Systems Engineering for Software Assurance

Kristen Baldwin
Office of the Under Secretary of Defense
Acquisition, Technology and Logistics
Systems Engineering

Software Assurance

- ❑ ***Scope***: Software is fundamental to the GIG and critical to all weapons, business and support systems
- ❑ ***Threat agents***: Nation-state, terrorist, criminal, rogue developer who:
  - » Gain control of IT/NSS through supply chain opportunities
  - » Exploit vulnerabilities remotely
- ❑ ***Vulnerabilities***: All IT/NSS (incl. systems, networks, applications)
  - » Intentionally implanted logic (e.g., back doors, logic bombs, spyware)
  - » Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- ❑ ***Consequences***: The enemy may steal or alter mission critical data; corrupt or deny the function of mission critical platforms

Software assurance (SwA) relates to the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software.

Background

- In July 2003, the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)] established the Software Assurance Initiative to examine software assurance issues
- On 23 Dec 04, Undersecretary of Defense for Acquisitions, Technology and Logistics [USD(AT&L)] and ASD(NII) established a Software Assurance (SwA) Tiger Team to:
  - » Develop a holistic strategy to reduce SwA risks within 90 days
  - » Provide a comprehensive briefing of findings, strategy and plan
- On 28 Mar 05, Tiger Team presented its strategy to USD(AT&L) and ASD(NII) and was subsequently tasked to proceed with 180 day Implementation Phase

Guiding Principles for DoD SwA Strategy

- Understand problem from a systems perspective
- Response should be commensurate with risk
- Sensitive to potential negative impacts
  - Degradation of our ability to use commercial software
  - Decreased responsiveness/ increased time to deploy technology
  - Loss of industry incentive to do business with the Department
  - Minimize burden on acquisition programs
- Exploit and extend relationships with:
  - National, international, and industry partners
  - DoD initiatives, e.g., trusted integrated circuits and Information Assurance

DoD SwA Strategy – Primary Elements

- Partner with Industry to focus science and technology on research and development of technologies
  - Improve assured software development tools and techniques
  - Strengthen standards for software partitioning and modularity
  - Enhance vulnerability discovery
- Employ repeatable Systems Engineering (SE) and test processes to identify, assess, and isolate critical components, and mitigate software vulnerabilities
- Leverage and coordinate with industry, academia and national and international partners to address shared elements of the problem

Industry Outreach

Goal: Partner with industry to create a competitive market that is building demonstrably vulnerability-free software

- ❑ USD(AT&L)/ASD(NII) memo to Industry
  - » Requested participation in an Executive Roundtable

- ❑ Tiger Team held initial meetings with directors:
  - » National Defense Industrial Association (NDIA)
  - » Government Electronics & Information Technology Association (GEIA)
  - » Aerospace Industries Association (AIA)
  - » Object Management Group (OMG)

- ❑ Identified areas of interest for SwA white papers
  - » OMG will leverage ongoing standards activities
  - » NDIA hosting SwA Summit; will consider SE, C4ISR, IT implications
  - » GEIA will share lessons and collaborate to develop new processes
  - » AIA will help integrate SwA processes into mainstream integration activities

NDIA Software Assurance Summit, 7-8 Sep 05

Summit Purpose

- Explore the range of opportunities for a long term solution to the issue of software assurance to consider how we can force the desired capability.

- Bring together Government and Industry in partnership to consider the way forward, such as
  - Focus on science and technology
  - Improve software development tools and techniques
  - Strengthen standards
  - Enhance vulnerability discovery
  - Use Systems Engineering and test processes to identify assess, and isolate critical components and mitigate vulnerabilities
  - Leverage and coordinate with industry, academia and national and international partners in achieving the desired goals
  - Apply techniques used in other industries for certification and mission assurance

SwA Summit Activities

❑ Plenary panel discussions/briefings from DoD, Department of Homeland Security and Industry

❑ Conducted Four Breakout Sessions:

- » Standards, Metrics, Models
- » Industry Best Practices
- » Engineering Processes
- » Science and Technology

❑ Attendance

- » 40 in attendance
  - 17 Industry
  - 5 Academia
  - 18 Government/FFRDC

❑ Proceedings posted on NDIA website

NDIA NATIONAL DEFENSE INDUSTRIAL ASSOCIATION STRENGTH THROUGH INDUSTRY & TECHNOLOGY

AFEI ASSOCIATION FOR ENTERPRISE INTEGRATION

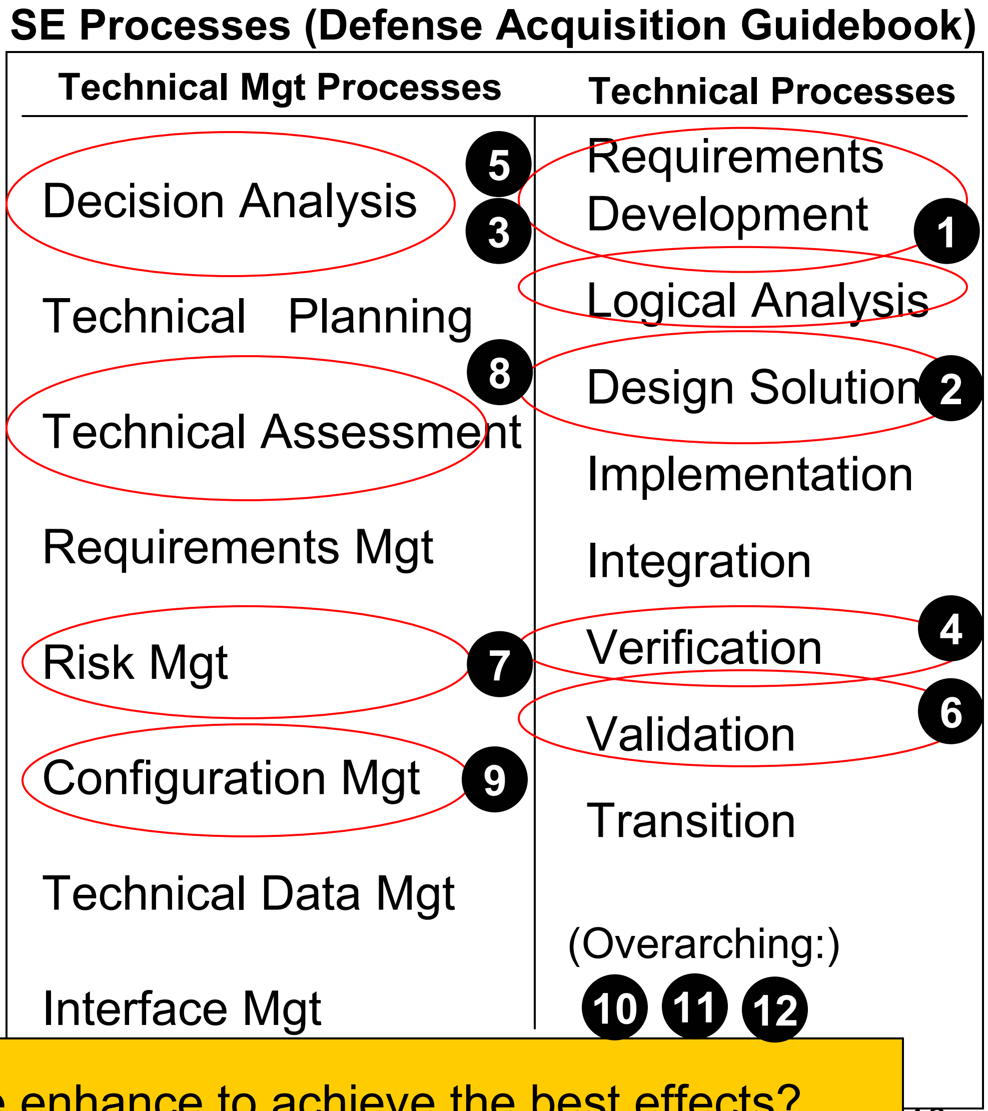
Systems Engineering for SwA - Many Alternatives to Consider

- □ Design around the problem
  - » Added emphasis on DoD systems engineering practices to mitigate COTS-based risks
- □ Build better products
  - » Vector commercial products to enhance bounding and controllability
- □ Better understanding of what’s in the product
  - » Enhance transparency, testability and understandability of product software code
- □ Use High Assurance products selectively where needed
  - » Use DoD security components in critical functions and at key architecture junctures
- □ Many more possible avenues…

Potential SE Support for SwA

- Top level definition:
  - Focus SE on the issues of SwA
  - Design SwA into the product instead of adding it on
- Top level approach:
  - Work with industry to define SE enhancements
- Derive reasonable and cost effective enhancements
  - Insert agreed enhancements into DoD acquisition policies & guidance

SE Processes (Defense Acquisition Guidebook)



Technical Mgt Processes

- Decision Analysis 5 3
- Technical Planning
- Technical Assessment 8
- Requirements Mgt
- Risk Mgt 7
- Configuration Mgt 9
- Technical Data Mgt
- Interface Mgt

Technical Processes

- Requirements Development 1
- Logical Analysis
- Design Solution 2
- Implementation
- Integration
- Verification 4
- Validation 6
- Transition

(Overarching:) 10 11 12

What Key SE processes can we enhance to achieve the best effects?

# = potential EID SE process intersects

Notional SE Support Mechanisms (1 of 2)

1. **Develop a common core set of tailorable SwA requirements & metrics**
2. **Develop an approach for performing operational SwA sensitivity analysis**
3. **Develop an approach for identifying SwA driven scenarios for use in Analyses of Alternatives (AOA) and hazard analyses**
4. **Develop candidate SwA test metrics for inputs to Test and Evaluation Master Plan (TEMP) SwA Annexes, to include applicable:**
5. **Define an approach for SwA applicable Modeling and Simulation (M&S)**
6. **Define a mechanism for selective technical "red-team" reviews of key software**

Notional SE Support Mechanisms (2 of 2)

7. Develop a common core set of SwA threats and vulnerabilities with probability and consequence metrics
8. Develop top-level Software and SwA Entry/Exit Criteria for SE Technical review(s)
9. Develop an enhanced SwA informed CM process to ensure full life cycle protection
10. Examine strategies for providing enhanced DoD SwA Standards leadership and management
11. Develop and implement education, training and certification avenues for acquisition participants
12. Define a continuous process improvement approach based upon evolving threat assessments through an engineering community sensitized to SwA

Way Ahead

We must create a competitive market that is building demonstrably vulnerability-free software