A Justification for Comprehensive Critical Component Identification During the Program Protection Process

Beverly Ware

Dennis Mangsen

The MITRE Corporation

MITRE

Approved for Public Release;
Distribution Unlimited Case # 16-3607.

BLUF – Proposed CC Identification Process

- **Working with many Air Force (AF) programs, the authors have developed an approach to identifying a system's comprehensive list of critical components (CCs) to support Program Protection activities and events.**
- **Generating a complete list of critical components through a methodical approach provides the recommended set that meets the needs of various stakeholders.**
- **This presentation:**
  - Makes the case for an approach that leads to a comprehensive CC list
    - Effort is expended to identify the complete set of ICT components that may introduce a vulnerability
  - Walks through the enhanced CC identification process which identifies all components that meet the Trusted Systems and Networks (TSN) definition in DoDI 5200.44.

Agenda

- Program Protection Overview
- Critical Component Overview
- Existing CC Identification Process
- Justification for Developing an Improved Process
- Proposed Comprehensive CC ID Process

Program Protection Overview

- Department of Defense (DoDI) 5000.02 requires each acquisition program to “employ system security engineering practices and prepare a Program Protection Plan (PPP).”
- During the process of preparing a PPP, each acquisition program considers how their system can be adequately protected.
- The identification of CCs is a fundamental activity in the Program Protection process.
- The PPP Outline and Guidance document requires that a criticality analysis be performed and that CCs be prioritized.

Critical Component Overview

- **The primary guidance used to address critical components in systems is Department of Defense Instruction (DoDI) 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)"**
  - Defines Information and Communications Technology (ICT) and CCs.
- **Latest version incorporates Change 1, Effective August 25, 2016**
  - Added "including spare or replacement parts"
  - Added emphasis on sustainment and industrial control systems

Current DoDI 5200.44 Definitions (25 August 2016)

- **Critical Component (CC)**

  A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

- **Information and Communications Technology (ICT)**

  Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in section 11101 of title 40, U.S.C.. Rather, this term reflects the convergence of IT and communications.

- **Criticality Analysis**

  An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions.

Existing AF CC Identification Process

- **Functional decomposition beginning with mission objectives**
  - Identify and prioritize mission threads
  - Decompose to mission functions
  - Decompose mission functions to identify critical system functions
  - Identify CCs that implement mission critical system functions
    - Resulted in list of CCs that support those critical functions, but may not include CCs that support non-critical functions
- **Process emphasized FPGAs, ASICs, and Printed Circuit Boards**
- **Threat assessment requests submitted to DIA were expected to be at an individual component level, rather than at higher assembly levels.**

Justification for Developing an Improved Process

- **Existing/established process resulted in a critical component list which was less than the full set of CCs in a system**
  - Process concentrated on mission functions and critical functions. Non-critical functions were not considered.
  - Filtering/prioritization too early in the process meant that CCs associated with non-critical functions were not included.
- **Vulnerabilities to a system can be introduced via any ICT component, not just those components supporting mission critical functions**
  - CCs in enabling systems can also introduce vulnerabilities to a system
- **Emerging threats indicate a more comprehensive CC list is needed**

Proposed AF CC ID Process

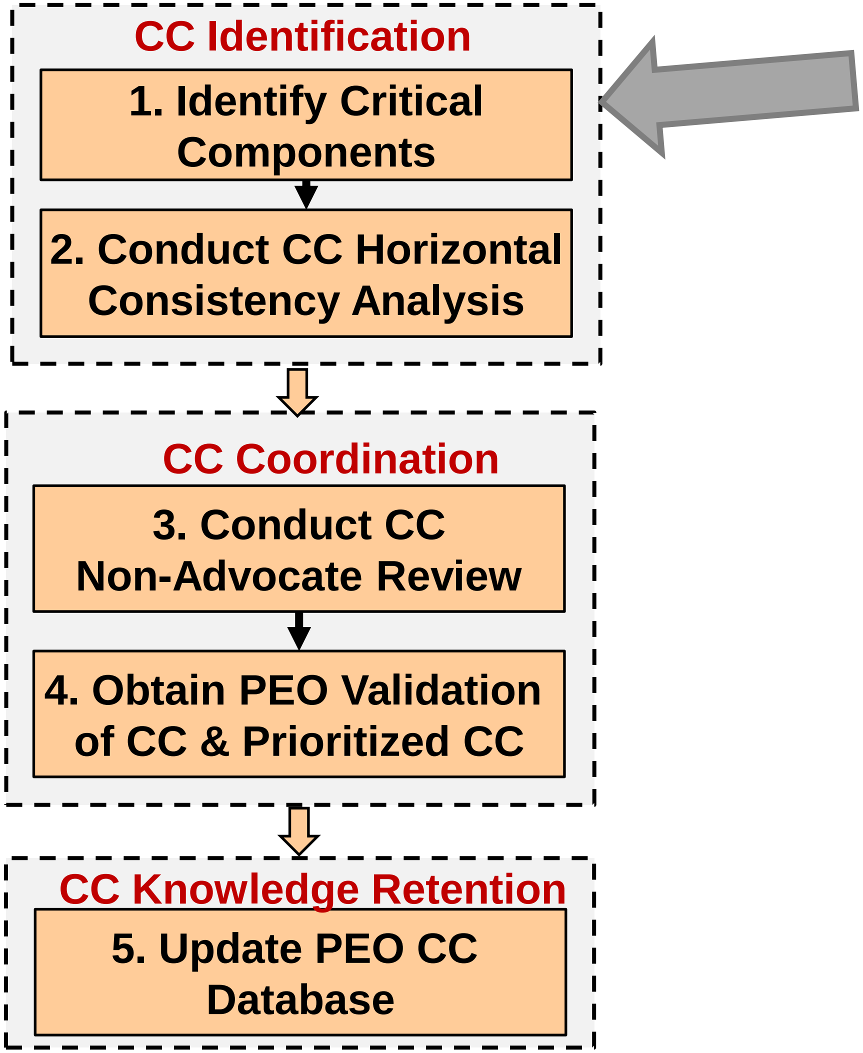
- ICT/CC identification is a comprehensive analysis across the full system (system-of-interest and enabling systems; definitions follow).
- The process produces the complete set of components that provide, protect or may introduce a vulnerability to the weapon system across the lifecycle. The analysis is completed once, resulting in a CC list that supports the needs of multiple stakeholders.
- Acquisition programs often discover that this systematic approach provides a thorough understanding of their system.
- Knowing the full set of CCs improves confidence in protection planning

Definitions for System Terms

System	Combination of interacting elements organized to achieve one or more stated purposes.
System-of-Interest	The bounded context that is the focus of the engineering effort. Bounds may be physical or logical.
Enabling System	System that exists in the life cycle of the system-of-interest and supports the development, manufacture, utilization, sustainment, or other life cycle activity associated with the system-of-interest.
Other System	System that interacts with the system-of-interest in its operational environment.

Adapted from ISO/IEC/IEEE 15288 “Systems and Software Engineering - System Life Cycle Processes”

CC ID Process Overview



CC Identification

1. Identify Critical Components

2. Conduct CC Horizontal Consistency Analysis

CC Coordination

3. Conduct CC Non-Advocate Review

4. Obtain PEO Validation of CC & Prioritized CC

CC Knowledge Retention

5. Update PEO CC Database

Focus of this presentation

Preparation for Conducting CC ID

Goal: Program prepares for critical component identification

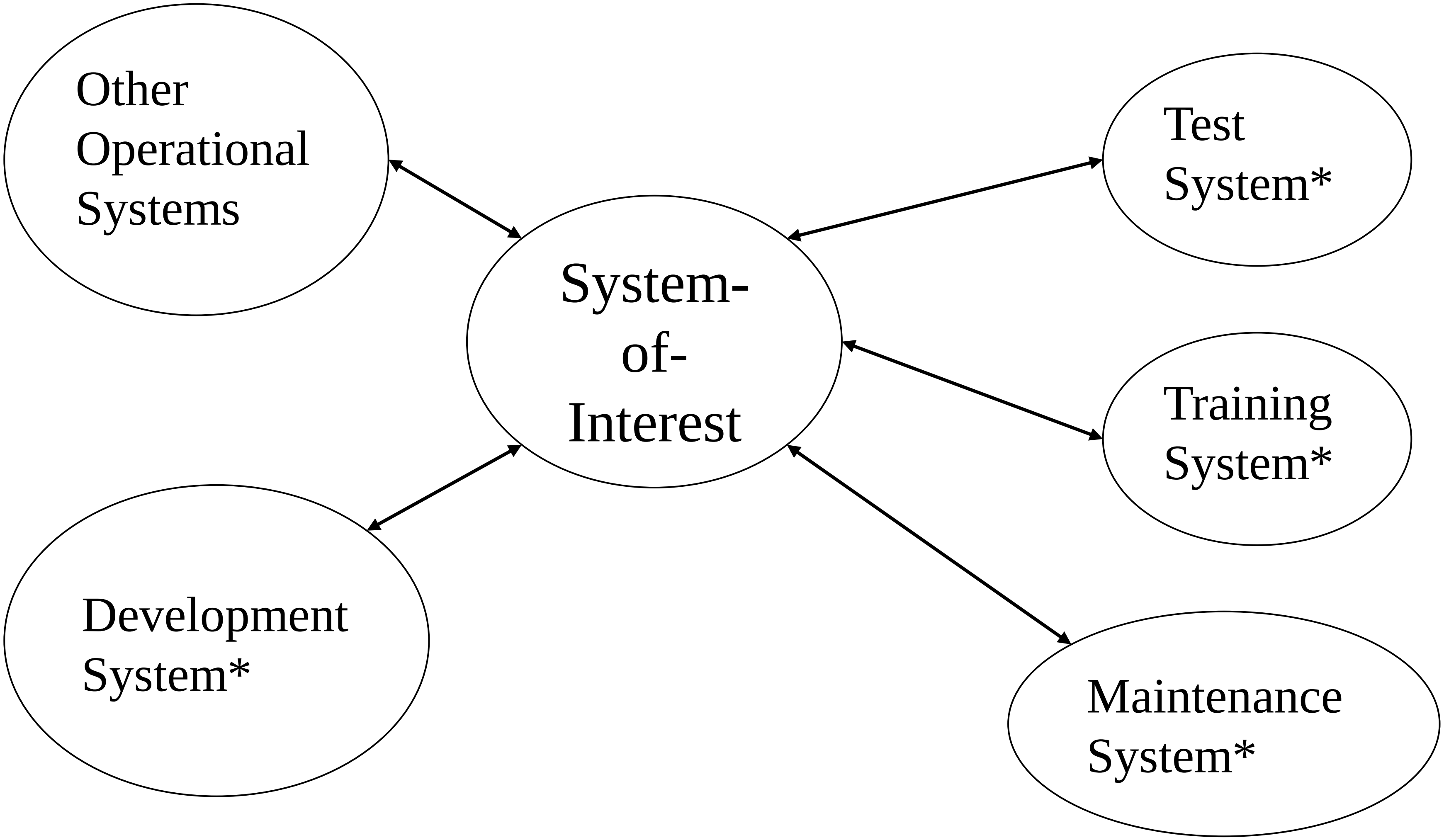
- **Set up a System Security Working Group (SSWG)**
  - Requires Government and Prime Contractor Subject Matter Experts (SMEs) across domains such as Cybersecurity, Supply Chain Risk Management, and Software Assurance
- **Gather documentation, such as:**
  - System Architecture & Functional Decomposition
  - System security boundary
  - Security Classification Guide (SCG)
  - System Requirements Document (SRD)
  - Capability Development Document (CDD)
  - Systems Engineering Plan (SEP)

CC ID Process Overview: Step 1. Identify Critical Components

- **To accomplish the identification of critical components:**
  - Task 1: Define System (include both the system-of-interest and the enabling systems)
  - Task 2: Define the boundary and interfaces for these systems
  - Task 3: Perform end-to-end functional decompositions of the system-of-interest and enabling systems to identify the mission functions.
  - Task 4: Trace each function to the hardware, software, and firmware components that implement those functions. Continue the decomposition until the lowest level of ICT components procured and/or managed as end-items are identified. List the CCs designed into the system-of-interest and in each enabling system.
  - Task 5: Prioritize the list of CCs according to stakeholder needs (e.g., TSN, RMF, Authorizing Official (AO))

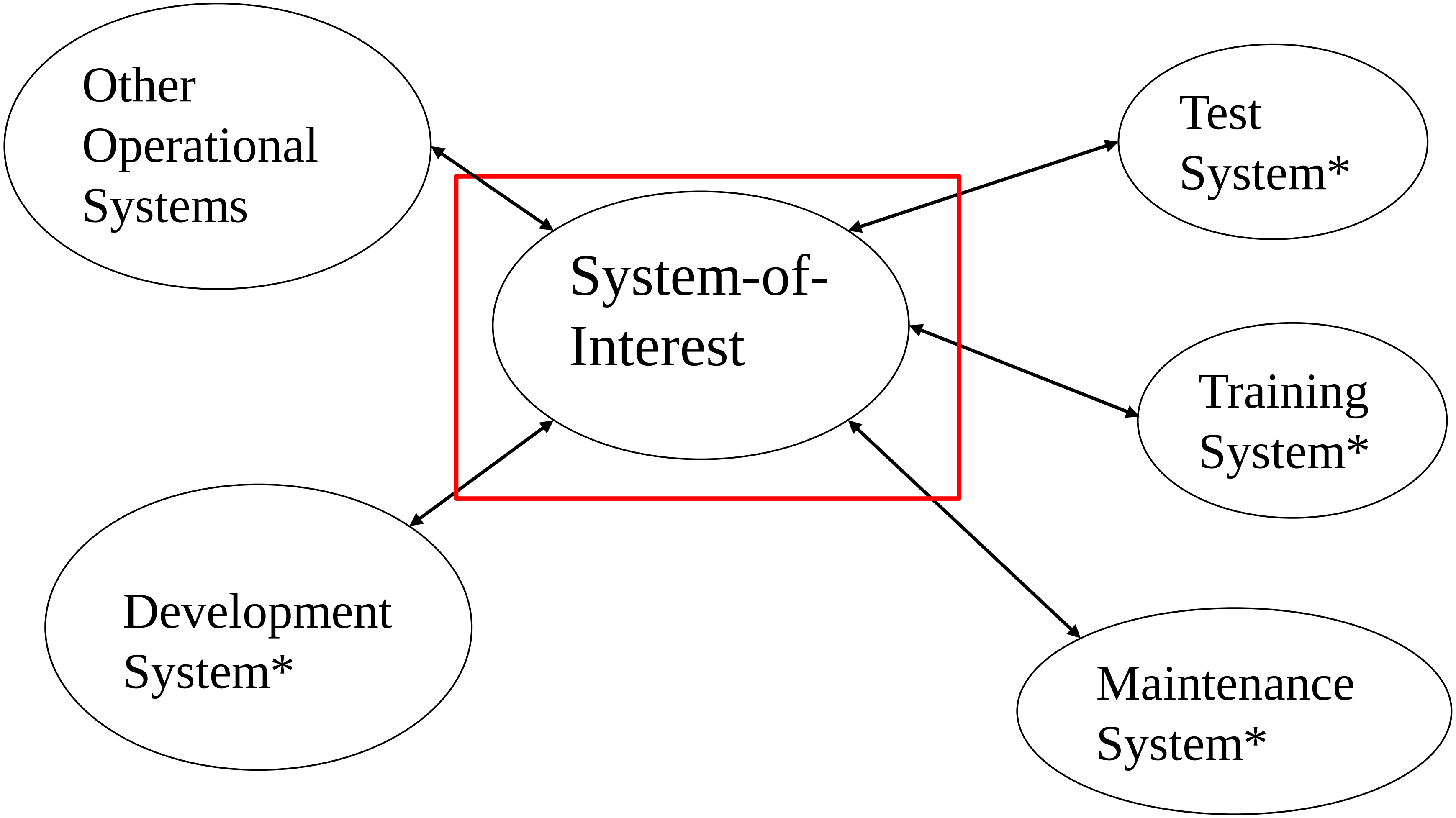
Outcome: Complete Set of Critical Components

Identify Critical Components – Task 1
Define System-of-Interest and its Enabling Systems



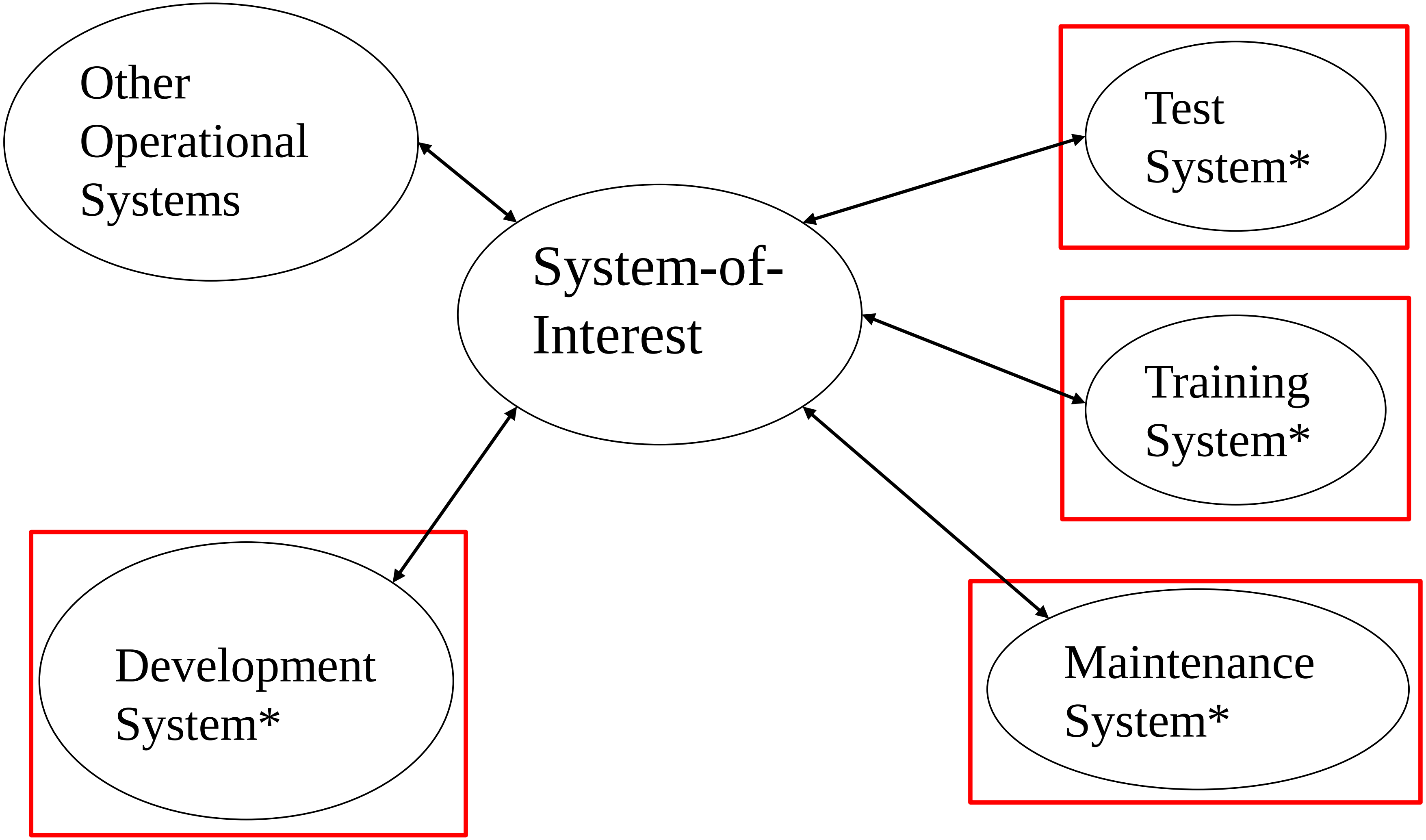
* Enabling System

Identify Critical Components – Task 2
Define System-of-Interest Boundary and Interfaces



* Enabling System

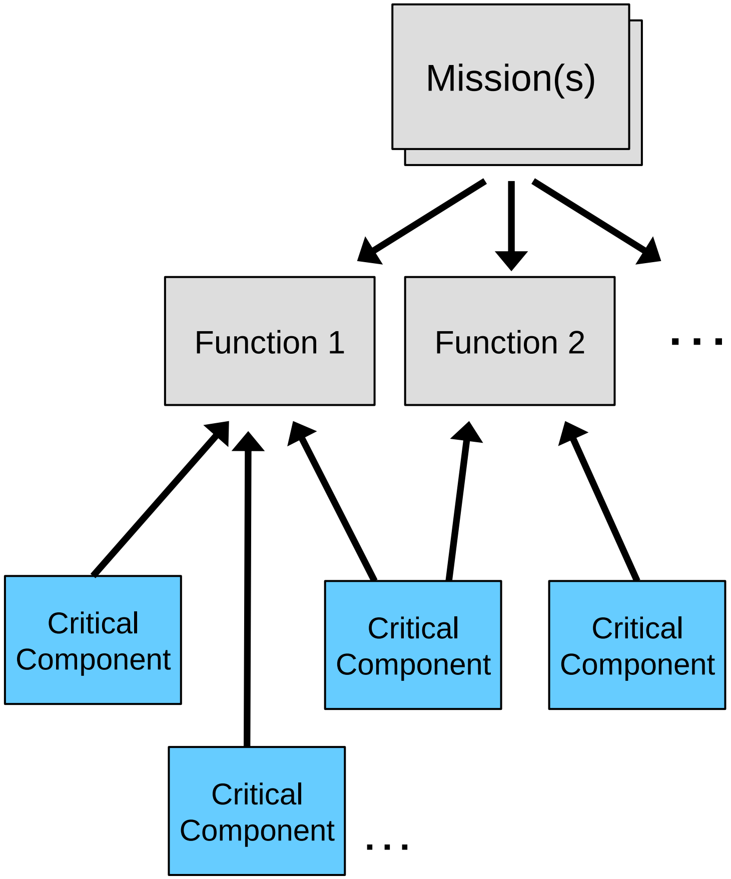
Identify Critical Components – Task 2
Define Enabling Systems Boundaries and Interfaces



* Enabling System

Identify Critical Components – Tasks 3 & 4
Perform Functional Decompositions to Generate the CC List

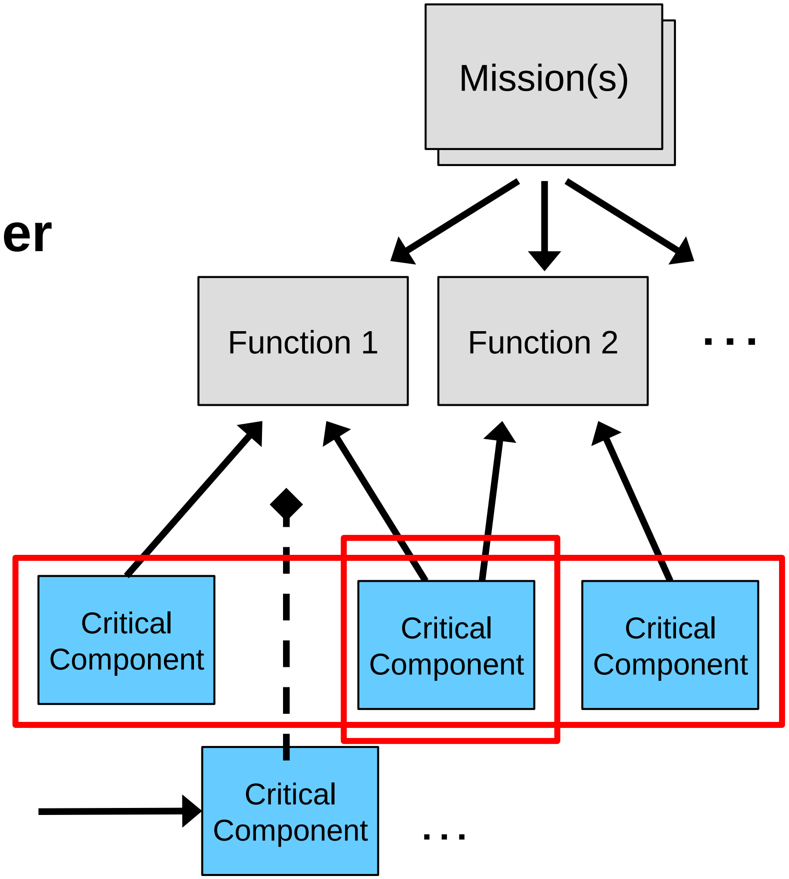
- **Identifies CCs through:**
  - **Performing a Functional Decomposition of mission(s) into mission functions**
  - **Mapping mission functions to supporting components**
  - **All components requiring unique item level traceability are included**
  - **Generating the complete set of CCs**



Outcome: Complete Set of Critical Components

Identify Critical Components – Task 5
Prioritize List in Accordance with Stakeholder Needs

- **Prioritize CC list in accordance with stakeholder needs**
- **May result in the same set of CCs being prioritized in a different manner**



May receive higher priority in a different stakeholder's view

Outcome: Prioritized Set of Critical Components for Stakeholder N

CC List Maintenance

- **Place CCs in a configuration-controlled list so that every Systems Engineering Technical Review (SETR) and milestone during an acquisition effort considers these items.**
- **Programs should request an intelligence assessment from the Defense Intelligence Agency (DIA) for the identified critical components.**
- **As the system transitions into the Operations and Support Phase, the CC list continues as an active artifact, and attention can be drawn to these items across the lifecycle of the system, further ensuring that the system's program protection needs are addressed.**
- **Manufacturers' databases, where available, should be leveraged in this process to ensure vulnerabilities are addressed and the system maintains its security posture.**
- **In addition to DIA, other stakeholders for CCs include RMF and entities looking for vulnerabilities in their weapon systems.**

Conclusion

- **Generating a complete list of critical components through a methodical approach:**
  - Provides increased confidence that adequate program protection can occur.
  - Provides the full set that meets the needs of various stakeholders.

Questions?

- **Beverly Ware**
  - MITRE Corporation
  - 781-271-2435
  - bware@mitre.org
- **Dennis Mangsen**
  - MITRE Corporation
  - 781-271-4637
  - dmangsen@mitre.org

Backup

Definitions for Unique Item Identifier Terms

Unique Item Identifier (UII)	A globally unique and unambiguous identifier that distinguishes an item from all other like and unlike items. The UII is derived from a UII data set of one or more data elements. (DoDI 8320.04)
Unique item level traceability	The requirement to trace life-cycle management events related to acquisition, storage, operation, maintenance, safety, physical security, retirement, and disposal by each individual item (e.g., for a single instance of a stock-numbered item or a single assembly or subassembly) (DoDI 8320.04)
Item Unique Identification (IUID)	A system of establishing globally ubiquitous unique identifiers on items of supply within DoD, which serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships. Defined in DFARS.