Software Engineering and System Assurance

Lifecycle Considerations

Kristen Baldwin

Deputy Director,
Software Engineering and System Assurance
US Department of Defense

January 2008

Briefing Purpose

- Respond to request from Chairman, AC327 and International Staff
  - Provide discussion context for software and system assurance lifecycle issues
  - Software
  - System assurance
  - System of Systems Engineering
- Discuss international interests and opportunities for AC327

Why Focus on Software: Software Growth in US Defense Systems

- Software Requirements Growth (% of functionality provided by software)[1]:
  - 1960s: 8%
  - 1980s: 40%
  - 1990s: 60%
  - 2000s: 80%
- Software Size Growth[2]
  - From < 2M estimated source lines of code in 1980s to > 10M lines of code in 1990s
  - Now approaching 20M ESLOC
- Software Overruns
  - 1994: 16.2% of SW projects completed on-time, on-budget[3]
  - 2005: 50% of SW projects still late, over budget[4]

1 Center for Strategic and International Studies (CSIS)
2 CSIS Analysis

*Top Software Issues**

1. The impact of requirements upon software is not consistently quantified and managed in development or sustainment. **"Requirements"**
2. Fundamental system engineering decisions are made without full participation of software engineering. **"SE/SW Integration"**
3. Software life-cycle planning and management by acquirers and suppliers is ineffective. **"SW Sustainment"**
4. The quantity and quality of software engineering expertise is insufficient to meet the demands of government and the defense industry. **"Human Capital"**
5. Traditional software verification techniques are costly and ineffective for dealing with the scale and complexity of modern systems. **"SW Testing"**
6. There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments. **"SW Assurance"**
7. Inadequate attention is given to total lifecycle issues for COTS/NDI impacts on lifecycle cost and risk. **"SW COTS/Reuse"**

*National Defense Industrial Association Report: Top Software Issues Workshop, August 2006

System of Systems Issues

- Why Systems of Systems (SoS)
  - **Asymmetric Threats** – New, ad hoc SoS configurations will be needed to address changing, unpredictable operational demands
  - **Joint / Coalition Operations** – SoS solutions enable interoperability
- Challenges
  - **Ownership / Management** – Individual systems are owned by member nations, introducing constraints on management and resources
  - **Legacy Systems** – Current systems will be part of the defense inventory for the long-term and need to be factored into any approach to SoS
  - **Criticality of Software** – SoS typically focus on integration across systems through cooperative or distributed software
  - **Role of Network** – Network based vision has not been fully implemented; challenges remain

US DoD Way Forward

- Goal: Establish strategy and activity to address all top issues and gaps
- Key Projects:
  - SW/SE Lifecycle Integration
  - SW Cost & Risk Estimation Guidance and Tools
  - SW Test Guidance
  - SW Sustainment Methods
  - SW COTS/Reuse Study
  - SW Requirements Guidance
  - SW Human Capital Strategy

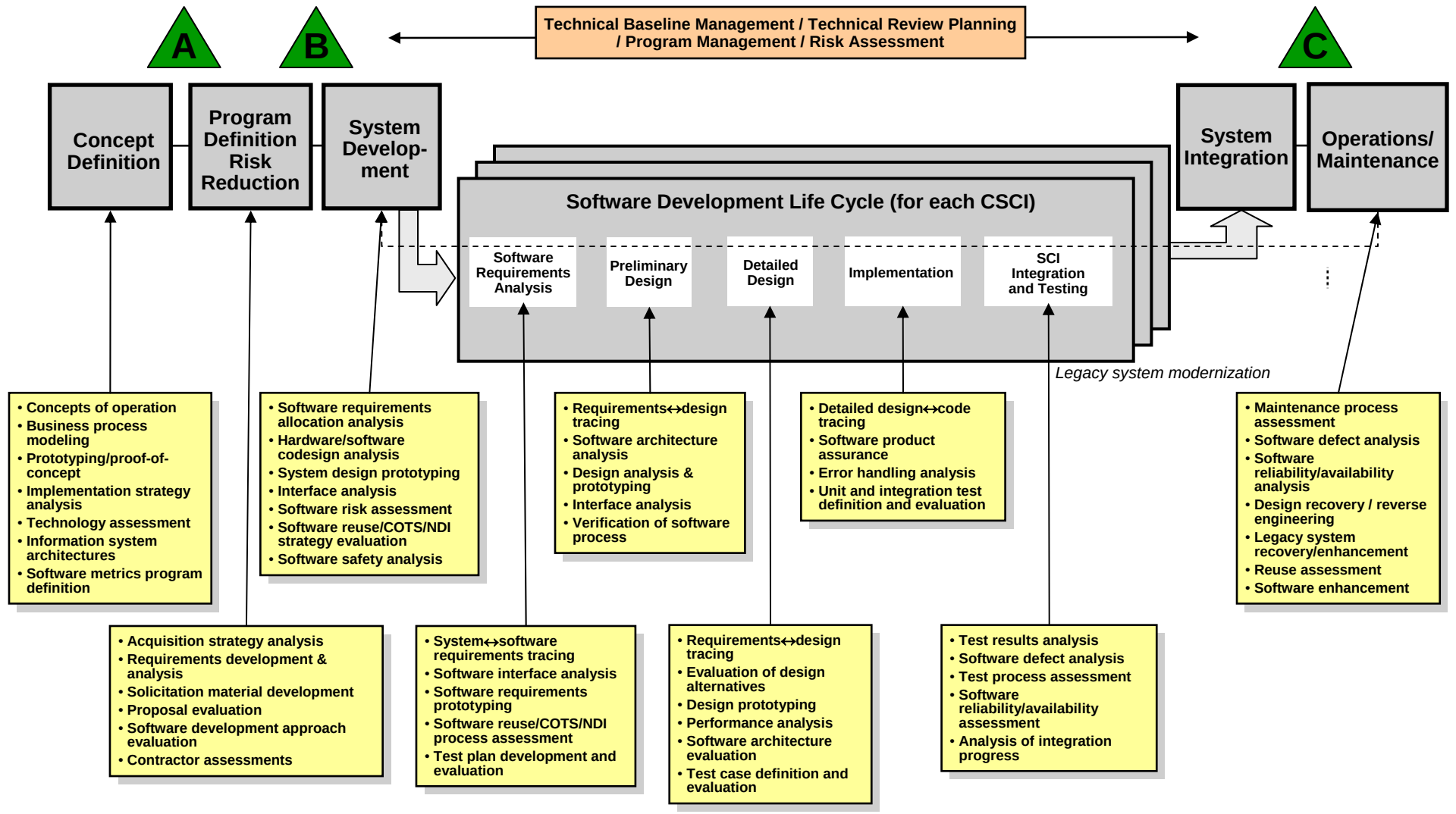
  Software
  - SoS Systems Engineering Guidebook
  - SoS Cost & Risk Drivers Research

  SoS Systems Engineering
  - System Assurance Guidebook
  - System Assurance Standard (ISO 15026)

  SW/System Assurance
- Outcomes
  - Policy, Education, and Acquisition Support tools/techniques
  - NATO: tbd

Software

Software Engineering Life Cycle Framework



Software Lifecycle Projects

A series of projects with appropriate expertise (government, industry, academia) to develop *near term* guidance and tools

- SW/SE Lifecycle Integration
  - Integration of software into systems engineering technical reviews, risk management, decision analysis
- SW Cost & Risk Estimation Guidance and Tools
  - Develop Earned Value Management policy for software programs
  - Develop Work Breakdown Structure method for software programs
- SW Test Guidance
  - Practices to address software testing and integration
- SW Sustainment Methods
  - Translating sustainment into a continuous lifecycle planning approach for software
- SW COTS/Reuse Study
  - Guidance on planning for and estimating COTS and Reuse in systems
- SW Requirements Guidance
  - Early allocation of requirements to software and hardware; impacts and risk

SW Human Capital Strategy
A project for the future…

Issue: There is no commonly accepted curriculum for software engineering education

- Project Description:
  - Develop a core university curriculum and core competencies for software engineering that can be adopted by the community
- Participants:
  - Industrial and government workforce customers of SW education
  - Universities who provide SW education
  - Professional societies with a vested interest in SW education (IEEE, ISO, INCOSE)
- Project Focus:
  - Inconsistencies in software engineering degrees
  - Poor definition of software labor categories
  - The divide between systems and software engineering education in industry, government, and academia
- Outcome Goal:
  - A more consistent training and hiring base for Software Engineers
  - Synchronization between SW and SE education

System Assurance

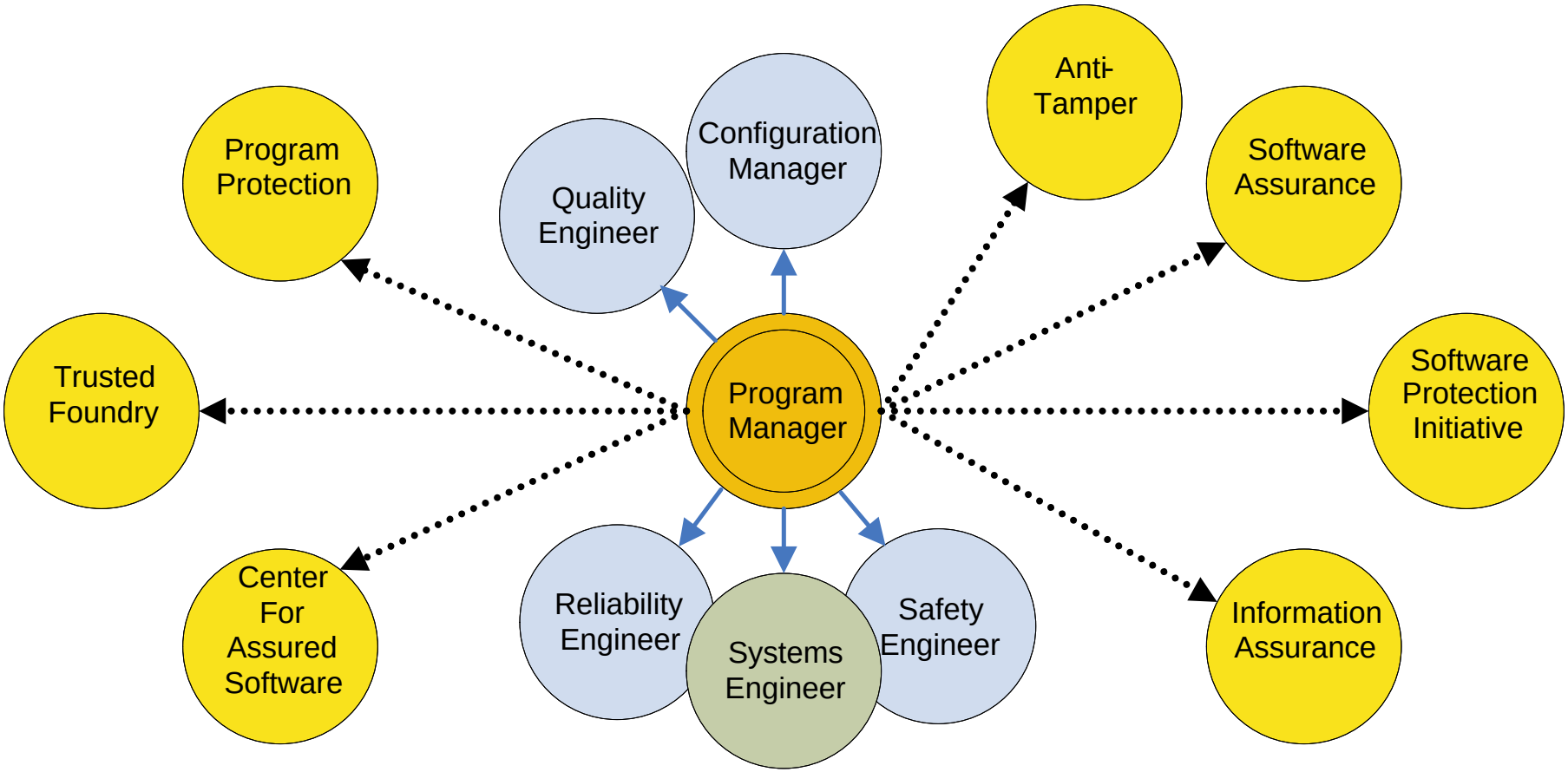
System Assurance Threat

- ***Threat agents***: Nation-state, terrorist, criminal, rogue developer who:
  - Gain control of system software/hardware/information through supply chain opportunities
  - Exploit vulnerabilities remotely
- ***Vulnerabilities***:
  - Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Counterfeit or tampered hardware
  - Exfiltration of information
- ***Consequences***:
  - Mission critical data and functions may be corrupted or denied
  - Systems and networks may be impacted

System Assurance –Definition

The measure of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the lifecycle.

System Assurance for the Program Manager



Lack of focused guidance to counter the threat

Acquisition Path Forward – Implementing the Requirement for Assurance

Raise the bar:	
Awareness	- Knowledge of the supply chain - Who has access to our critical assets
Protection	- Protect critical assets through security practices - Design our systems for assurance

- Create a framework to integrate multiple security policies and guidance
  - Leverage Program Protection requirement for all acquisition programs as set by 5200.39 policy
  - Integrate all assurance oversight, planning, and risk mitigation activity at the system level
- Develop Guidance on Engineering for System Assurance
  - Guidebook on Engineering for Assurance for program managers/engineers
  - Defines how assurance can be incorporated into system engineering and design:
    - e.g. Isolation, Redundancy, Quality and Fault Analysis

International Standard for System Assurance

- ISO 15026 – Systems and Software Assurance
  - Provides a delta to 15288 and 12207 SE and SW standards
  - Defines assurance process for the lifecycle
- Status
  - New work proposal approved by vote of 18-2-8
  - US, UK and Japan major comments
  - Author team has initiated drafting in 4 parts
- Construct: 4-part standard
  - 15026-1: Concepts and vocabulary
  - 15026-2: Assurance case
  - 15026-3: System integrity levels
  - 15026-4: Assurance in the lifecycle

This standard provides a foundation for defense and commercial industry to build more assured systems

SoS Systems Engineering

Guidebook for System of Systems Systems Engineering

SoS Guide Version 0.9

- **Initiative of the Office of the Secretary of Defense**
- **Collaborative approach with Industry, Academia, International Partners**
- **Purpose:**
  - **Develop guidance on technical considerations for system engineering at a SoS level**
- **Audience: PMs and Lead/Chief Systems Engineers**

Pilot

- **6 month pilot phase: "Beta test" the SoS SE Guide**
  - **Based on structured walkthroughs with practitioners**
  - **Refine guide content, identify areas for future study**
- **Update findings and release Version 1.0 (Jan 2008)**

A mechanism to share emerging insights on SoS and implications for SE

SoS SE Guide
Key Roles of a SoS SE

- Translating SoS capability objectives into high level requirements over time
- Understanding the systems in the SoS and their relationships
- Assessing extent to which the SoS meets capability objectives over time
- Developing, evolving and maintaining a design for the SoS
- Anticipating and assessing impacts of potential changes on SoS performance
- Evaluating new and evolving requirements on SoS and options for addressing these
- Orchestrating upgrades to SoS

Guide will incorporate new techniques and solutions as SoS pilots progress

SoS – Focus for FY08 Study

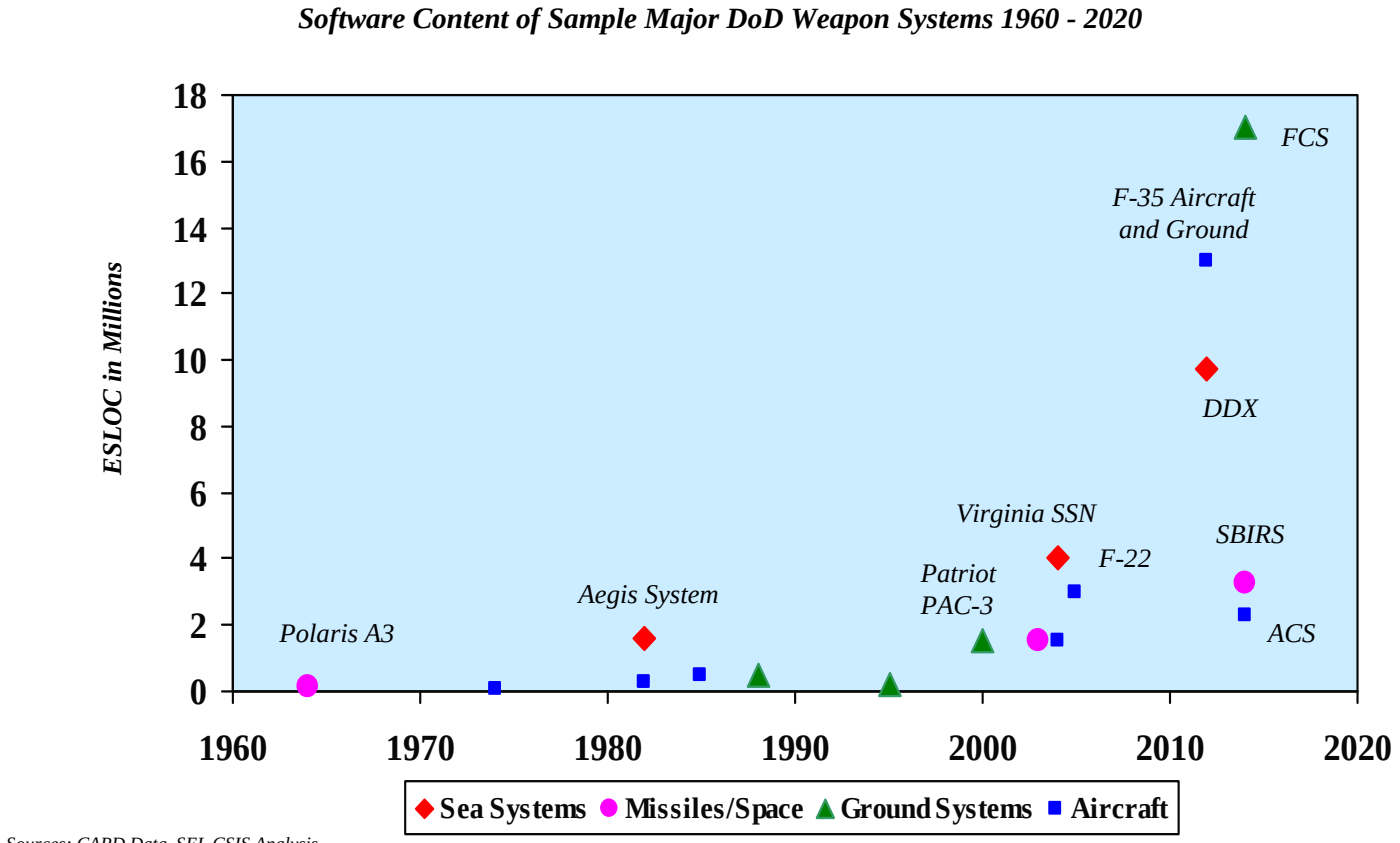
- Testing in a SoS environment
  - Testing multiple constituent systems, possibly at different stages in development
- SoS risk and cost drivers
  - Identify key SoS technical risk drivers to aid in planning
  - Cost of the SoS is not only the sum of the constituent systems
- Net-centric issues
  - Should we change the way we engineer individual systems to produce more net-centric solutions?
- Enablers to allow SEs to better operate
  - New contracting methods
  - New management models
  - How to adapt system lifecycle acquisition models to SoS?

Recap and Discussion

- AC327 relationship
  - Software impacts procurement management, maintenance and logistic support systems
  - Software is a critical enabler for SoS
  - Assurance is a consideration across the lifecycle
- Opportunities exist to leverage international interest and experience
  - Near term software lifecycle projects
  - Far term software education strategy
  - Techniques and standards to improve design for system assurance
  - Guidance for systems of systems acquisition
- Discussion

Back-ups

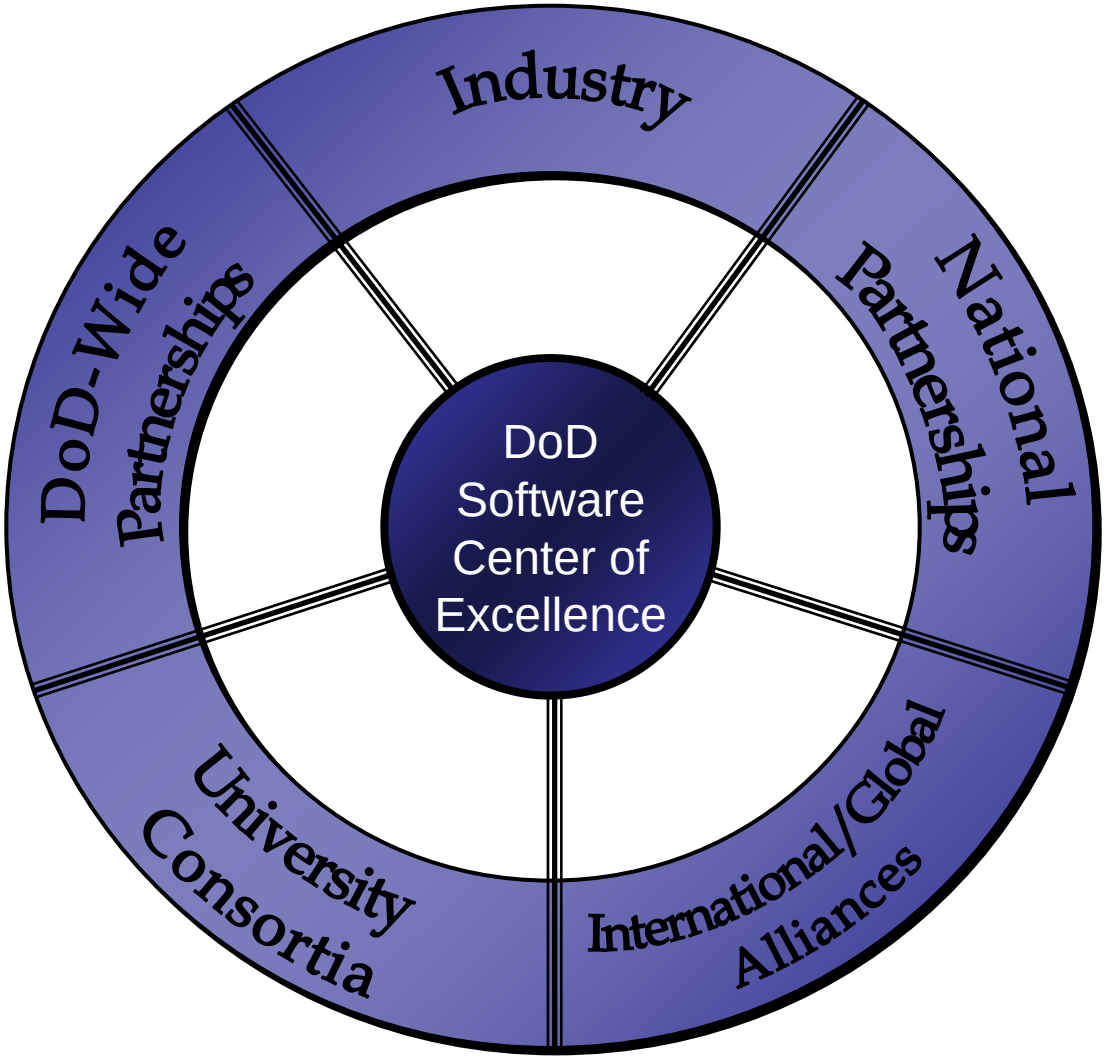
DoD Software Demand
System Size and Complexity (continued)



Sources: CARD Data, SEI, CSIS Analysis

DoD's dependence on larger, more complex software increases the risk of failing to deliver systems on schedule and within budget

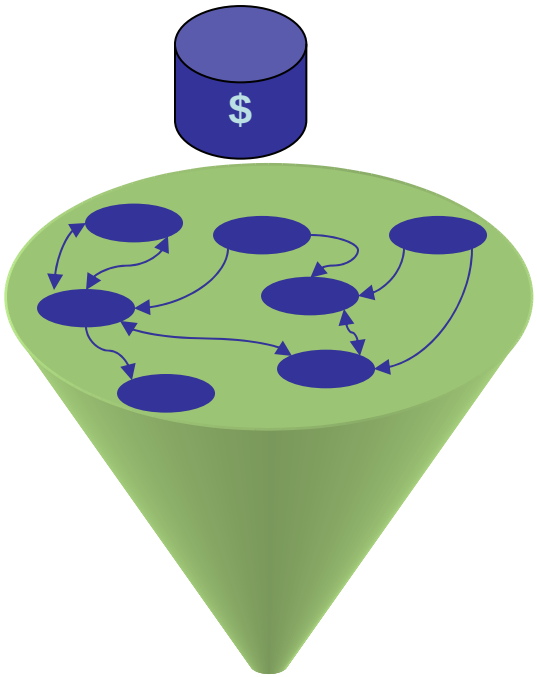
Establishing a DoD Software Center of Excellence

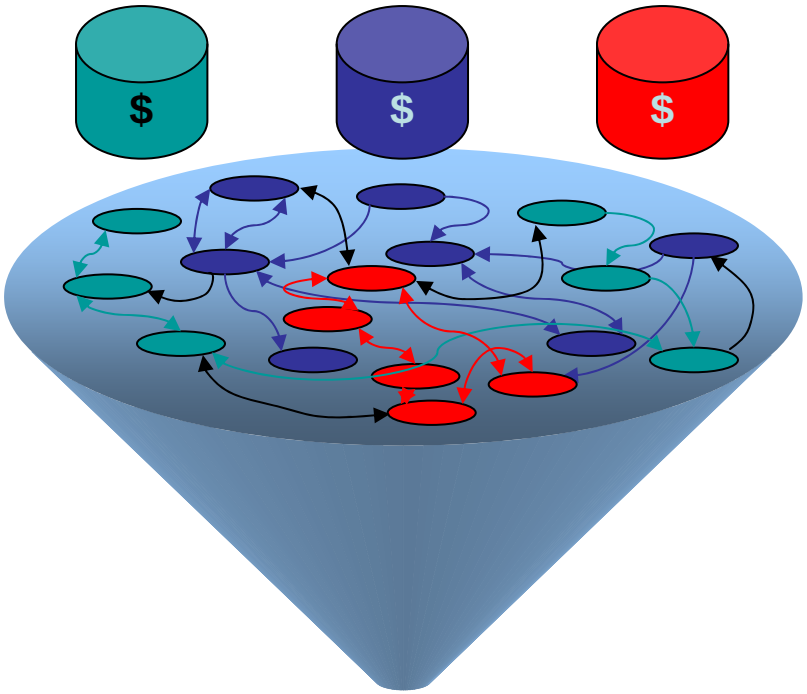


DoD Software Center of Excellence

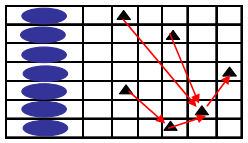
- Support Acquisition Success
- Improve State-of-the-Practice of Software Engineering
- Leadership, Outreach and Advocacy
- Foster Resources to Meet DoD Needs

System of Systems
The Management Challenge

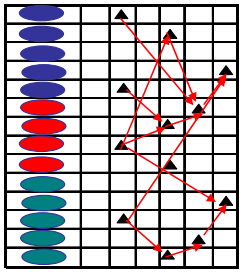




SoS:
Within
Single
Organization



Joint SoS:
Interdependencies
Across
Multiple
Organizations



Political and Cost Considerations impact on Technical Issues