System and Software Technology Conference 2007

Mission Assurance-Driven Processes for Software-Intensive Systems

Suellen Eslinger
The Aerospace Corporation

June 19, 2007

THE AEROSPACE CORPORATION

Mission Assurance Definitions

- **Mission Assurance: the disciplined application of general systems engineering, quality, and management principles towards the goal of achieving Mission Success, and, towards this goal, provides confidence in its achievement**

- **Mission Success: the achievement by an acquired system (or system of systems) to singularly or in combination meet not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability and supportability**

The Mission Assurance Problem for Software-Intensive Systems

- **NSS system acquisition failures attributable to software continue to mount, especially for the large, software-intensive systems**
  - Performance deficiencies
  - Extensive software defects
  - Large, unanticipated cost and schedule overruns
- **These failures contribute to a lack of mission success for these critical national security programs**
- **However, many of the development contractors for these space systems advertise high maturity levels**
  - Levels 3, 4 and 5 when appraised against the Capability Maturity Model® Integration℠ (CMMI®)

The Mission Assurance Problem for Software-Intensive Systems

- **NSS system acquisition failures attributable to software continue to mount, especially for the large, software-intensive systems**
  - Performance deficiencies
  - Extensive software defects
  - Large, unanticipated cost and schedule overruns
- **These failures contribute to a lack of mission success for these critical national security programs**
- **However, many of the development contractors for these space systems advertise high maturity levels**
  - Levels 3, 4 and 5 when appraised against the Capability Maturity Model® Integration℠ (CMMI®)

Process Improvement Using the CMMI®

- The CMMI® is a generic model, designed to be useful for process improvement in all product domains and for multiple disciplines (e.g., systems engineering, software engineering)
- Therefore, the CMMI® provides great latitude in how its expected practices can be implemented to meet its stated goals
- In Levels 4 and 5, process improvement is based on "quality and process performance objectives", which are driven by the organization's business objectives*

* "CMMI® for Development, Version 1.2 (CMMI-DEV, V1.2)", CMU/SEI-2006-TR-006, August 2006. See, for example, pp. 91, 92, 198, 261, 364, 536, and 552.

CMMI® Process Areas Needed for Mission Assurance for Software-Intensive Systems

- **The principal CMMI® process areas (PAs) needed for mission assurance consist of the following Level 2 and 3 PAs:**
  - Engineering
    - Requirements Management, Requirements Development, Technical Solution, Product Integration, Verification, Validation
  - Support
    - Configuration Management, Process and Product Quality Assurance
  - Project Management
    - Risk Management, Supplier Agreement Management
- **However, mission assurance goes well beyond the CMMI® expected practices in these PAs!**
  - **Processes also need to be effective in producing high quality products that will not require significant downstream rework**
- **CMMI® Level 4 and 5 process areas are not required to achieve mission success**
  - Level 4 and 5 can certainly help, but only if the organization's "quality and process performance objectives" are targeted to mission assurance

Software Mission Assurance

- **This briefing will focus on two sets of processes that are essential for software mission assurance:**

1. **Conducting a robust software test program**
   - ❖ Focused on finding defects that escaped the quality gates for earlier software development activities

2. **Building quality in** throughout the entire development life cycle
   - ❖ Using techniques focused on finding and removing defects within each development activity
   - ❖ Example techniques: peer reviews, product evaluations, joint technical reviews and software quality assurance audits

Key Mission Assurance-Driven Processes

1. Testing* Activities

- Software unit testing
- Software integration testing, including
  - Software unit integration testing
  - Software/hardware integration testing
  - Both within and across software items
- Software qualification testing

2. Quality-Enhancing Activities

- Peer reviews
- Product evaluations

* The word “testing” in this presentation includes the use of all verification methods (i.e., I, A, D, T, S)

Software Unit Testing

CMMI®

- **Software unit testing NOT required or even expected**
  - Subpractice 4 in the Technical Solution PA under the expected practice SP 3.1: "Implement the designs of the product components" states "Perform unit testing of the product component as appropriate"**
  - Subpractices are part of the informative material (not required or expected)

** All quotations from the CMMI® in this presentation are taken from the following reference:

"CMMI® for Development, Version 1.2 (CMMI-DEV, V1.2)", (CMU/SEI-2006-TR-006), August 2006.

Mission Assurance

- **Software unit testing required for each software unit**
- **Exit criteria specified for unit testing, e.g.,**
  - All statements and branches
  - Error and exception handling
  - Interfaces, including boundary and limit conditions
  - Algorithms
- **Required regression testing of affected unit test cases for all changes to previously tested software**
- **Conditions specified for unit testing of reuse software, e.g.,**
  - If any changes made
  - If poor track record
  - If critical function

Software Integration Testing

CMMI®

- **Addressed by three expected practices in the Product Integration PA**
  1. SP 1.3: "Establish and maintain procedures and criteria for integration of the product components"
  2. SP 3.2: "Assemble product components according to the product integration sequence and available procedures"
  3. SP 3.3: "Evaluate assembled product components for interface compatibility"
- **Software integration testing not explicitly required**

Mission Assurance

- **Software integration testing required**
  - ❖ On target hardware, under conditions as close to operations as possible
- **Exit criteria specified for software integration testing, e.g.,**
  - ❖ Interfaces, including limits and boundary conditions
  - ❖ Integrated error and exception handling
  - ❖ End-to-end functional capabilities
  - ❖ Start up, termination, restart
  - ❖ Verification of software requirements allocated to the integrated units
  - ❖ Performance testing; stress testing
  - ❖ Fault detection, isolation and recovery
  - ❖ Resource utilization measurement
- **Required regression testing of affected software integration test cases for all changes to previously tested software**
- **Software integration testing of Commercial Off-the-Shelf (COTS) and reuse software required**

Software Qualification Testing

CMMI®

- **Addressed by four expected practices in the Verification PA**
  1. SP 1.1: "Select the work products to be verified and the verification methods that will be used for each"
  2. SP 1.3: "Establish and maintain verification procedures and criteria for the selected work products"
  3. SP 3.1: "Perform verification on the selected work products"
  4. SP 3.2: "Analyze the results of all verification activities"
- **Software qualification testing not explicitly required**

Mission Assurance

- **Software qualification testing required**
  - On a target hardware configuration, as close to operations as possible
  - Operational data rates, databases/data constants, workloads, scenarios
- **Exit criteria specified for software qualification testing, e.g.,**
  - Verification of all sw requirements
  - Verification of all sw interface requirements (using actual I/Fs or high fidelity simulators)
  - Verification of all sw specialty engineering requirements, especially sw reliability and fault detection, isolation and recovery
  - Stress testing, including worse case scenarios
  - Resource utilization measurement
  - Verification of all software requirements allocated to COTS and reuse (modified or unmodified) software
- **Required regression testing of affected software qualification test cases for all changes to previously tested software**

Peer Reviews

CMMI®

- **Addressed by three expected practices and one goal in the Verification PA**
- **Goal: "Peer reviews are performed on selected work products"**
- **Expected Practices:**
  - SP2.1: "Prepare for peer reviews of selected work products"
  - SP 2.2: "Conduct peer reviews on selected work products and identify issues resulting from the peer review"
  - SP 2.3: "Analyze data about preparation, conduct and results of the peer reviews"
- **Peer reviews on software work products not explicitly required**

Mission Assurance

- **Peer reviews of all sw work products from mission assurance-critical PAs required**
- **Specific requirements include, e.g.,**
  - Identifying type of peer review
  - Identifying mandatory key reviewers
  - Ensuring entry criteria met
  - Reviewing materials by each reviewer before the meeting
  - Using standard checklists for each type of product
  - Identifying and documenting defects and other issues
  - Recording results of peer review, including action items
  - Ensuring exit criteria met
  - Analyzing data about preparation, conduct and results of the peer reviews
- **Strict guidelines on maximum amount of material that can be reviewed and on preparation and meeting times**
- **Integrated into all participants' schedules**

Software Product Evaluations

CMMI®

- **Software product evaluations NOT explicitly addressed**
  - The Verification PA addresses ensuring that selected work products meet their specified products
  - However, only peer reviews are required
  - All other examples of verification methods for software are types of testing (informative material)

Mission Assurance

- **In-progress and final software product evaluations required for major software products (e.g., requirements, architecture, design, test, operations products)**
- **Criteria specified for each type of software product, e.g.,**
  - Adequate, accurate, consistent, complete, feasible, testable, understandable
  - Meets requirements (technical and contractual)
  - Follows Software Development Plan, including Standards and Procedures
- **Independence in software product evaluation required**
  - Technically cognizant people who are not the developers of the product

Advice for Development Organizations With Customers to Whom Mission Success is Important

- **Some customers required a high degree of mission assurance for their programs (e.g., NSS)**
- **The processes used on these programs need to be mission assurance-driven**
  - These programs need more than just mature processes (i.e., institutionalized, predictable) based on CMMI® expected practices
  - You may need to **tailor up** your organizational processes to achieve the program's mission assurance objectives
- **Better yet: Mission-assurance driven organizational processes need to be defined and deployed**
  - With guidance on the types of programs for which these processes are to be used

Advice for Acquisition Organizations to Whom Mission Success is Important

- **Make a robust software development standard contractually compliant**
  - The CMMI® is NOT a standard!
- **Require key mission assurance-related software technical deliverables**
  - ❖ e.g., software requirements, architecture, test plans, procedures and reports
- **Incentivize mission success and the use of high mission assurance processes, in order to align the development contractor's business objectives with the government's business objectives**
  - ❖ Don't just incentivize schedule!

A mission assurance-driven contract is essential for achieving mission success.

New Software-Related Standards for NSS

- **The military standard for software development (MIL-STD-498) has been updated to include explicit requirements for high mission assurance processes**
  - R. J. Adams et al, "Software Development Standard for Space Systems," The Aerospace Corporation, TOR-2004(3909)-3537 Revision B, 11 March 2005
  - Part of the USAF Space and Missile Systems Center (SMC)/National Reconnaissance Office (NRO) Mission Assurance Improvement initiative
  - Now being used as a compliance document on new SMC and NRO programs
  - The standard is not space-specific—Can be applied to any software development effort where mission assurance is a concern
- **Robust software testing requirements for space and launch vehicles have been included in an update to MIL-STD-1540 for the first time in its history**
  - Perl, E. "Test Requirements for Launch, Upper Stage, and Space Vehicles." TR-2004(8583)-1, The Aerospace Corporation, 31 January 2004.
  - Also being used as a contractual compliance document on new SMC and NRO programs

Conclusion

- Using mission assurance-driven processes is essential for mission success
- High maturity level processes are NOT the same as mission assurance-driven processes
- Both development and acquisition organizations need to take action to ensure that mission assurance-driven processes are used on their programs with critical mission success needs

Acronyms and Abbreviations

CMMI®	Capability Maturity Model® Integration℠
CMU	Carnegie Mellon University
COTS	Commercial Off-the-Shelf
DEV	Development
I, A, D, T, S	Inspection, Analysis, Demonstration, Test, Special
MIL	Military
NRO	National Reconnaissance Office
NROD	NRO Directive
NSS	National Security Space
PA	Process Area
SEI	Software Engineering Institute
SM	Service Mark
SMC	Space and Missile Systems Center
STD	Standard
SW	Software
TOR	Technical Operating Report
TR	Technical Report
U. S.	United States
USAF	United States Air Force

Speaker Contact Information

Suellen Eslinger
Distinguished Engineer
Software Engineering Subdivision
Computers and Software Division
The Aerospace Corporation
Mailing Address:

Suellen Eslinger
The Aerospace Corporation--M1/112
P. O. Box 92957
Los Angeles, CA 90009-2957

Phone: **(310) 366-2906**
FAX: **(310) 336-4070**
email: **suellen.eslinger@aero.org**

Use of Trademarks, Service Marks and Trade Names

All trademarks, service marks, and trade names are the property of their respective owners.