Discussion of Engineering in Depth for SwA Breakout report Out

Ken Hong Fong
Chuck Johnson
OUSD(AT&L), Defense Systems
Systems Engineering/Enterprise Development
ekenneth.hongfong@osd.mil; (703) 695-0472
chuck.johnson.ctr@osd.mil; (703) 602-0851 X123

Mitch Komaroff
OASD(NII) ODCIO
mitchell.komaroff@osd.mil
703-602-0980 x146

Participants

Name	Affiliation	email
Baldwin, Kristen	OUSD(AT&L) DS/SE	kristen.baldwin@osd.mil
Bourquin, Rene	GDC4S	rene.bourquin@gdc4s.com
Carpenter, Peter	SAIC	peter.carpenter@saic.com
Doohan, Brad	DCMA HQ	bradley.doohan@dcma.mil
Frisina, Joseph	BAE Systems	joseph.frisina@baesystems.com
Goertzel, Karen	BAH	goertzel_karen@bah.com
Hong Fong, Ken	OUSD(AT&L) DS/SE ED	ekenneth.hongfong@osd.mil
Johnson, Chuck	OUSD(AT&L) DS/SE AS	chuck.johnson.ctr@osd.mil
Keeler, Kristi	SEI	kkeeler@sei.cmu.edu
Komaroff, Mitchell	OASD(NII)	mitchell.komaroff@osd.mil
Liu, June	SAIC	liujh@saic.com
Nash, Sarah	IDA	nash@ida.org
Patel, Raju	USAF	kalabhai.patel@wpafb.af.mil
Redwine, Sam	JMU	redwinst@jmu.edu
Rose, Dan	SAIC	rosedj@saic.com
Steffey, Raymond	NGC	ray.steffey@ngc.com
Wheeler, David	IDA	dwheeler@ida.org

Sensitivity Analysis

- Q1, 1 What functional statements in the SOW for vendors best enable optimal vendor solutions to require Sensitivity Analysis
  - UK MoD "Assurance Case"
    - Claim
    - Arguments
    - Case
  - SOW crafted to explicitly call out SwA
    - Due diligence on getting "assurance statements" including a description of methodology
    - For integrators: methodology for integration considerations for SwA
    - ID, assess risks (consequence, probability)
    - Provide us with your "SwA Plan"
    - SOW language maybe too early to predict architecture
    - Could request in RFP a high level design concept (with conceptual "key components) for proposal
    - Include "checklist" in RFP (developers and integrator) to ensure "apple-to-apples" comparison
      - ID's critical components and approximate characteristics
      - Ounce Labs SOW Model
      - Application Development "STIG" from DISA
  - An overarching set of domain tailorable language might be useful
  - Where design is insufficiently developed ensure evidence of past performance
  - Vendor responses based on/commensurate with customer focus, e.g., SwA
    - E.g., if specify "Unit Test" will do whether most effective (including cost) or not
  - Propose Integrating currently "stovepipe" processes, i.e., IA, AT, C&A, into a comprehensive "Systems Assurance" function

Bottom Line: Determination of how to craft SOW with respect to degree/character of detail should be tailored to domain

Discussion on cost for Sensitivity Analysis

- Concern expressed that too much SOW guidance will be costly
- Sensitivity Analysis will likely add ~3% to design
- Analysis step should be something vendors are already doing as a part of SE
- Vendors cannot do what is not in contract
- Having trained people is overhead cost
- If government wants SwA, it need to specify contractually
  - Vendors will associate price
  - NSA estimates ~8% additional cost for IA over the lifecycle
  - NASA estimates 10-30% additional cost for IV&V

Sensitivity Analysis…

- How do we address n-tiered subcontracting, including COTS, where specific product mixes change significantly?
  - » Make the Prime responsible for securing necessary statements of assurance from subs/suppliers
    - Put language to that effect in Prime's contract with Subs/suppliers
    - Need to have mechanisms to ensure legitimacy of claims
    - Cannot impose requirements on COTS products, but can use as criteria for selection decision
    - Can ask for a risk management plan:
      - Where criteria not met, decision must be raised to PM/Prime level
      - Prime might ask subs for their RMP

Bottom Line: Responsibility on Primes, with emphasis on Risk Management Plan(s)

Sensitivity Analysis

- How do we measure and manage subsequent trade decisions through the product lifecycle?
  - Require updates to software assurance case
  - Should be part of standard SE processes
  - Going down path that may be too costly.
    - Proof that of good origin different than evidence that not of bad origin
  - Only applies to “critical components” “as well as reasonably practical”
    - Unacceptable still unacceptable – criteria needed
  - Set criteria for event related reviews (not necessarily formal “Design Reviews”)
  - Contractual agreement on required critical and supporting artifacts
    - May not get support for COTS vendor if not leveraged with sales volume/value
    - But…if critical enough, may be needed and a selection criteria
    - Wording that requires integrator to do SwA testing
  - Over time will be a cumulative influence on vendor behavior in general

Bottom Line: Assurance Case for Sensitivity Analysis must stay current throughout lifecycle ~inculcated practice over time

Sensitivity Analysis

- How do we execute this at different phases in the product lifecycle?
  - Deltas across life-cycle phases
  - Should ideally maintain assurance case throughout lifecycle
  - Should establish mechanisms to ID conditions when assumptions change
  - Successful projects embrace a team concept with PM, prime, subs and suppliers
    - Need qualified/ SwA knowledgeable people in PM office
    - Need SME base in PMO

Bottom Line: Responsibility on Primes

Requirements

- What functional statements in OSD Guidance for SwA requirements best enable optimal vendor solutions?
  - Require higher level written policy to specify need for SwA requirements
  - "Compelling arguments and evidence that…commensurate with risk"
  - Written SwA Principles in policy
    - Looked at 8500, 5000.2, 5000, 3170, 6212, …
    - In 8500.2 Annex language to potentially leverage for SwA:
      - "…use IA best practices…,"
      - "…software will be well behaved…"
      - Point to language in contracts
    - Contract language to show equivalence to ISO 15026 practices
    - Burden on PMO to understand and have confidence in level of SwA
    - Requirement in policy that whenever a new risk is ID's or an old risk changes, contractor must be notified

TEST

- What functional statements in the SOW for vendors, OSD test guidance best enable optimal vendor solutions
  - Should be linked to assurance case
  - Incorporate assurance case in TEMP
  - Ensure that if not specified in requirements, can do risk based testing and not just requirements based testing (i.e., “in operationally representative environment”)
  - Testing must be coordinated with certification, accreditation activities
    - SSAA with TEMP linkage
    - Assurance case, including evidence, must be adequate to pass certification
    - Iterative throughout lifecycle
    - Should include static analysis
      - Execution testing is just one kind of evidence
      - Classic end state too late
    - Requirements analysis process is key
      - Recursive sensitivity analysis
      - VV&A
      - IV&V
      - M&S
      - C&A…
    - Security requirements mainly about properties less towards functionality
      - Statements of constraint

Hazard Analysis

- What functional statements in the SOW for vendors and in OSD guidance best enable optimal vendor solutions for ID and Assessment of SwA hazards
  - Must set acceptable risks, consequences
  - Can capture in standard/standard set for SOW
  - Need to have consistent definitions for contracts
  - Source/origin of software should not be a determinant factor for assurance level; should be based on evidence of SwA properties
  - Concept of trusted 3rd party, e.g., reviewer escrow should be considered
    - Gold disk concept