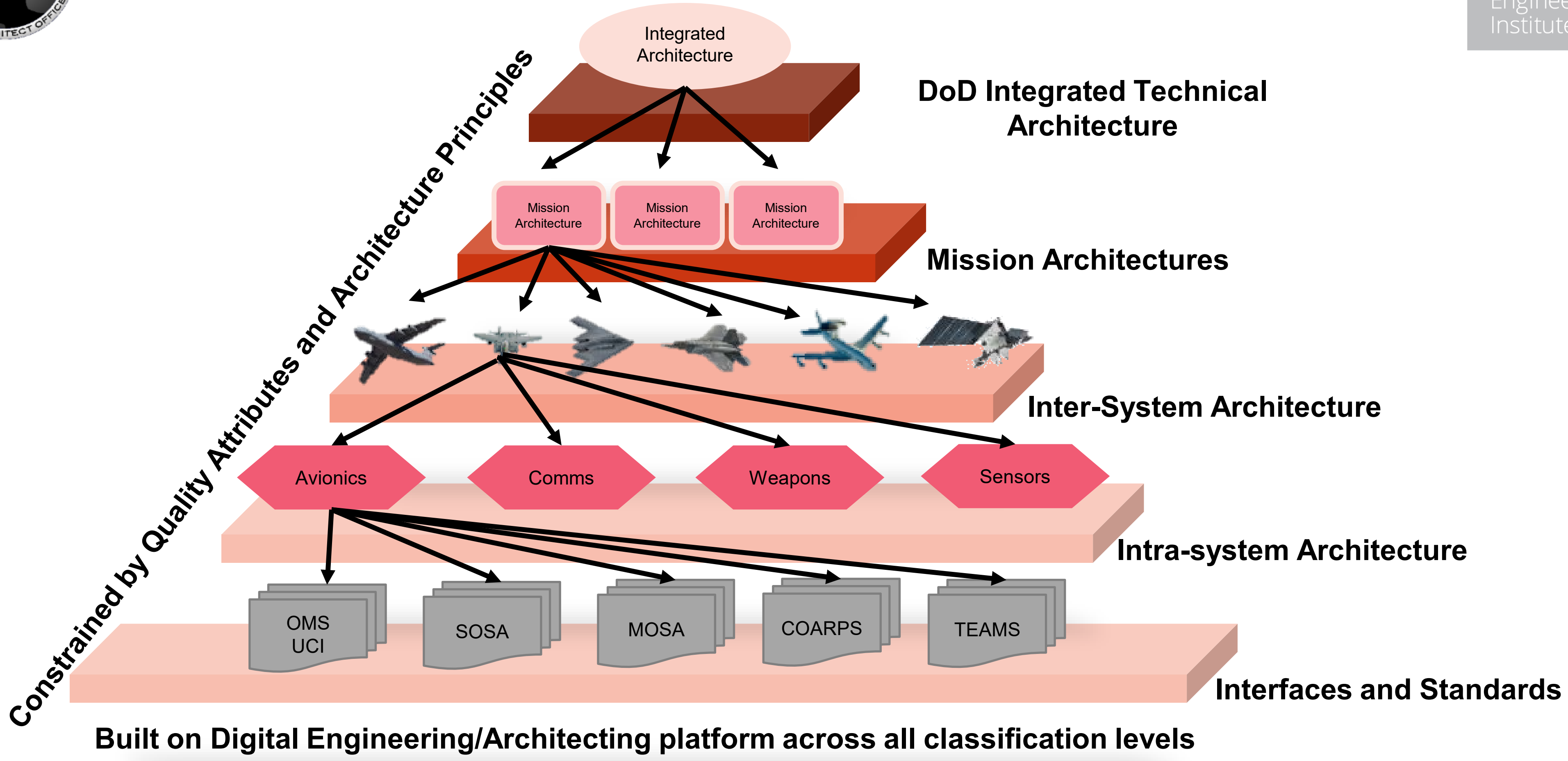


Mission Engineering Methodology

- Mission Characterization
  - Scenarios
  - Vignettes
  - ROE/Conops
  - Assumptions
  - Threat laydown and capability
- Mission Metrics
  - MOSs & MOEs
  - Quantifiable and relevant
  - Link MOEs
- Design of Analysis - Define MTs/METs
  - Define trial approaches to evaluate
  - Define per trial
    - Models
    - Data
    - Analytics
    - End-products
  - Define architecture
    - As-Is baseline
    - To-Be alternative
  - Gather data/models
- Perform Analysis/Run Models
  - Mission efficacy
  - Sensitivity analyses
  - Monte-Carlo
  - Parametrization
  - Cost trades
  - Confidence-level

Artifacts derived from applying the methodology are used to develop and refine the model-based system engineering (MBSE) efforts.

DoD Architecture Layers


Integrated Architecture
DoD Integrated Technical Architecture
Mission Architecture
Mission Architecture
Mission Architecture
Mission Architectures
Inter-System Architecture
Avionics
Comms
Weapons
Sensors
Intra-system Architecture
OMS UCI
SOSA
MOSA
COARPS
TEAMS
Interfaces and Standards
Constrained by Quality Attributes and Architecture Principles
Built on Digital Engineering/Architecting platform across all classification levels

Threats to Zero Trust Implementations

1. Subversion of the zero trust architecture (ZTA) decision process
2. Denial-of-service or network disruption
3. Stolen credentials/insider threat
4. Visibility of the network (i.e., awareness of the components and data within a network)
5. Storage of system and network information
6. Reliance on proprietary data formats or solutions
7. Use of NPEs in ZTA administration
8. Attack, which is directed at the APIs, that alters the data stream to permit access through tampered telemetry during conditions/entitlement checks

[Rose 2020]

Threat Mapping –1

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Subversion of the ZTA Decision Process	Policy Engine Policy Administrator	Configuration Management Monitoring Detection
Denial-of-Service or Network Disruption	Policy Engine Policy Administrator Policy Enforcement Point	Resilience
Stolen Credentials/Insider Threat	ID Management Data Access Policy	Architecture Contextual Trust Algorithm
Visibility on the Network	Activity Logs SIEM	Network Traffic Inspection Network Traffic Logging Metadata Machine Learning

[Sanders 2021]

Threat Mapping –2

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Storage of System and Network Information	Policy Engine Policy Administrator Activity Logs CDM Systems Industry Compliance Data Access Policy PKI ID Management SIEM Information	Restrictive Data Access Policies
Reliance on Proprietary Data Formats and Solutions	Policy Engine Policy Administrator Policy Enforcement Point	Service Provider Evaluation Vendor Security Controls Enterprise Switching Costs Supply Chain Risk Management Performance/Stability

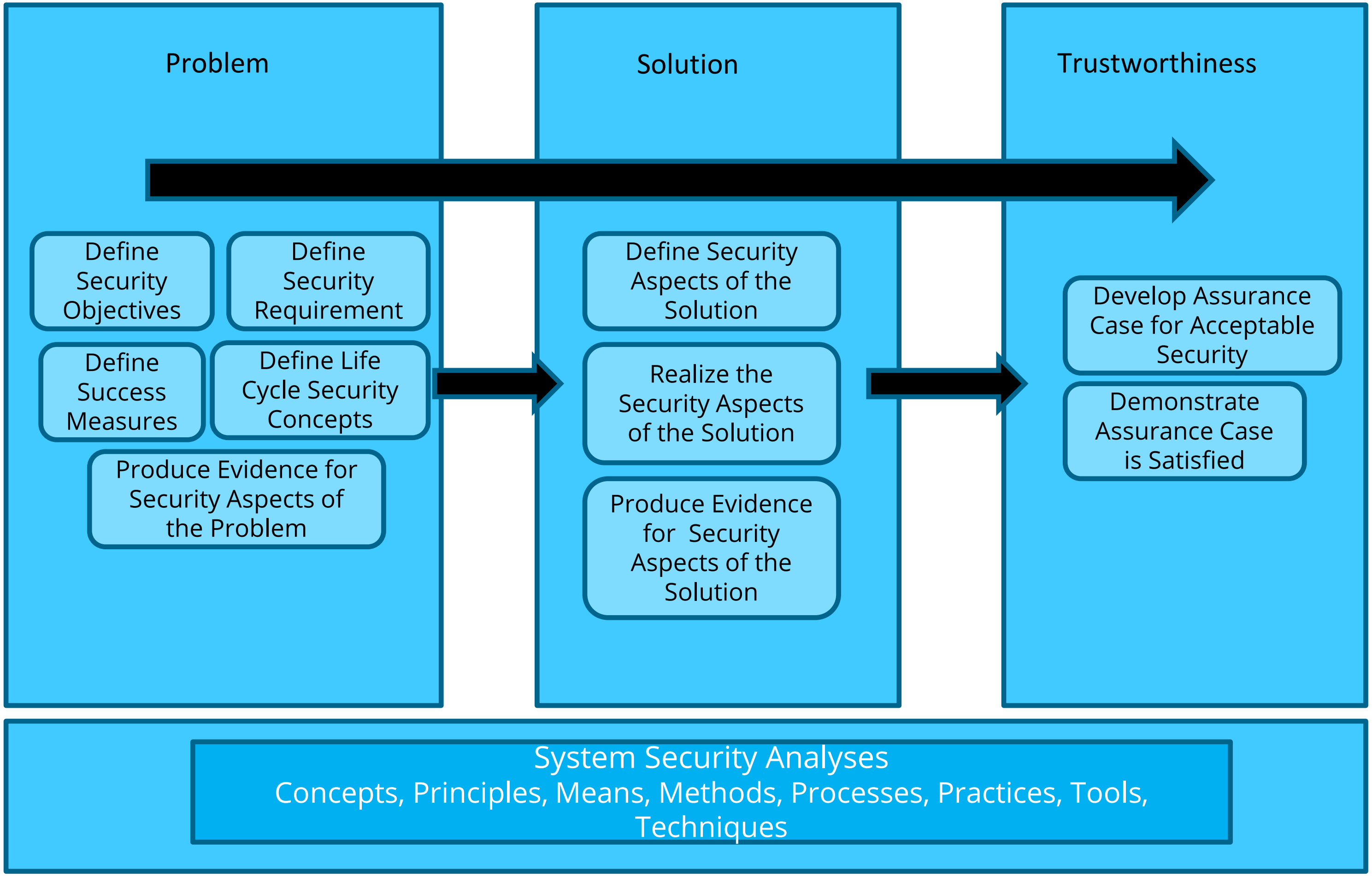
[Sanders 2021]

Threat Mapping –3

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigations
Use of Non-Person Entities (NPEs) in ZTA Administration	Policy Engine Policy Administrator	Regular Retuning Analysis
API Attacks	Policy Engine Policy Administrator CDM System ID Management SIEM Information	Encrypt Requests and Responses Validate the Data Assess API Risks

[Sanders 2021]

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems



Problem

Define Security Objectives

Define Security Requirement

Define Success Measures

Define Life Cycle Security Concepts

Produce Evidence for Security Aspects of the Problem

Solution

Define Security Aspects of the Solution

Realize the Security Aspects of the Solution

Produce Evidence for Security Aspects of the Solution

Trustworthiness

Develop Assurance Case for Acceptable Security

Demonstrate Assurance Case is Satisfied

System Security Analyses
Concepts, Principles, Means, Methods, Processes, Practices, Tools, Techniques

Figure 10

DAF System Security Engineering Cyber Guidebook (SSECG) - Cyber Survivability Attributes

CSA	Pillar	Cyber Survivability Attribute (CSA)
CSA-01	Prevent	Control Access
CSA-02	Prevent	Reduce System’s Cyber Detectability
CSA-03	Prevent	Secure Transmissions and Communications
CSA-04	Prevent	Protect System’s Information from Exploitation
CSA-05	Prevent	Partition and Ensure Critical Functions at Mission Completion Performance Levels
CSA-06	Prevent	Minimize and Harden Cyber Attack Surfaces
CSA-07	Mitigate	Baseline & Monitor Systems, & Detect Anomalies
CSA-08	Mitigate	Manage System Performance if Degraded by Cyber Events
CSA-09	Recover	Recover System Capabilities; Actively manage System’s Configuration to Counter Vulnerabilities at Tactically Relevant Speeds
CSA-10	Adapt	Achieve & Manage System’s an operationally relevant Cyber Survivability Risk Posture (CSRP) and to counter risk changes in adversary’s capabilities

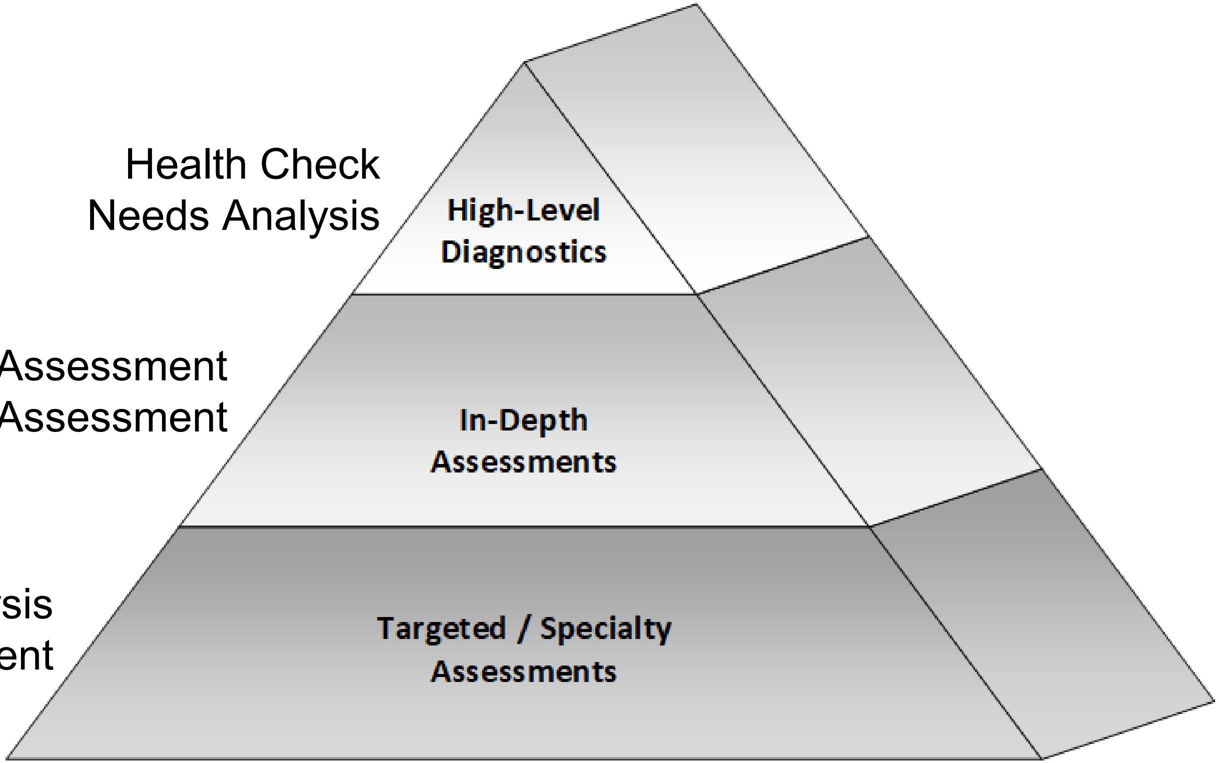
System Survivability Key Performance Parameter

Types of Assessments and Analysis

Health Check
Needs Analysis

Architecture Risk Assessment
Process Assessment

Code Analysis
Vulnerability Assessment

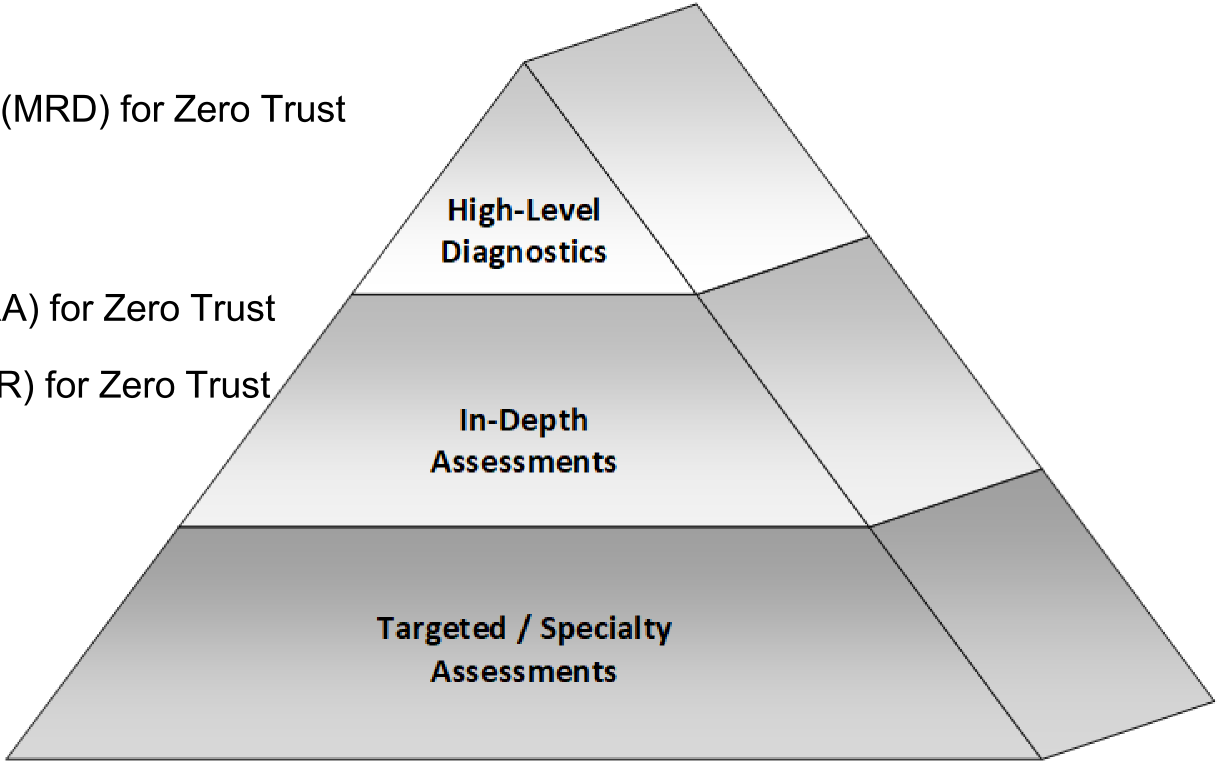


Proposed Zero Trust Assessments

Mission Risk Diagnostic (MRD) for Zero Trust

Security Engineering Risk Analysis (SERA) for Zero Trust

Cybersecurity Engineering Review (CSER) for Zero Trust



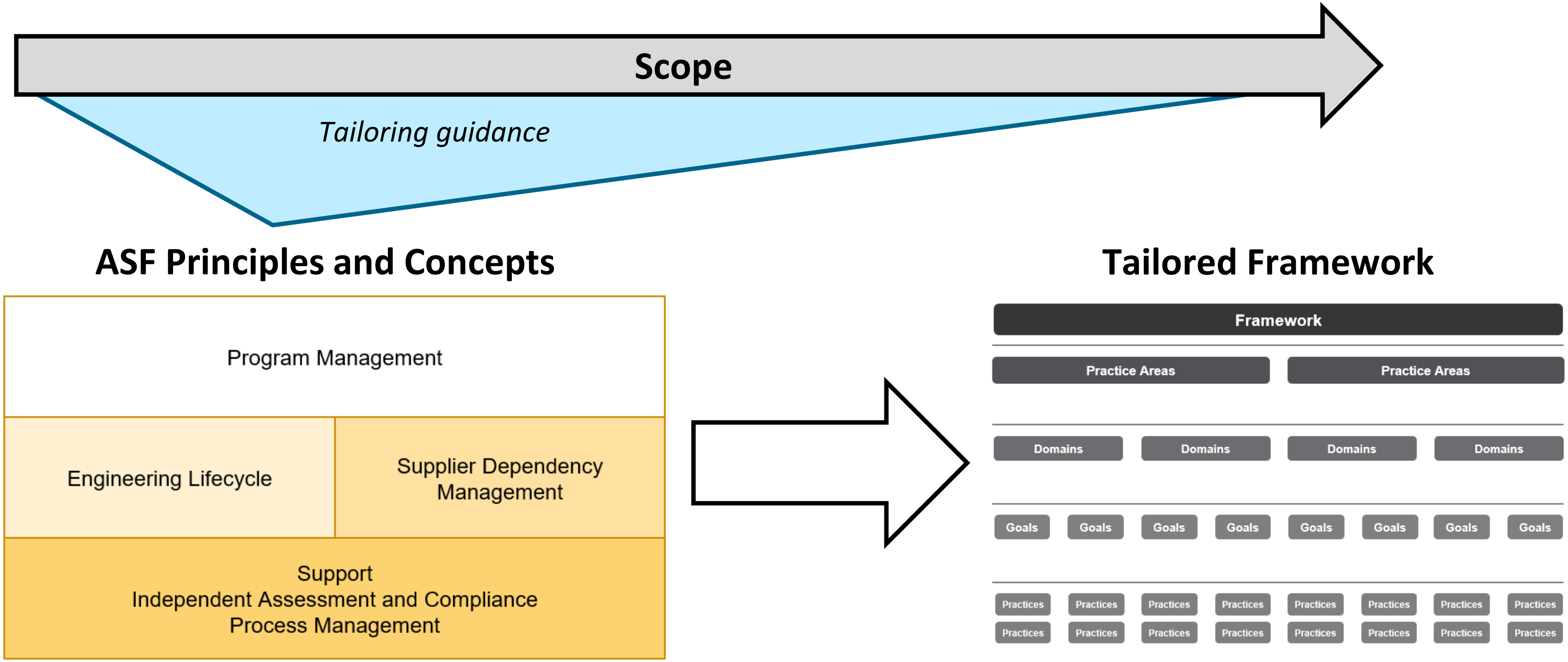
What is the Acquisition Security Framework (ASF)?

The ASF is a collection of leading practices for building and operating secure and resilient software-reliant systems.

The ASF is designed to proactively enable system security and resilience engineering across the lifecycle and supply chain.

- Provides a roadmap for building security and resilience into a system rather than “bolting it on” after deployment
- Facilitates efficient and predictable systems environments and more manageable delivery and risk outcomes

Creating Tailored Risk Frameworks



Scope

Tailoring guidance

ASF Principles and Concepts

Program Management

Engineering Lifecycle

Supplier Dependency Management

Support
Independent Assessment and Compliance
Process Management

Tailored Framework

Framework

Practice Areas | Practice Areas

Domains | Domains | Domains | Domains

Goals | Goals | Goals | Goals | Goals | Goals | Goals | Goals

Practices | Practices | Practices | Practices | Practices | Practices | Practices | Practices

Practices | Practices | Practices | Practices | Practices | Practices | Practices | Practices

Envisioned Zero Trust Framework: Guidance

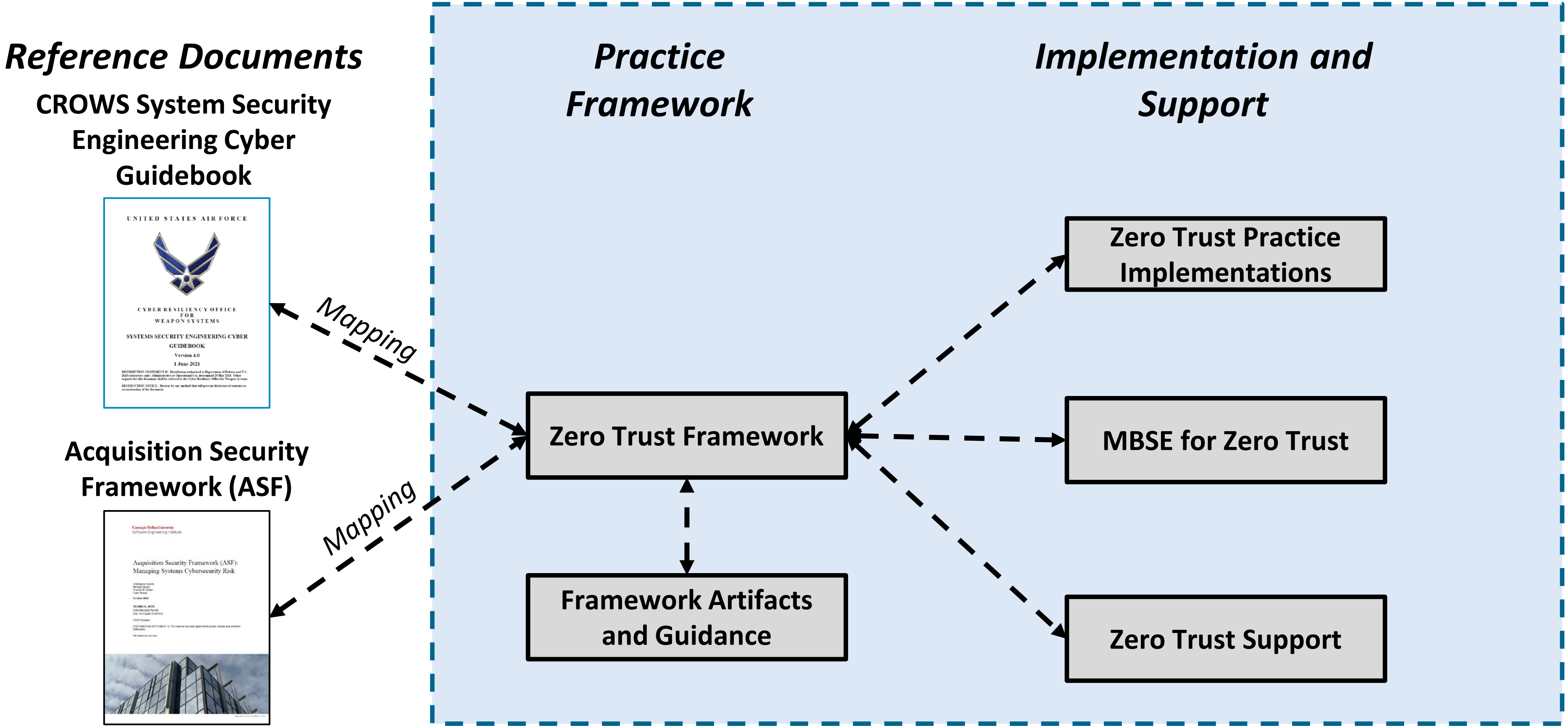
Goal-Level Guidance

- Description and Context
- Competencies

Practice-Level Guidance

- Question Intent
- Typical Work Products
- Criteria for “Yes” Response
- Criteria for “Incomplete” Response

Notional ZT Framework Application


Reference Documents
CROWS System Security Engineering Cyber Guidebook
Acquisition Security Framework (ASF)
Mapping
Mapping
Practice Framework
Implementation and Support
Zero Trust Framework
Framework Artifacts and Guidance
Zero Trust Practice Implementations
MBSE for Zero Trust
Zero Trust Support

UNITED STATES AIR FORCE

CYBER RESILIENCY OFFICE
FOR
WEAPON SYSTEMS

SYSTEMS SECURITY ENGINEERING CYBER
GUIDEBOOK

Version 4.0

1 June 2021

DISTRIBUTION STATEMENT D: Distribution authorized to Department of Defense and U.S. DoD contractors only: Administrative or Operational Use, determined 29 Mar 2018. Other requests for this document shall be referred to the Cyber Resiliency Office for Weapon Systems.

DESTRUCTION NOTICE - Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Carnegie Mellon University
Software Engineering Institute

Acquisition Security Framework (ASF):
Managing Systems Cybersecurity Risk

Christopher Alberts
Michael Bandor
Charles M. Wallen
Carol Woody

October 2022

TECHNICAL NOTE
CMU/SEI-2022-TN-003
DOI: 10.1184/R1/21357027

CERT Division

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

http://www.sei.cmu.edu

Summary

Developing context using mission engineering approach enables security architectures to reason about zero trust strategy, design, and possible implementations for weapon systems, as well as enterprises.

Set of zero trust assessments need to be developed to support the life cycle of weapon system/enterprise.

Need to use an approach like ASF to build in security and resilience into weapon systems/enterprise in support of efforts like CROWS SSECG to provide the artifacts to enable zero trust assessments

Backup

Mission Risk Diagnostic (MRD)

Artist's Concept

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

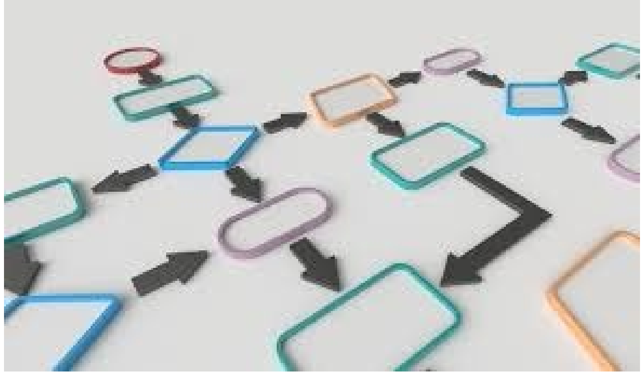
Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Cybersecurity Engineering Review (CSER)



What

- Evaluates an acquisition program's security practices for conformance to accepted CSE practices

Why

- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Assessment Information

Mission Risk Diagnostic (MRD) Method Description

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

Security Engineering Risk Analysis (SERA) Collection

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485410

ASF Information

Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889215

Acquisition Security Framework (ASF): An Acquisition and Supplier Perspective on Managing Software-Intensive Systems' Cybersecurity Risk

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887698

Acquisition Security Framework (ASF)

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=889453

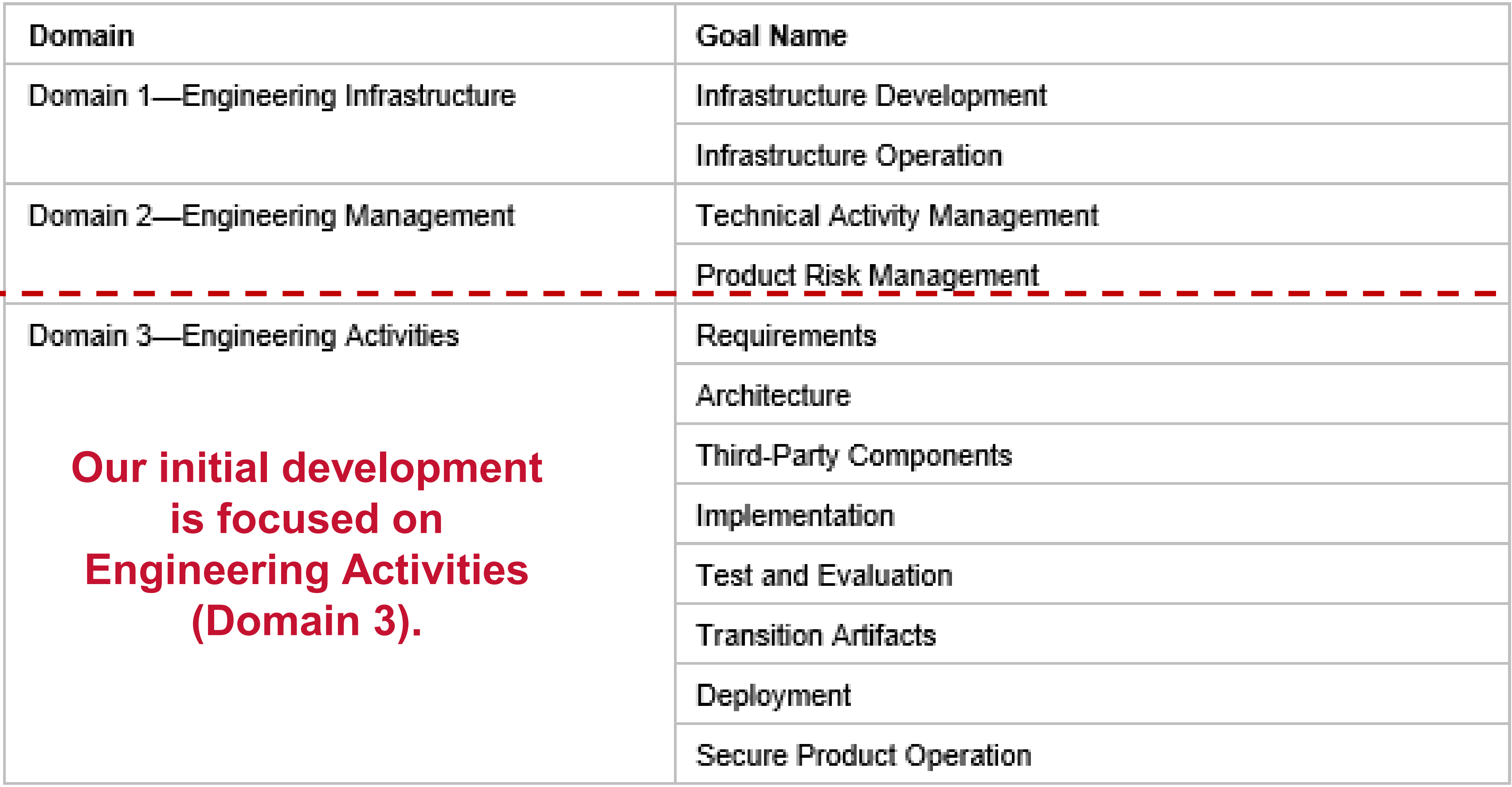
Addressing Supply Chain Risk and Resilience for Software-Reliant Systems

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974293

Asking the Right Questions to Coordinate Security in the Supply Chain

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=974136

ASF Engineering Lifecycle: Domains and Goals



Domain	Goal Name
Domain 1—Engineering Infrastructure	Infrastructure Development
	Infrastructure Operation
Domain 2—Engineering Management	Technical Activity Management
	Product Risk Management
Domain 3—Engineering Activities	Requirements
	Architecture
	Third-Party Components
	Implementation
	Test and Evaluation
	Transition Artifacts
	Deployment
	Secure Product Operation

Our initial development is focused on Engineering Activities (Domain 3).