An Architecture of IA Processes

Jackson.Wynn@INCOSE.org

This essay considers an architectural model comprised of Information Assurance (IA) processes. I use the term *IA process architecture* to refer to an aggregation of processes whose objective is to ensure and promote the secure development and operation of an information system. The objective of this essay is to show how the application of architectural principles and best practices to process architecture can lead to process improvement. While the focus of this essay is on IA processes applied to the acquisition of information systems for the Department of Defense (DoD), the application of architectural modeling advocated in this paper has general value to systems engineers and can be used to facilitate process improvement in other contexts as well.

A system's architecture constantly evolves, and one approach for evaluating architecture is to compare it with what it either has been in the past or could be in the future. I refer to these as the "As-Is" and "To-Be" architecture, respectively. My intent is to show how this standard approach for looking at architecture can be applied to process architectures as well.

This essay begins with a discussion of processes, dependencies, and process aggregates. This is followed by a discussion of general architectural principles, including stratification, cohesion, and loose coupling as they apply in the context of process architectures. I then perform an analysis of the “As-Is” IA process architecture currently used in Department of Defense (DoD) acquisition programs, and outline a “To-Be” IA process architecture that addresses identified discontinuities. Funding to write this essay was provided by my employer, the MITRE Corporation, and is not intended to convey or imply MITRE’s concurrence with, or support for, the positions, opinions or viewpoints expressed herein.

Processes

Webster defines a process as “a series of actions or operations conducing to an end.” In this context, the end refers to the process’s intended goal or objective. A process is also defined by a number of additional properties or characteristics, which include:

- A methodology or planned sequence of tasks
- A process owner and/or process stakeholder(s) who define and implement the process
- Process inputs, which include information, resources, funding, etc.
- Process outputs, which include work products, artifacts, etc.
- The current cost, schedule, and performance “state” of a process being executed
- The effect or actual result of the process once executed

These characteristics of a process are graphically depicted in Figure 1.

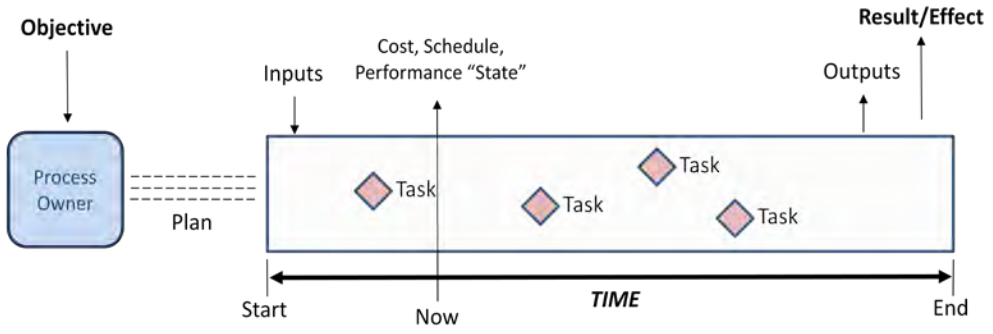

Figure 1. The process execution model

Process Architectures

Process architectures are compositions of processes that have similar or aligned objectives and share information. Processes that share information form dependencies where an output of one process is a required input to another process, either triggering its execution or providing it with required information. The alignment of processes within a process aggregate, whether serial, nested, or staggered, depends on the process dependencies within that aggregate. Arbitrarily complex process architectures can be composed by combining process aggregates, as illustrated in Figure 2 below.

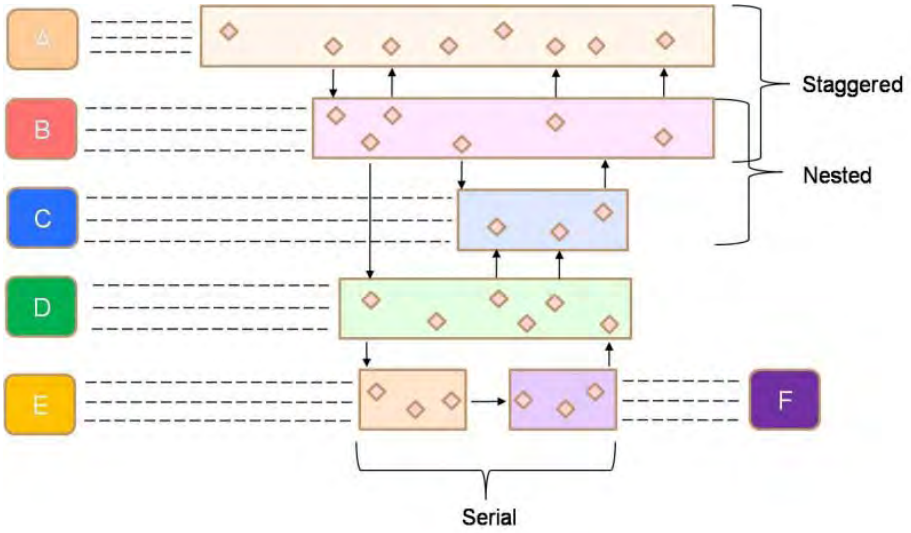

Figure 2. Complex process architecture constructed from process aggregates

For purposes of this discussion, one objective of architecture is to define a system boundary that contains architectural elements that allow for the allocation of requirements within that system boundary. In the context of process architecture, the system boundary corresponds to a business enterprise, architectural elements correspond to individual processes developed and executed within that enterprise, and requirements correspond to the business objectives those processes are intended to satisfy.

One basis for evaluating the maturity of any architecture is by assessing how well it achieves this objective. Architectures mature through the elimination of requirement gaps and overlaps in the

allocated baseline, and by maximizing cohesion while minimizing coupling between architectural strata. In the context of process architecture, a gap results when a process has a "missed step," while an overlap results when there is duplication of effort. Cohesion is achieved through the common alignment of process objectives. Loose coupling is achieved by minimizing dependencies among processes within the architecture, with the fair expectation that this will reduce the likelihood that a change in one process will force a change in another process.

The "As-Is" IA Process Architecture

The "As-Is" IA process architecture considered in this paper is comprised of six (6) IA processes, detailed below, which are performed in association with a standard process framework used for DoD acquisitions, as defined by DoD directives 5000.1 and 5000.02. The reader is referred to these documents for more information on the DoD acquisition process.

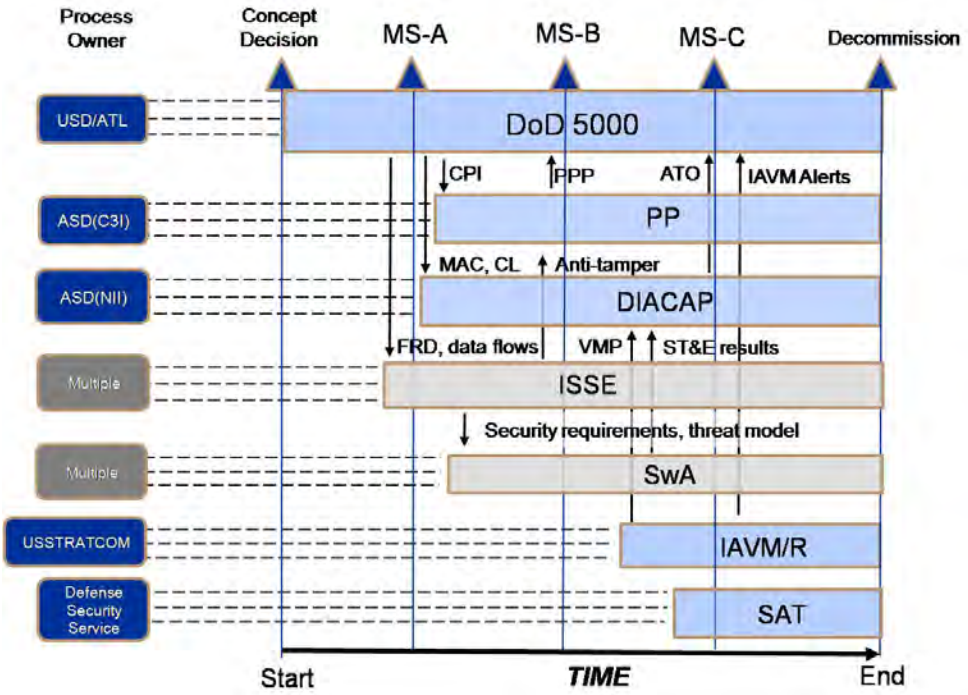

Figure 3. The "As-Is" IA process architecture for DoD system acquisitions

Program Protection (PP)

The objective of Program Protection is to protect critical information, technology, and resources used in the development, deployment or operation of a weapons system from being compromised over the development and operational life of that system. This process is defined by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I), and is documented by DoD 5200.1-M "Acquisition Systems Program Protection", and DoD 5200.39 "Critical Program Information (CPI) Protection within the Department of Defense."

DoD Information Assurance Certification and Accreditation Process (DIACAP)

The objective of DIACAP is to manage the implementation of IA capabilities and provide a basis for certification and accreditation decisions regarding the operation of DoD Information Systems. This process is defined by the Assistant Secretary of Defense for National Information

Infrastructure (ASD/NII), and documented in DoD 8510.01 “DIACAP” and DoD 8500.2 “Information Assurance Implementation.”

Information Security Systems Engineering (ISSE)
The objective of ISSE is to apply security engineering principles and techniques to the Systems Development Life Cycle (SDLC). There is no DoD-defined, standard ISSE process. However considerable guidance is available both commercially and from government sources that include National Institute for Science and Technology (NIST) Special Publications (SP), such as NIST SP 800-27 “Engineering Principles for Information Technology Security”.

Software Assurance (SwA)
The objective of SwA is to ensure that software functions in its intended manner and is free of vulnerabilities. There is no DoD-defined, standard SwA process. However considerable guidance is available from government sources that include the Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG), and the Data and Analysis Center for Software (DACS) publication “Enhancing the Development Life Cycle to Produce Secure Software."

Incident and Vulnerability Management/Response (IAVM/R)
The objective of IAVM/R is to manage and respond to security incidents and discovered vulnerabilities over the operational life of a deployed system. This process is defined in CJCSI 6510.01E “Information Assurance (IA) and Computer Network Defense (CND)”, which specifies requirements for DoD systems to incorporate incident handling and vulnerability management capabilities.

Security Awareness Training (SAT)
The objective of SAT is to ensure that personnel are trained to make appropriate security decisions. This process is discussed in DoD 3305.13 “DoD Security Training”, which assigns overall responsibility to the Defense Security Service (DSS).

Strengths of the As-Is IA Process Architecture
The As-Is IA process architecture includes processes that use common terminology and have well-defined objectives, inputs, outputs, and outcomes. DIACAP, for example, takes as input a system’s Mission Assurance Category (MAC) and Confidentiality Level (CL), and produces as an outcome a favorable accreditation decision, namely an Approval to Operate (ATO). Additionally, DoD-defined processes integrate into the DoD 5000 acquisition process at established milestones. For example, DIACAP must achieve an IATO accreditation before operational testing and evaluation (OT&E) can commence, sometime around Milestone C.

Discontinuities with the As-Is IA Process Architecture
While DoD-defined processes have well-defined inputs and outputs, dependencies among these processes are not always identified by DoD directives, which can lead to confusion about how these IA processes align with one another. For example, DIACAP discusses responsibilities for vulnerability management but not specific requirements, which are detailed in DoD 8500.2 as IA controls VIVM-1, VIIR-1, and VIIR-2. Implementation of these IA controls is an outcome of the IAVM/R process, while DIACAP verifies compliance.

Another issue is the dependence of DoD-standard IA processes on IA processes that are not required by DoD directive, which may be incorrectly or incompletely applied by the acquisition program. Program protection, for example, may require anti-tamper capabilities, which are a by-product of the security engineering process. A program manager may not recognize the dependence of program protection on anti-tamper analysis and security engineering, and regard it to be out of scope for the acquisition program.

What is not explicitly defined by DoD directive is considered guidance, and guidance from multiple sources may have gaps and/or overlaps. The problem with guidance gaps is that guidance may not fully address the need, while guidance overlaps may be in conflict. Guidance gaps may result when non-DoD guidance does not address DoD-specific needs. For example, mission criticality characterizes the degree to which a system supports the warfighter. A DoD-defined software assurance process would specify whether IV&V is required for a system based on its mission criticality. Non-DoD software assurance guidance might not make this distinction.

Guidance overlaps can also lead to duplication of effort. An example of this can be attributed to the lack of uniform terminology distinguishing between mission assurance, system assurance, software assurance, and information assurance. Does a DoD acquisition program need to apply all of these processes in order for assurance to be achieved?

A "To-Be" IA Process Architecture

The following "To-Be" IA process architecture attempts to address some of these discontinuities. This IA process architecture consists of five (5) IA processes performed concurrently with the DoD 5000 framework, as depicted by Figure 5.

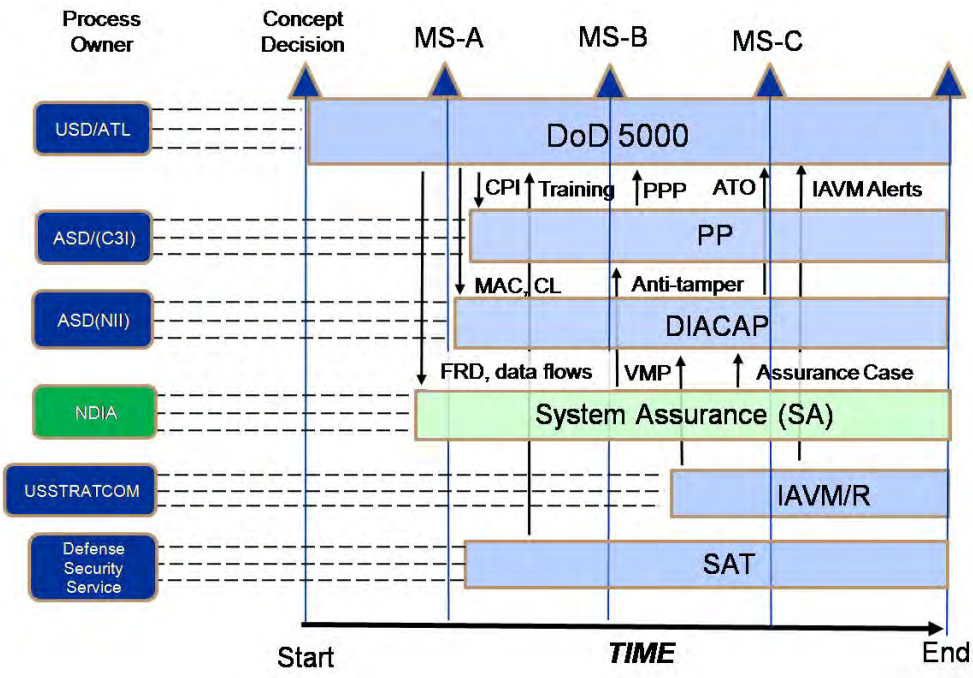

Figure 4. A "To-Be" IA process architecture for DoD system acquisitions

The System Assurance (SA) Process
In this IA process architecture, security engineering and software assurance processes are combined into a single, DoD-standard process called System Assurance (SA). The objective of the SA process is to integrate security engineering, hardware and software assurance, and trusted supply chain activities spanning the entire system life cycle. The SA process is detailed in a recently-published National Defense Industry Association (NDIA) guidebook entitled "Engineering for System Assurance," which is endorsed by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD/ATL). This endorsement by USD/ATL means that DoD acquisition programs are free to use the NDIA guidance, but that its use is not required.

Security Awareness Training for Systems Developers
A second change proposed by the "To-Be" IA process architecture is for security awareness training to start earlier in the system development lifecycle with training geared towards engineering personnel engaged in the design and implementation of DoD systems. Acquisition programs would generally benefit from systems engineers receiving training in security engineering principles and best practices. Along the same lines, my hope is that DoD program managers who read this paper will have a better awareness of the IA processes that come into play in their acquisition programs.

References

Stoneburner, G., C. Hayden, A. Feringa, 2004, NIST SP 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)," Washington, DC: U.S. Department of Commerce, http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

Data and Analysis Center for Software (DACS), 2008, "Enhancing the Development Life Cycle to Produce Secure Software," https://www.thedacs.com.

National Defense Industry Association (NDIA), 2008, "Engineering for System Assurance," Version 1.0, http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf.

Department of Defense (DoD), 2007, DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," Washington, DC: Office of the Assistant Secretary of Defense for (Networks & Information Integration), http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.

Chairman of the Joint Chiefs of Staff, 2007, CJCS Instruction 6510.01E, "Information Assurance (IA) and Computer Network Defense (CND)," Washington, DC: Joint Staff (J-6), http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.

DoD, 2003, DoD Directive 5000.1, "The Defense Acquisition System," Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.

DoD, 2008, “DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.

DoD, 1994, DoD 5200.1-M, “Acquisition System Program Protection,” Washington, DC: Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, http://www.dtic.mil/whs/directives/corres/pdf/520001m.pdf.

DoD, 2003, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” Washington, DC: Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.

DoD, 2008, DoD Instruction 5000.39, “Critical Program Information (CPI) Protection within the Department of Defense,” Washington, DC: Office of the Under Secretary of Defense for Intelligence, http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf.

Defense Information Systems Agency, 2008, “Application Security and Development Security Technical Implementation Guide,” Version 2 Release 1, Washington, DC: Department of Defense, http://iase.disa.mil/stigs/stig/application_security_and_development_stig_v2r1_final_20080724.pdf.