Cybersecurity in the Systems Engineering Processes:
A High Level SE Process Orientation

Defense Acquisition University


Certification Training


Knowledge Sharing


Continuous Learning


Mission Assistance

Greg Butler, Ph.D.
CISSP ISSEP
gregory.butler@dau.mil

LTC Stephani Hunsinger
stephani.hunsinger@dau.mil

Kim Kendall
kim.kendall@dau.mil

Overview

Purpose:

The purpose of this presentation is to give the participant a high-level overview of how cybersecurity fits into the systems engineering technical and technical management processes.

Topics:

- Define System Security Engineering
- System Security Engineer (SSE) Role and Expectations
- SSE in the SE Technical Processes
  & SE Technical Management Processes
- DAU Training and Other Support Options
- References

System Security Engineering

An element of system engineering (SE) that applies scientific and engineering principles to

- Identify security vulnerabilities
- Minimize or contain risks associated with these vulnerabilities.

DoD Instruction 5200.44 Nov 12

MIL-HDBK-1785 Aug 95

Characteristics and Expectations of a System Security Engineer

An optimal Systems Security Engineer has

- Depth and breadth in system engineering and security
- Specific knowledge of technology and the domain

refined by the level of assurance to which the system is being engineered.

Expertise and experience in:

- Systems engineering processes and methodologies
- Protection needs assessment
- Requirements elicitation
- Security architecture
- Threat assessment
- Computer and communications security
- Networking
- Security technologies
- Hardware and software development
- Test and evaluation
- Vulnerability and Security Specific Assessments
- Hardware Assurance (HwA)
- Software Assurance(SwA)
- Supply Chain Risk Management (SCRM)

System Security Engineering – An Organizational Mindset

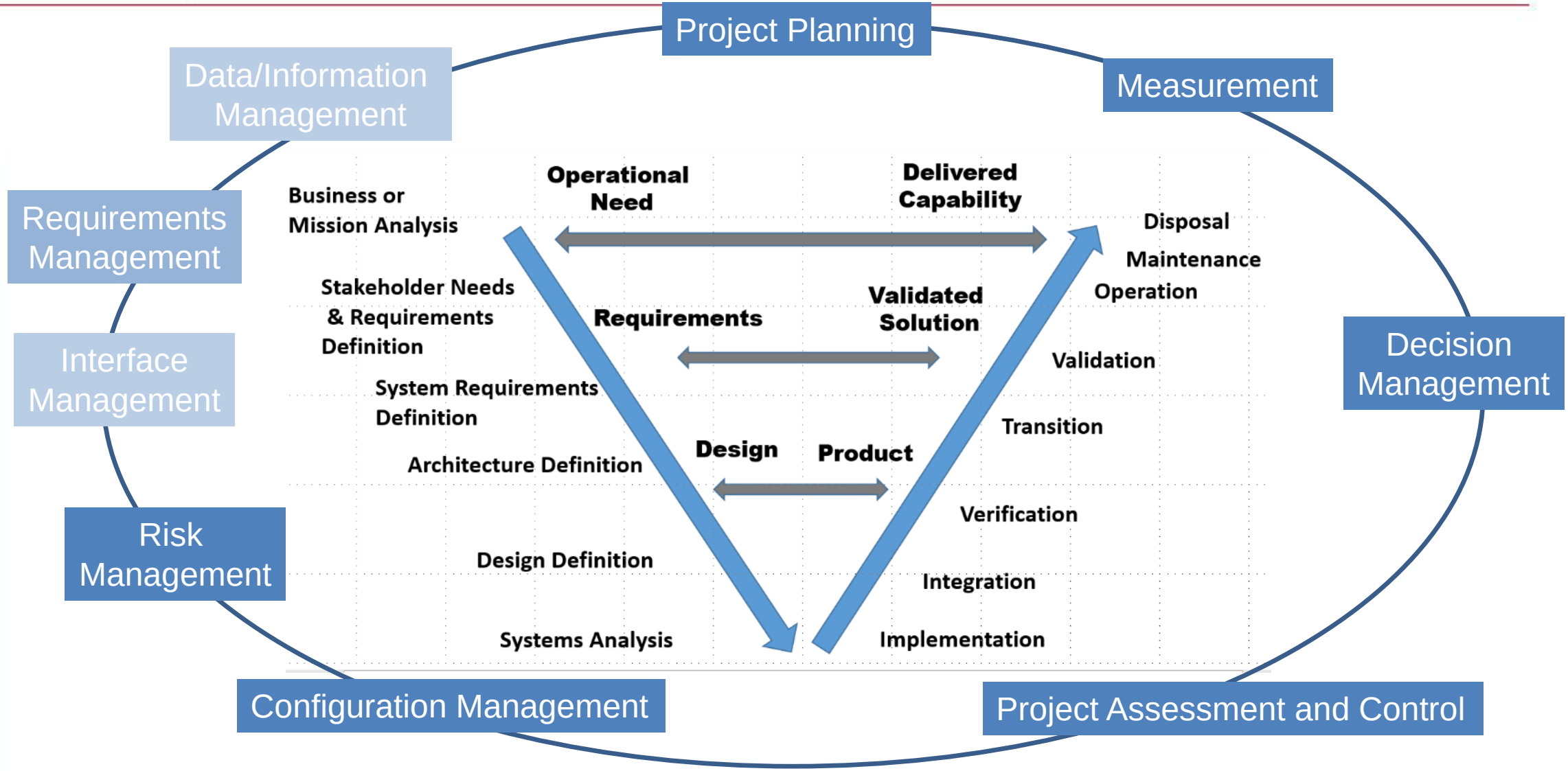
In order to provide robust, secure, and resilient systems that can perform the mission in the operational environment

- Security is a team sport– everyone (users, maintainers, logistics, PM, engineering..) needs to understand the need for secure, robust systems and their role in making it happen
- SE has key role- systems engineering must ensure that security and resilience needs are identified, evaluated, and implemented across
  - All SE Technical and Technical Management processes
  - All acquisition phases

Institutionalized Operationalized

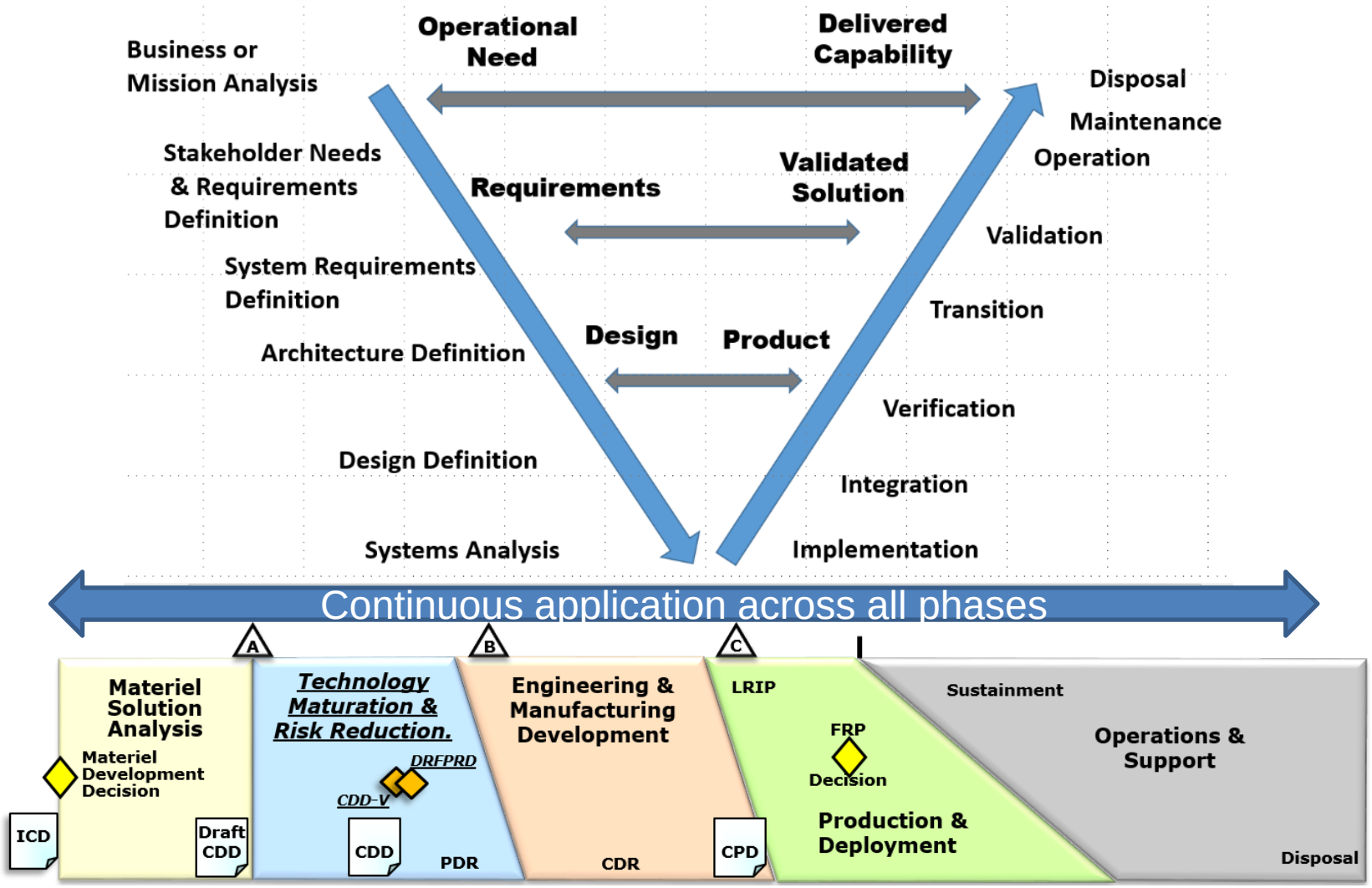
SE Processes

Technical Processes and Technical Management Processes



SE Processes
Across the Lifecycle

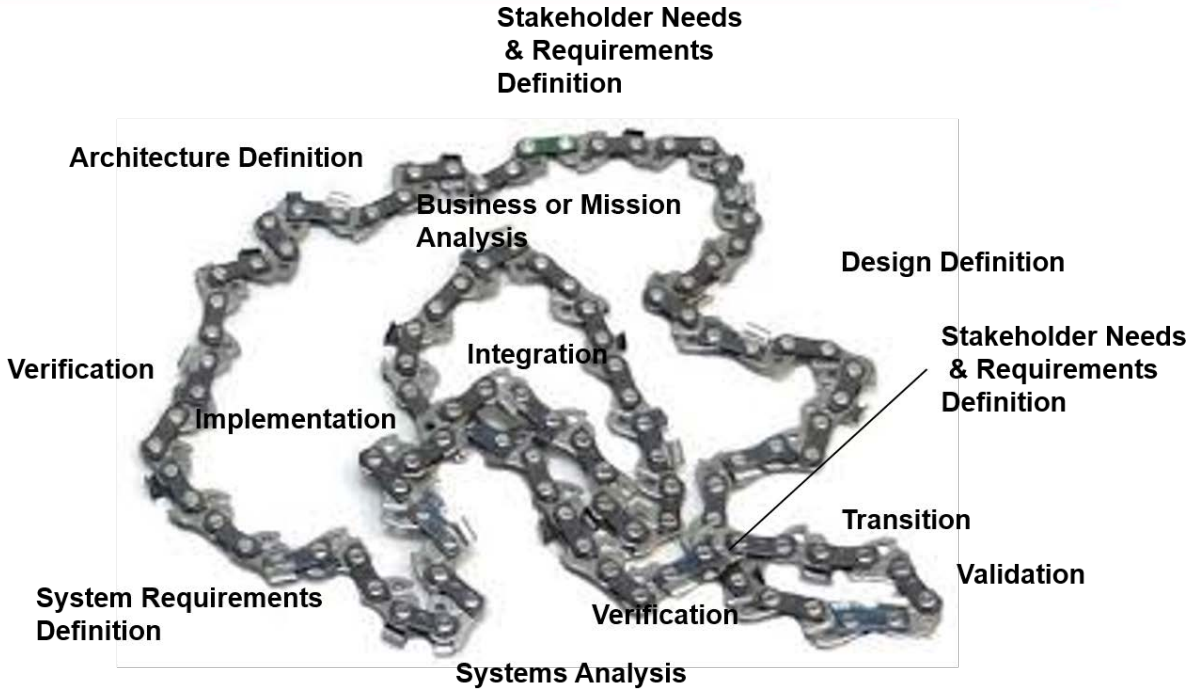
Systems engineering processes are tailored and applied at *every* stage of the acquisition lifecycle as appropriate

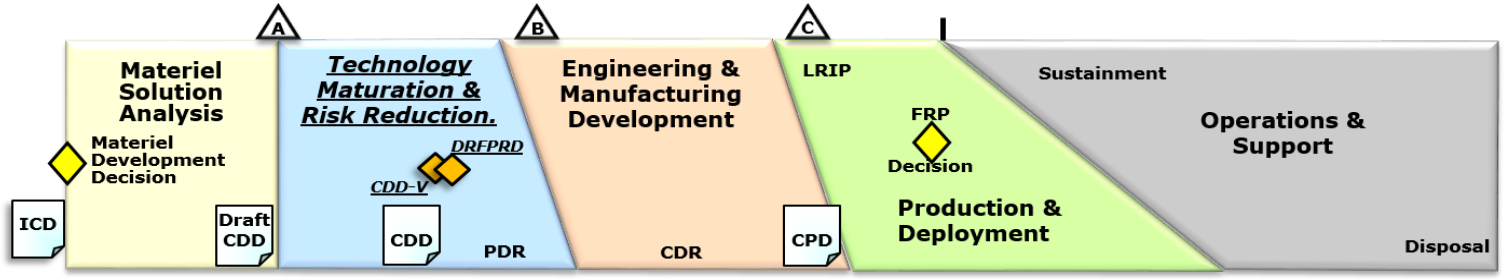


SE Processes
Not a sequence of steps

The systems engineering technical and technical management processes are not sequential

They may be
- Iterative
- Recursive
- Concurrent



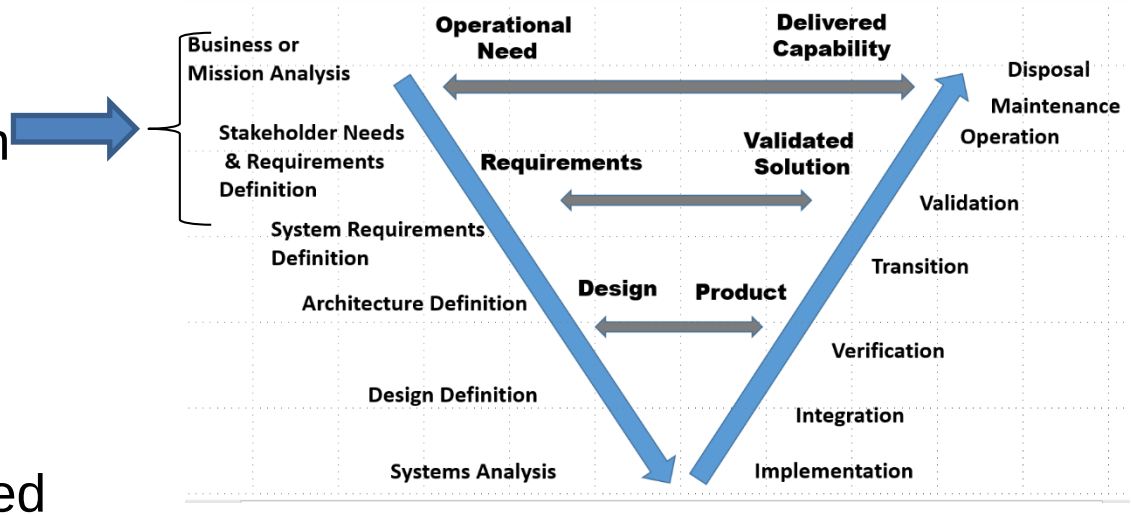


Technical Processes

Business or Mission Analysis/Stakeholder Needs & Requirements Definition

Purpose- General:

- Define the problem or opportunity, characterize the solution space
- Define the requirements that will provide a system that meets user/stakeholder needs in the intended operational environment
- Identify critical performance measures



Purpose- Cybersecurity

- Security aspects of the problem space defined
- Candidate and preferred solution classes are analyzed and selected explicitly to account for security objectives, concerns, and constraints
- User requirements captured and explicitly agreed upon

Technical Processes

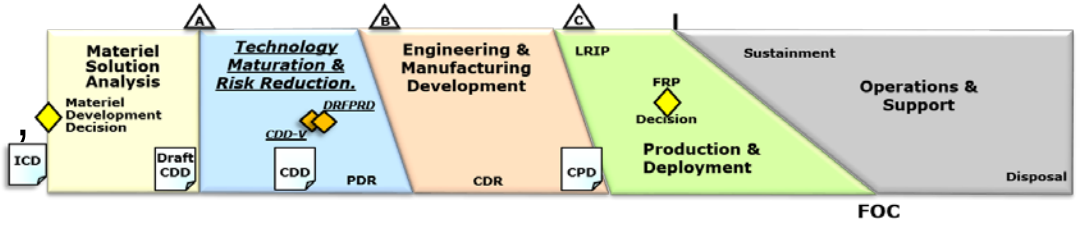
Business or Mission Analysis/Stakeholder Needs & Requirements Definition

Representative Activities

- Assess cybersecurity risk in AoA
- Define the operational environment
- Identify cybersecurity capability requirements (JCIDS)
- Specify what is critical to mission success
- Identify statutory and regulatory requirements

Highlights:

- Threat
- Survivability KPP
- Criticality Analysis and Determination
- Interfaces and dependencies
  - user interactions
  - Enabling systems
  - Supporting systems
- CONOPS
- FMA- Operational scenarios
- Lifecycle approach

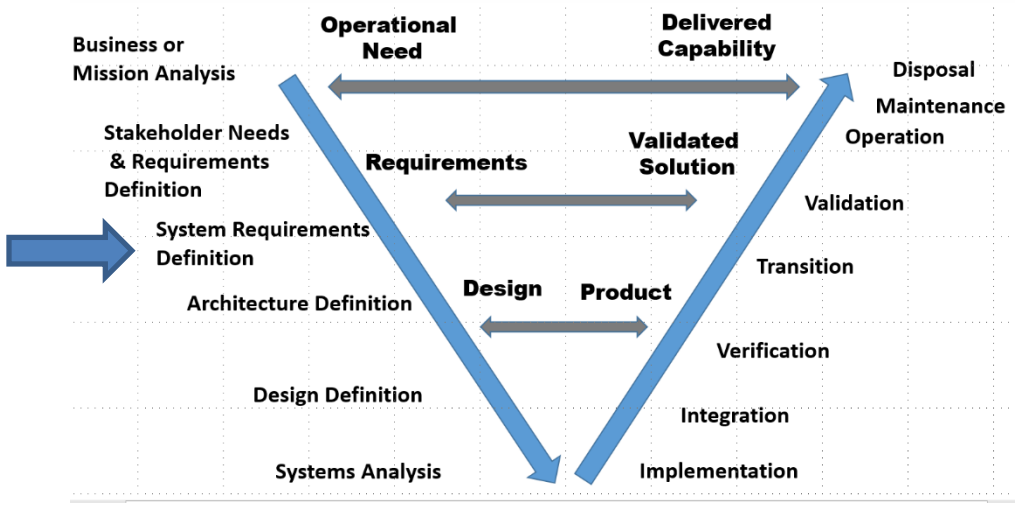


Technical Processes
System Requirements Definition

Purpose- General: Transform the user/stakeholder oriented view of desired capabilities into a technical view of a solution that meets user needs.

Purpose- Cybersecurity: System security description including

- Boundary: All interactions and behaviors with systems that are part of mission environment, enabling systems, the environment, and the level of assurance associated with each
- Security functions: All system states, modes, and conditions focusing on delivering capability and the ability of the system to execute and maintain a secure state
- Constraints imposed on the design or functionality of a system by security needs and those effecting the security of a system



Technical Processes
System Requirements Definition

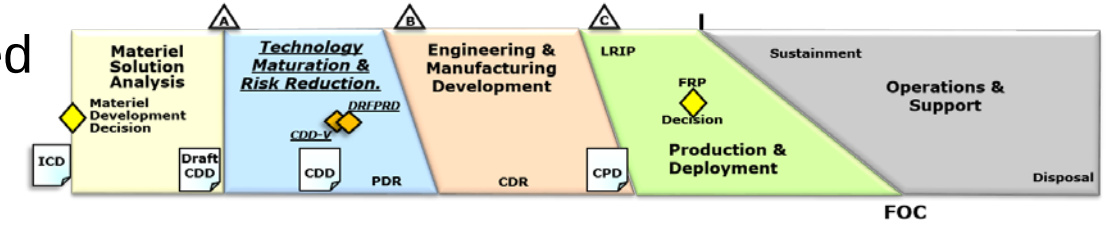
Representative Activities

SE/SSE - working with the ISSM, user, and AO

- Identify security related requirements, perform trades and define the trade space available. Some sources are:
  - Risk mgmt. (RMF)
  - Compliance (HIPPA, PII)
  - Certifications
  - Threat and the operational environment
  - JCIDS
  - Functional mission analysis, CONOPS, top level architecture-I/Fs (OV-1) and actors
  - Legacy and related systems
- Define evaluation criteria
- Tag all requirements that are security related

Highlights:

- Threat
- RMF Controls
- Mission Threads
- Specifications, IRS, SRS, ICDs, etc.
- Trades
- SRR
- SFR

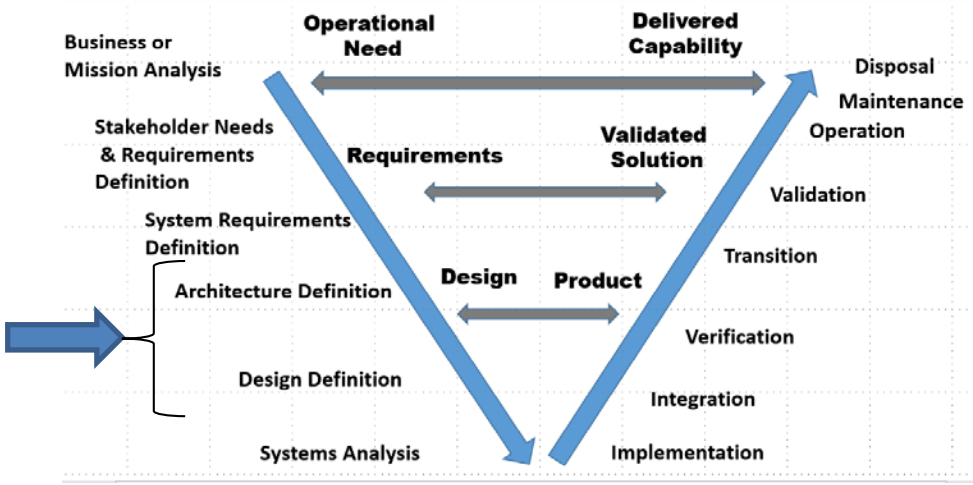


Technical Processes
Architecture and Design Definition

Architecture is:

- …the conceptual model that defines the structure, behavior, and more views of a system
- … a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.
- … description of the structure of a system and the relationship between its element (including external dependencies and I/Fs)
- Multiple viewpoints, logical and physical, at various levels of abstraction

Design is: Allocating the required functionality to the system elements and elaborating the requirements in sufficient detail to allow for implementation.



SECURITY PRINCIPLES

Security Architecture and Design	
Clear Abstraction	Hierarchical Trust
Least Common Mechanism	Inverse Modification Threshold
Modularity and Layering	Hierarchical Protection
Partially Ordered Dependencies	Minimized Security Elements
Efficiently Mediated Access	Least Privilege
Minimized Sharing	Predicate Permission
Reduced Complexity	Self Reliant Trustworthiness
Secure Evolvability	Secure Distributed Composition
Trusted Components	Trusted Communication Channels
Security Capability and Intrinsic Behaviors	
Continuous Protection	Secure Failure and Recovery
Secure Metadata Management	Economic Security
Self-Analysis	Performance Security
Accountability and Traceability	Human Factored Security
Secure Defaults	Acceptable Security
Life Cycle Security	
Repeatable and Documented Procedures	Secure System Modification
Procedural Rigor	Sufficient Documentation

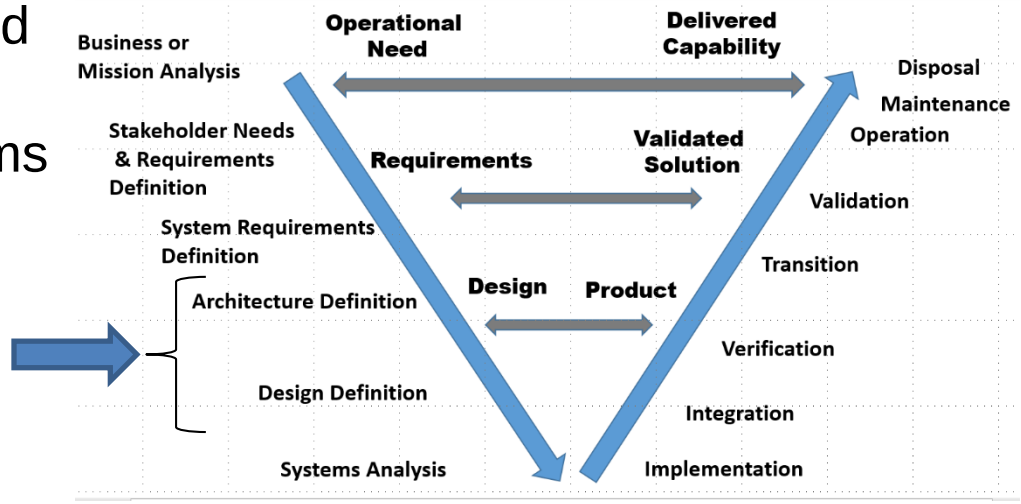
Detailed descriptions are available at Appendix F, NIST SP 800-160 (2nd draft)

Technical Processes
Architecture and Design Definition

Cybersecurity

- **Architecture**: System architecture that describes how system security and resilience is addressed
  - Across system boundaries
  - Between system components and subsystems
  - In the allocation of privilege and access
  - Including actors and processes

  Considers vulnerabilities and susceptibility to disruption or compromise and approaches to minimizing the risk



Design:

- Specify the appropriate application of security technologies
- Accomplishing the trades necessary to balance security, cost, and functionality
- Allocate security and resiliency responsibilities/functionality to subsystems, hardware and software components

Technical Processes
Architecture and Design Definition

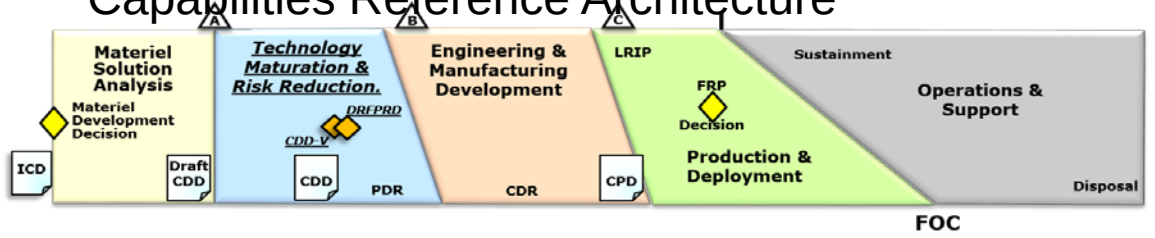
Representative Activities

- Identify key drivers: statutory, regulatory, policy, standards, etc.
- Identify other constraints
- Viewpoints, views, models created
  - Boundaries
  - Interfaces (physical, logical, data, shared/inherited controls)
  - Components, subsystems,
  - Roles, privileges and access, procedures, etc.
- Capabilities allocated to subsystems, assemblies, components, users…
- Define evaluation criteria
- Security related are tagged and traceable

Highlights:

- Abuse-Misuse Cases
- Government reference architecture
- Contractor system architecture
- Iterations between requirements, architecture and design
- PDR
- CDR

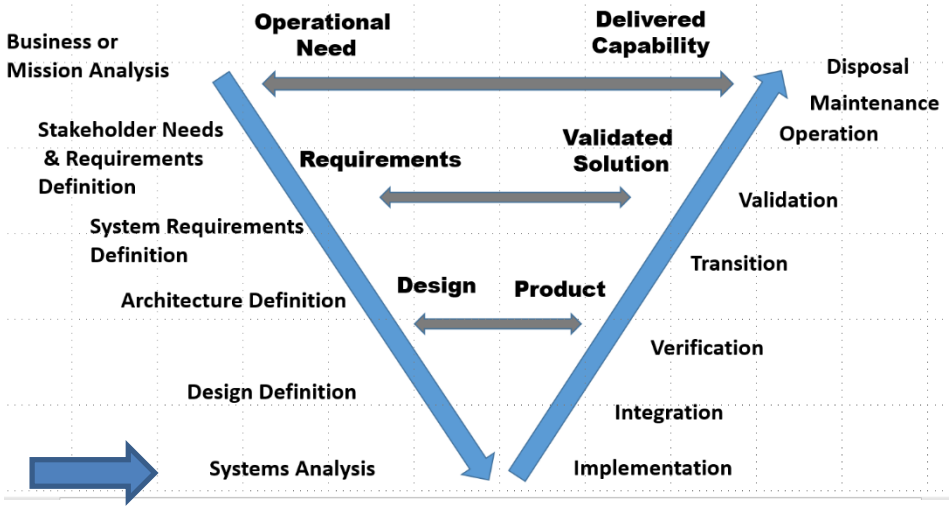
Examples: DoD Information Enterprise Architecture, DOE IT security architecture, DoD Unified Capabilities Reference Architecture



Technical Processes
Systems Analysis

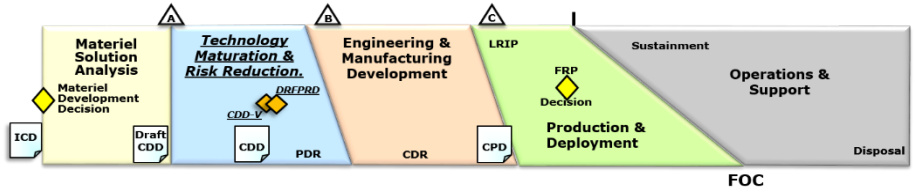
Purpose- General

- Analyze proposed requirements, solutions, decision across all processes with the rigor commensurate with the criticality of the object under analysis.
- Document the analysis, trades and decisions, and rationale
- Make all assumptions explicit, validate each, and document them



Cybersecurity Highlights

- Security Engineering and RMF trades
- Resiliency trades
- HwA and SwA
- Assess anomalies for risk to system



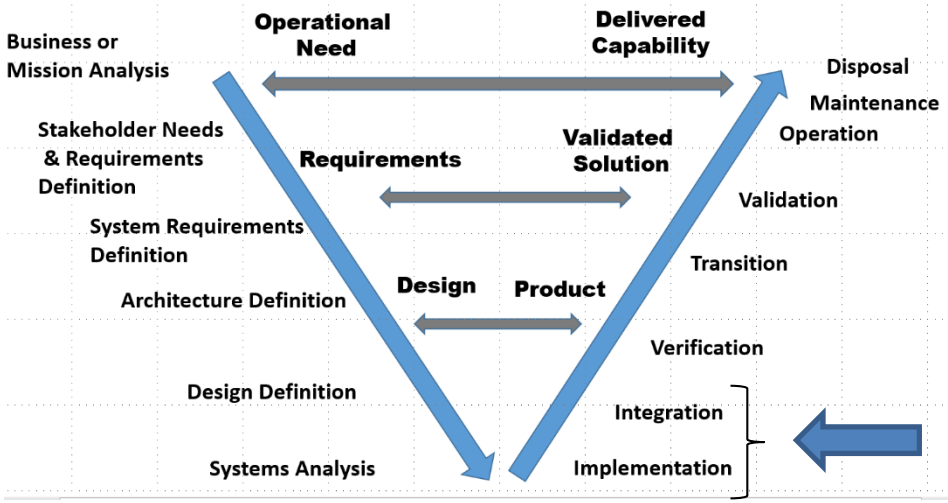
Technical Processes
Implementation and Integration

Purpose- General

- Implementation - Realize the specified system elements
- Integration - Synthesize the elements into a realized system that satisfies the mission need

  Elements, interfacing mission systems, enabling system, and recourses operate/fit together as required

- As-built documented and traceable



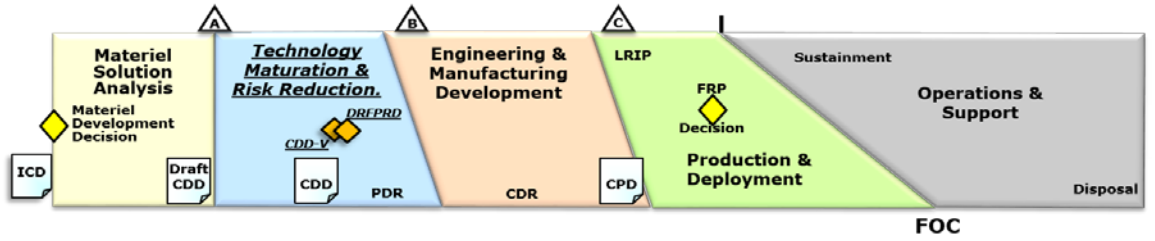
Purpose- Cybersecurity

- Protection is realized and the system element meets the requirements.
- The system elements, when assembled, provide the protection and resilience required for the system to perform its mission in the operational environment

Technical Processes
Implementation and Integration

Representative Activities

- Identify and mitigate risks associated with hardware and software developed or purchased for use on the system
- Define checkpoints to show that security requirements for elements and interfaces are being achieved
- Protect elements during creation, storage, and integration
- Ensure integrating systems when integrated support the protection and resilience needs to the system
- Document as-built and security compliance and provide for traceability
- Capture and assess non-compliance and anomalies



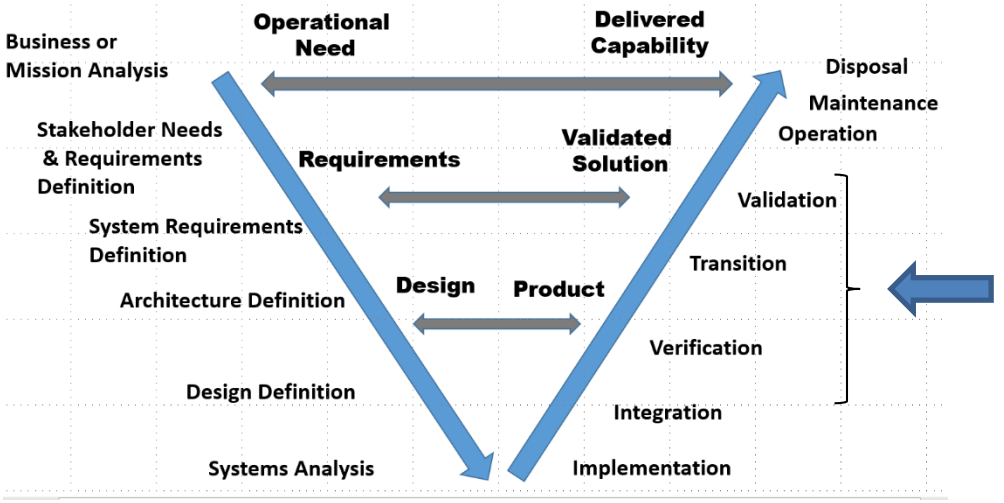
Technical Processes
Verification

Purpose- General

- Provide objective evidence that a system or system element fulfills its specified requirements and characteristics
- Identify anomalies in the implemented system elements, integrated system, information items, or lifecycle processes.

Purpose- Cybersecurity

- Does the system only exhibit specified behaviors, interactions, and outcomes- absence of certain behaviors.
- Methods, techniques, and processes are evaluated for fidelity and rigor
- Flaws, weaknesses, defects are evaluated for risk (vulnerability) in context of requirements
- System security requirements are satisfied



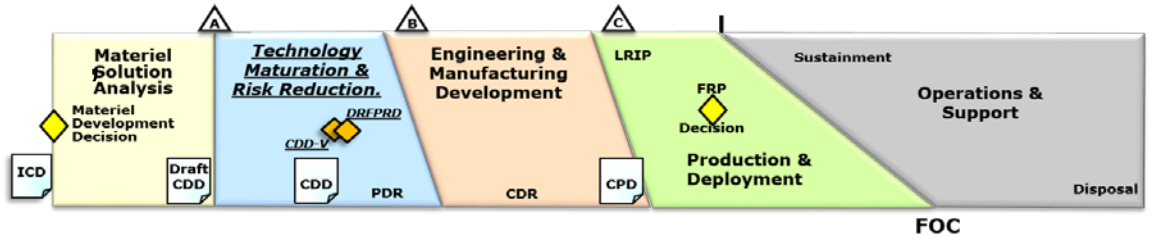
Technical Processes
Verification

Representative Activities

- Identify constraint on verification
- Get access to enabling and associated mission systems
- Verify interface compliance and that they don't weaken system of interest
- Identify methods, define procedures
- Verify as you go during architecture and implementation
- Record results and anomalies and residual risk assessment
- Get stakeholder agreement to results

Highlights:

- RTMs
- Test plans and Procedures
- Code/Design Walkthroughs
- Test results
- Review minutes
- Residual risk assessment
- DT&E
- FCA
- PCA



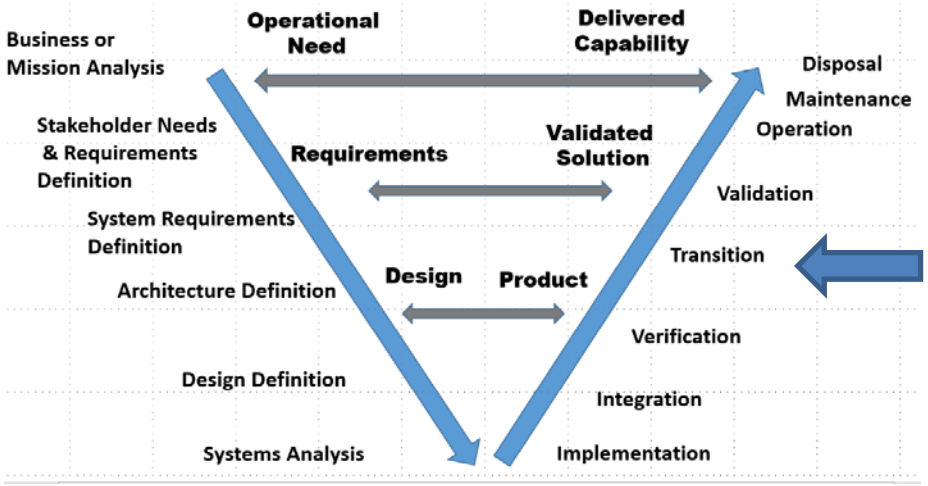
Technical Processes
Transition

Purpose- General

- Establish the capability for the system to provide the capability required by the stakeholder in the operational environment

Purpose- Cybersecurity

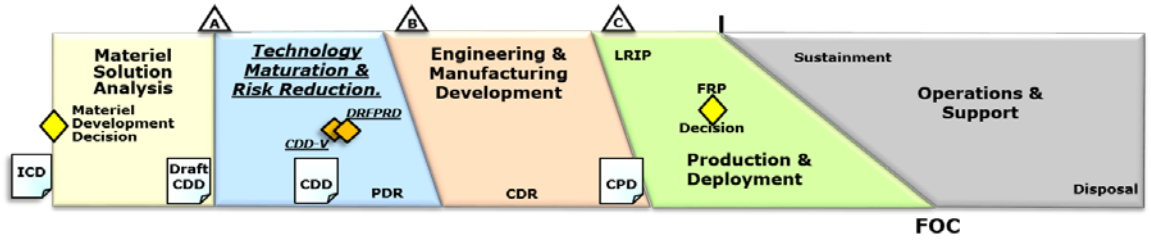
- Ensure cybersecurity and resilience characteristics are preserved
- Operators and users are trained to preserve and update security as required
- Documentation is provided to support daily operations while preserving security and resilience
- Demonstrate its installed correctly and security and resiliency is preserved
- Obtain authorization to operate



Technical Processes
Transition

Representative Activities

- Deploy methods and tools to ensure
  - System (including support equipment) integrity preserved during fielding, operations, and maintenance releases
  - System security is monitored and updates are made
- Procedures and training in place to ensure system security and resiliency can be maintained during operations and maintenance
- Documentation and other artifacts prepared that allows for system updates and support while preserving security and resilience characteristics
- System installed/deployed/ready for operations and security and resilience capability verified



Technical Processes
Validation

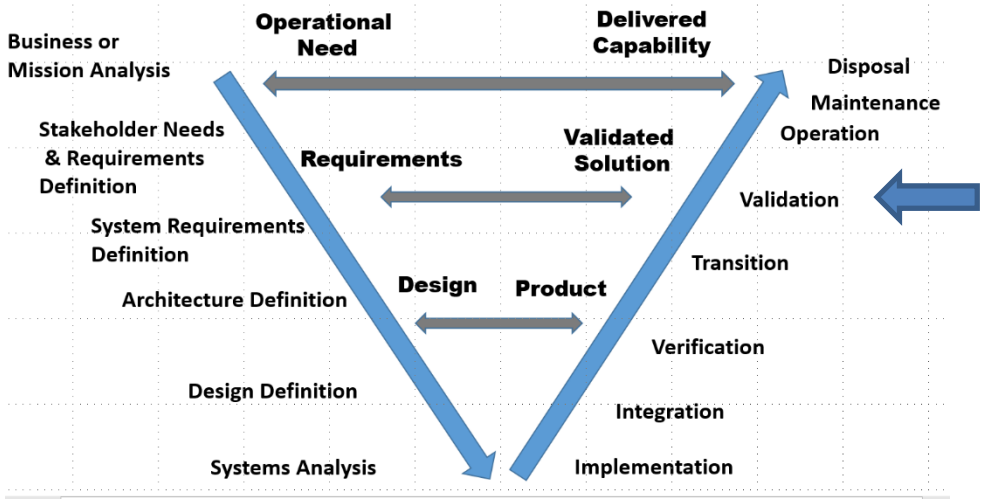
Purpose- General

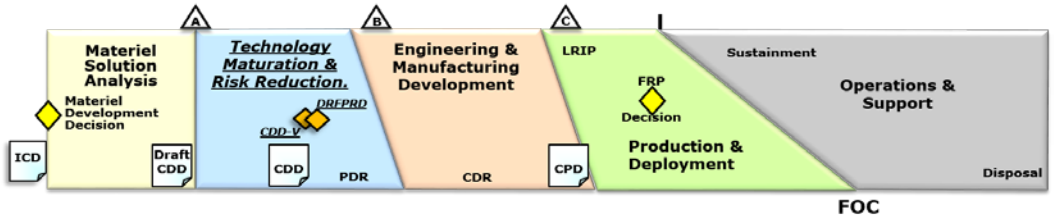
Provide objective evidence that the system fulfills its mission objectives and stakeholder requirements in its intended environment (IOT&E OT&E)

Purpose- Cybersecurity

Demonstrate that the system protection is adequate relative to disruptions, hazards, and threats in its intended operational environment

- System meets it mission objectives
- Provides adequate protection/Minimizes losses and consequences
- Does what it is supposed to do and only what it is supposed to do



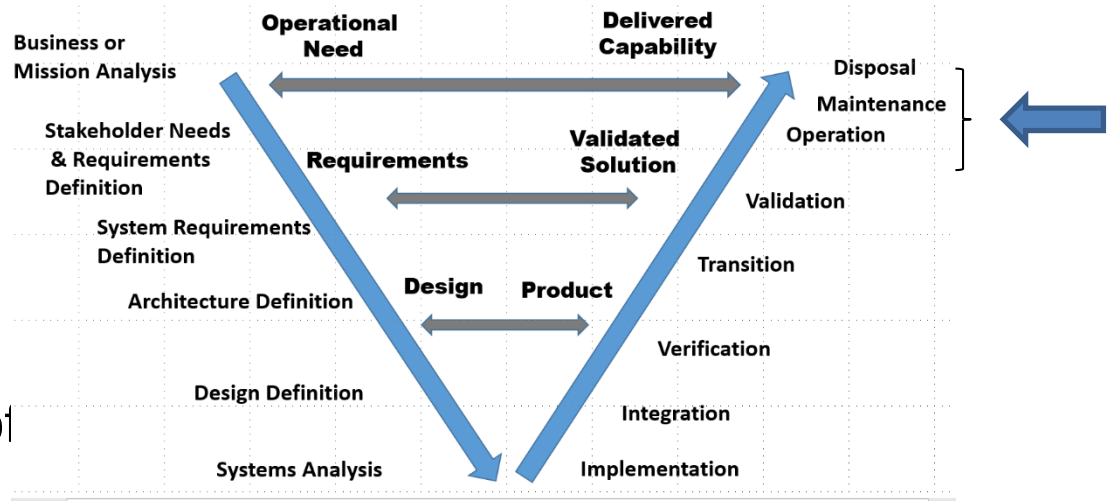


[OSD Memo, Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, 1 Aug 2014]

Technical Processes
Operations and Maintenance

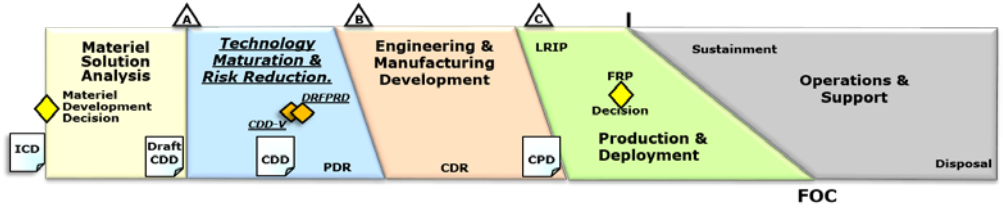
Purpose- General

- System is in operational use
- Ability of the system to provide required services is monitored and required actions to restore or amend services are provided



Purpose- Cybersecurity

- Cybersecurity operational and maintenance needs were considered in the development of the system
- Any enabling systems, materials, training, etc required for the secure operation of the system and maintaining an adequate security posture are available
- Security related issues are identified, assessed, and managed
- Security is adapted to new realities as required



Cybersecurity Across the ALM

Foundational Learning

Classroom & Online Student Engagement

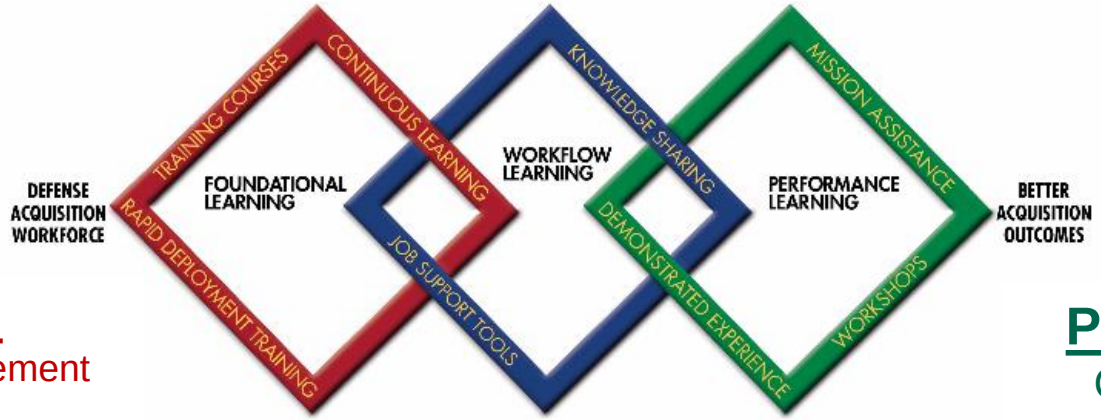
Deployed Course

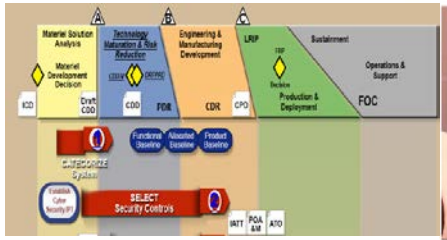
- **CLE 074** (Cybersecurity Throughout DoD Acquisition) - March 2015, over 6,000 graduates to date

Courses in Development

- **Program Protection Planning** (100 and 200 level)
- **Risk Management Framework for Practitioners**
- **Supply Chain Risk Management**
- **Software Assurance**

Cybersecurity content across career fields (IT, Engineering, PM, Contracting, Logistics, …)





Threat Vector or Threat Actor

Workflow Learning

Resources and Job Support Tools

- Cybersecurity Black Card Quick Reference
- Tuesday Talks, Lunch and Learns, Hot Topic Forums
- On-line videos
- RMF/ Acquisition Lifecycle Integrated Tool

Performance Learning

Consulting and Workshops

Mission Assistance and Workshops

- System Security Engineering
- Software Assurance
- RMF
- Creating internal CS/PIT Processes
- National Initiative for Cybersecurity Education (NICE) Workforce Framework

References

- DoD SE Website (http://www.acq.osd.mil/se/pg/guidance.html) with specific attention to Initiatives-Program Protection and Security Engineering
- DAG
- DoDI 5000.02, *Operation of the Defense Acquisition System,* 7 Jan 15
- DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,* 5 Nov 12
- DoDI 8510.01, *Risk Management Framework for DoD Information Technology,* 12 Mar 14
- CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 27 Mar 14
- IEEE Std 15288.2-2014, *IEEE Standard for Technical Reviews and Audits on Defense Programs,* 10 Dec 14
- *Outline and Guidance for the Cybersecurity Strategy,* 10 Nov 15
- *Program Protection Plan Outline & Guidance, V1.0, Jul 11*
- MIL-HDBK-1785, *Systems Security Engineering Program Management Requirements*, 1 Aug 95
- NIST SP 800-37, Rev 1, *Guide for Applying the RMF to Federal Information Systems*, Feb 10
- NIST SP 800-160, 2nd Public Draft, *Systems Security Engineering*, May 16
- ISO/IEC/IEEE 15288, Systems and Software Engineering- System Lifecycle Processes, 15 May 15
- *Cybersecurity Strategy Progress Summary, v1.0*, 10 Nov 15
- IEEE15288.1-2014, *IEEE Standard for Application of Systems Engineering on Defense Programs*, 10 Dec 14
- Engineering for System Assurance, V1.0, NDIA, Oct 08 (http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf)