DoD Software Engineering and System Assurance

Kristen Baldwin

Deputy Director, Software Engineering and System Assurance

Office of the Under Secretary of Defense

Acquisition, Technology and Logistics

Elements of AT&L Strategy for Software

- Support Acquisition Success
  - Ensure effective and efficient software solutions across the acquisition spectrum of systems, SoS and capability portfolios
- Improve the State-of-the-Practice of Software Engineering
  - Advocate and lead software initiatives to improve the state-of-the-practices through transition of tools, techniques, etc.
- Leadership, Outreach and Advocacy
  - Implement at Department and National levels, a strategic plan for meeting Defense software requirements
- Foster Software Resources to meet DoD needs
  - Enable the US and global capability to meet Department software needs, in an assured and responsive manner

Promote World-Class Leadership for Defense Software Engineering

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/NDI/Reuse"**

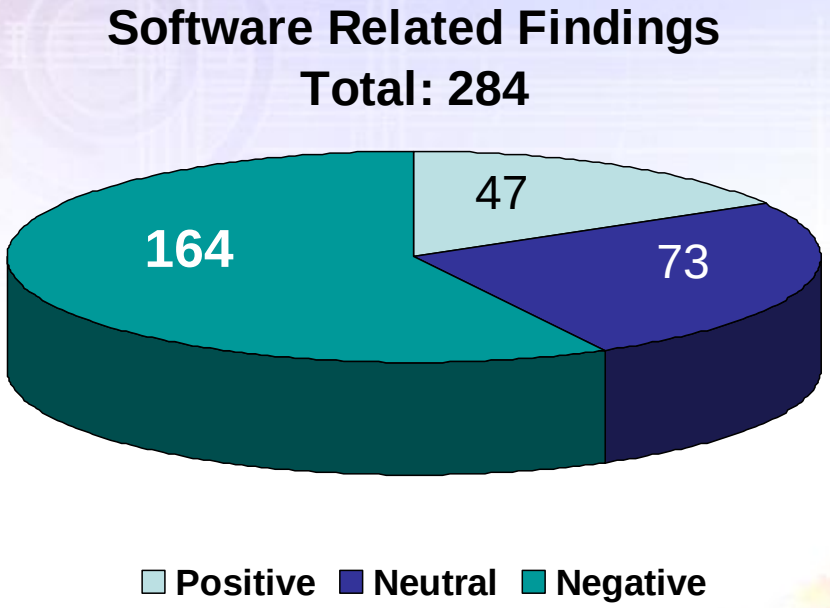
***NDIA Top Software Issues Workshop**
August 2006

OSD Software Systemic Analysis

- OSD(AT&L)/SSE Systemic Analysis Database
- Current Dataset: 68 reviews on 38 different ACAT 1D systems acquisition programs since early 2004
  - Approx 4,000 findings from these reviews placed into formal database repository
- Data extracted using the following key words:
  - Software
  - Systems-of-Systems (SoS)
  - Assurance
  - Architecture
  - Security
- 600+ findings resulted from the keyword search

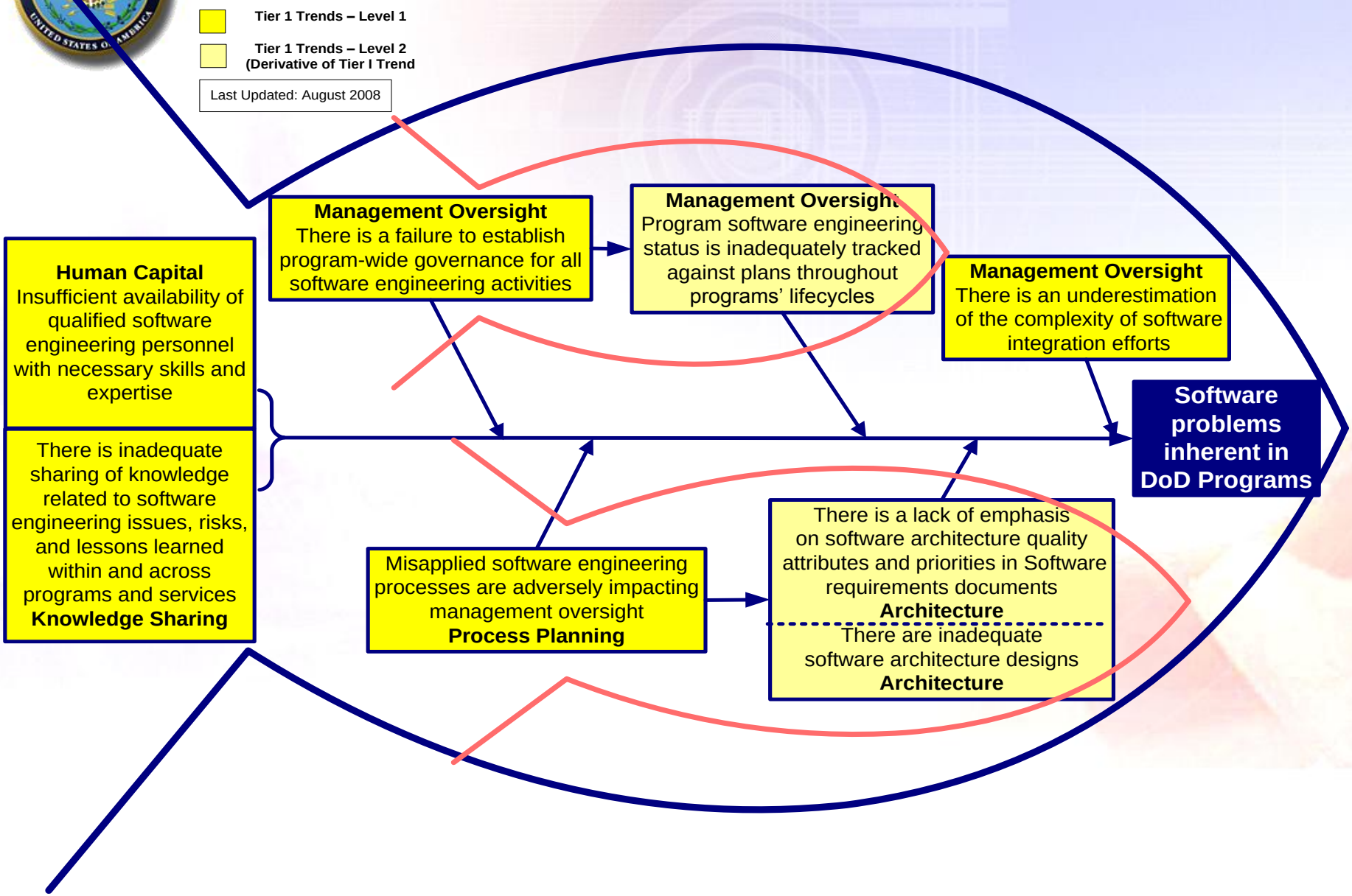
Data Validation

- Data validation was conducted to:
  - Remove any extraneous records from the resulting report unrelated to SW
  - Ensure that positive, neutral, and negative findings were identified properly
- Resulted in 284 Directly Software Related Findings

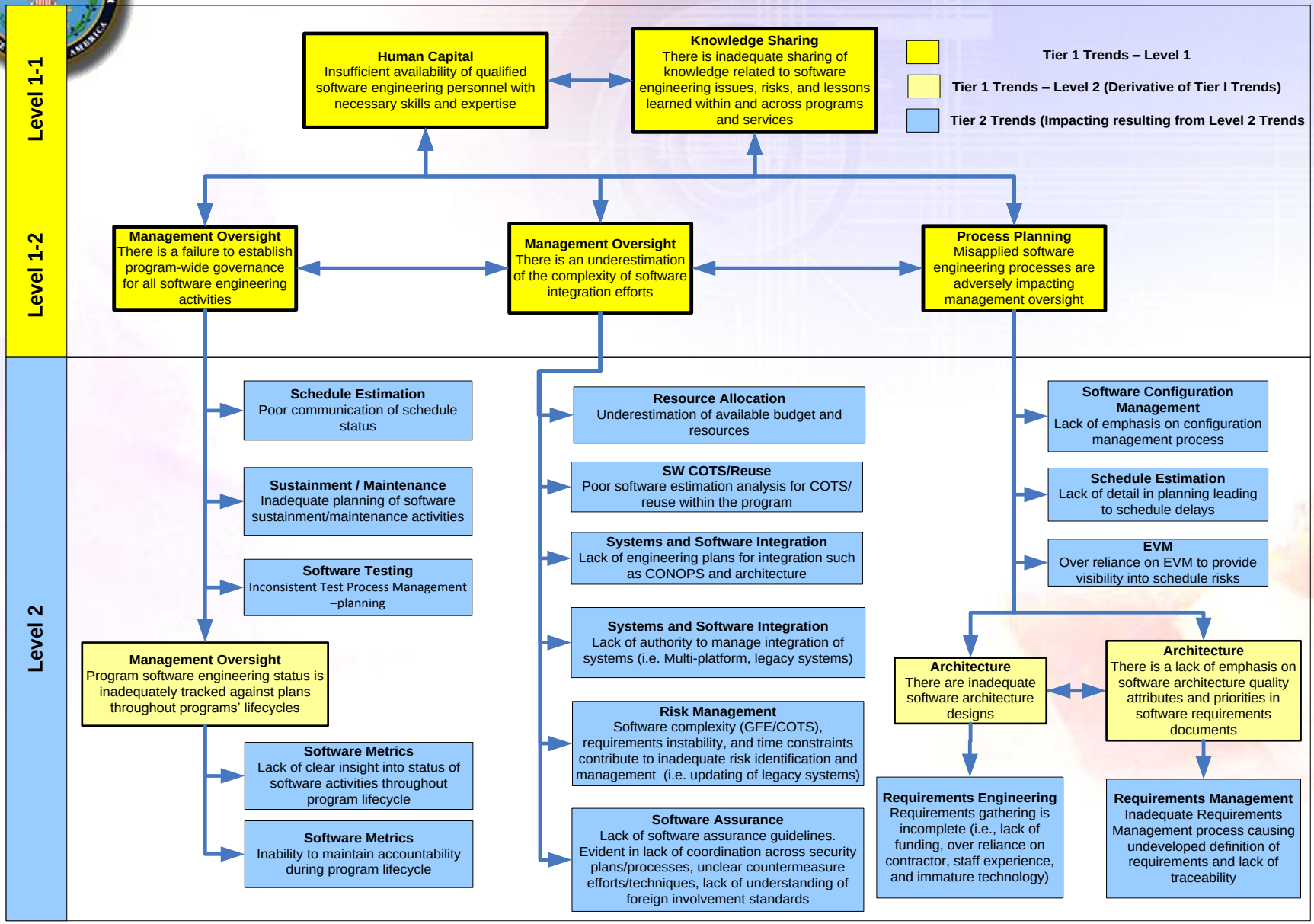


We examined these software findings without a predefined taxonomy in order to allow issue areas and recurring trends to emerge

What leads to Software Problems in DoD Programs?



Detailed Results of Overarching Trends



NDIA/DUSD(A&T)SSE Issues Validation

National Defense Industrial Association (NDIA)
Top 7 Software Issues
August 2006

- Software Human Capital
- Software Requirements
- Systems/Software Integration
- Software Assurance
- Software Testing
- Software Sustainment
- Software COTS/NDI

DUSD(A&T) SSE Directorate
Program Review Software Systemic Analysis Findings

- **Software Human Capital**
  - Resources
  - Quality Level
- **Software Requirements**
  - Engineering
  - Management
  - Acquisition Strategy
- **Systems/Software Integration**
  - Systems of Systems
  - Interoperability
  - Tech Refresh
- **Software Assurance**
- **Software Development**
  - Software Testing*
  - Software Sustainment/Maintenance*
  - Software COTS/NDI*
  - Technology Readiness
  - Software Architecture
- **Software Metrics**
  - Software Metrics
  - EVM
- **Software Engineering Management**
  - Project Planning
  - Management Oversight
  - Software Configuration Management
- **Knowledge Sharing**
  - Process
  - Reporting

SW Roundtable Results

- Shared Army, Navy, Air Force software strategies
  - Found synergy in many areas
- Identified/prioritized 22 proposed initiatives to tackle software issues – Top 5 of these:
  - Synergize/Harmonize "core SW metrics" across DoD; develop approaches for incorporating them into gate reviews, processes, earned value
  - Organize start-up teams and infrastructure to facilitate software program success
  - Establish SE/SW architecture "review board" to engage early with programs and provide constructive suggestions
  - Define analysis process for reuse/reusable assets to improve estimation accuracy; including consideration of product features
  - Develop approaches for SW testing and evaluation to enable mission success

ODUSD(A&T) SSE/SSA Way Forward

- Goal: Prosecute top software and assurance issues
- SSA FY08/09 Activities:
  - SW Lifecycle Touchpoints: SW guidance to complement Enhanced SE and SE Technical Reviews
  - SW Human Capital Strategy: Graduate-level and DoD acquisition workforce software curricula
  - SE/SW Integration: Design a framework to define and measure integration. Partnership with academia, industry
  - SW Measurement: Guidance on collection and use of SW Data
  - SW Test, SW Reliability: New in FY09
  - System Assurance: SA Guidebook; Program Protection Policy/Guidance, DIB Cyber Security Strategy

DoD SW Community Way Forward

- Review all initiatives to determine opportunity for collaboration/augmentation
  - DoD Software Working Group
  - NDIA Software Expert Panel
- Discuss plans for individual initiatives (top 5) on Collaborator teleconferences
- Organize collaborator events for FY09
  - Focused working groups/workshops as appropriate
- Continue to increase software visibility in NDIA SE Conference
  - Plan event for FY09

Increased Priority for System Assurance

- *Threats*: Nation-state, terrorist, criminal, rogue developer who:
  - Gain control of IT/NSS/Weapons through supply chain opportunities
  - Exploit vulnerabilities remotely
- *Vulnerabilities*: All IT/NSS/Weapons (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*: Stolen critical data & technology; corruption, denial of critical warfighting functionality

System Assurance is the confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted during the lifecycle

Program Protection - The Road Ahead

- DoD System Assurance
  - Evolved from Software Assurance Efforts
  - Creates a ‘framework’ to integrate multiple security disciplines and policies
  - Leverages 5200.39: expanding CPI definition to include system assurance and total life cycle
- DoDI 5200.39 CPI: Three Categories of CPI:
  - Information, Technology, Components
- Programs will
  - Define CPI at Milestone A
  - Develop a Program Protection Plan (PPP) for Milestone B
  - Be Subject to Review and Oversight
  - Execute mitigation strategies (such as use of Trusted Foundries or Anti-Tamper)

Engineering for System Assurance

- "Engineering for System Assurance" V1.0 Guidebook signed out at NDIA October 1, 2008
- Posted on SSE Web site at:
  - http://www.acq.osd.mil/sse/ssa/guidance.html
- Provides guidance on how to address System Assurance through Systems Engineering processes
  - Aligns to DoD acquisition lifecycle processes with actionable criteria
  - Adds emphasis to ISO/IEC 15288 SE processes
- Enhanced IA focus and alignment with current processes
  - Focus on hardware, software and operational environment
  - Dovetails with Program Protection Planning (PPP) processes
  - Supports identification of trusted foundry resources
  - Informs Anti-tamper considerations

Expanding DoD Industry Partnership

- Acquisition Cyber Security is a long term interest for DoD
  - Fully anticipating Cyber Security is expected to be a ongoing priority for the new administration
- DoD will continue to take advantage of the global marketplace and COTS solutions
  - Engineering for System Assurance seeks to identify and fortify critical components allowing
- Industry is part of the solution
  - NDIA System Assurance Committee will continue to focus on the solution strategy
  - ITAA, GEIA, INCOSE, others all participate on this committee

Questions