



# **SOFTWARE ASSURANCE FORUM**

## **BUILDING SECURITY IN**

## **Processes and Practices Working Group**

Paul Croll, CSC  
Michele Moss, BAH

October 15, 2008



# **SOFTWARE ASSURANCE FORUM**

## **BUILDING SECURITY IN**

### ***Summary of Processes and Practices Activities***

- Enhancing the Development Life Cycle to Produce Secure Software, v2.0
- Engineering for System Assurance, v1.0
- ISO/IEC/IEEE 15026, System and Software Assurance
- Assurance for CMMI



# **SOFTWARE ASSURANCE FORUM**

## **BUILDING SECURITY IN**

### ***Enhancing the Development Life Cycle to Produce Secure Software, v2.0***

- Rationale
  - Does not espouse a specific approach or philosophy.
  - Does not attempt to evaluate or critique security-enhancement approaches
  - Does provide information to help readers understand, assess, and choose from among the growing number of security-enhancing SDLC processes, methodologies, practices, techniques, and supporting tools
- Status
  - released October 3, 2008 via the Data and Analysis Center for Software (DACS)
  - A copy can be accessed via [https://www.thedacs.com/techs/enhanced\\_life\\_cycles/](https://www.thedacs.com/techs/enhanced_life_cycles/)



# SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

## *Engineering for System Assurance, v1.0*

- Rationale
  - NDIA/DoD guidebook providing process and technology guidance to increase the level of system assurance.
  - Intended primarily to aid program managers (PMs) and systems engineers (SEs) who are seeking guidance on how to incorporate assurance measures into their system life cycles.
  - Oriented to ISO/IEC 15288 “System Life Cycle Processes” and U.S. DoD Defense Acquisition Guidebook (DAG)
- Status
  - Released October 1, 2008 via the DoD SSE/SSA and NDIA web sites
  - A copy can be accessed via
  - <http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf>
  - or
  - [http://www.ndia.org/Template.cfm?Section=NDIA\\_Divisions\\_Page&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=3&ContentID=677](http://www.ndia.org/Template.cfm?Section=NDIA_Divisions_Page&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=3&ContentID=677)



# SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

*ISO/IEC/IEEE 15026, System and Software Assurance*

- Four-part standard
  - 15026-1: Concepts and vocabulary
  - 15026-2: Assurance case (including planning for the assurance case itself)
  - 15026-3: System integrity levels (a revision of the 1998 standard)
  - 15026-4: Assurance in the life cycle (including project planning for assurance considerations)

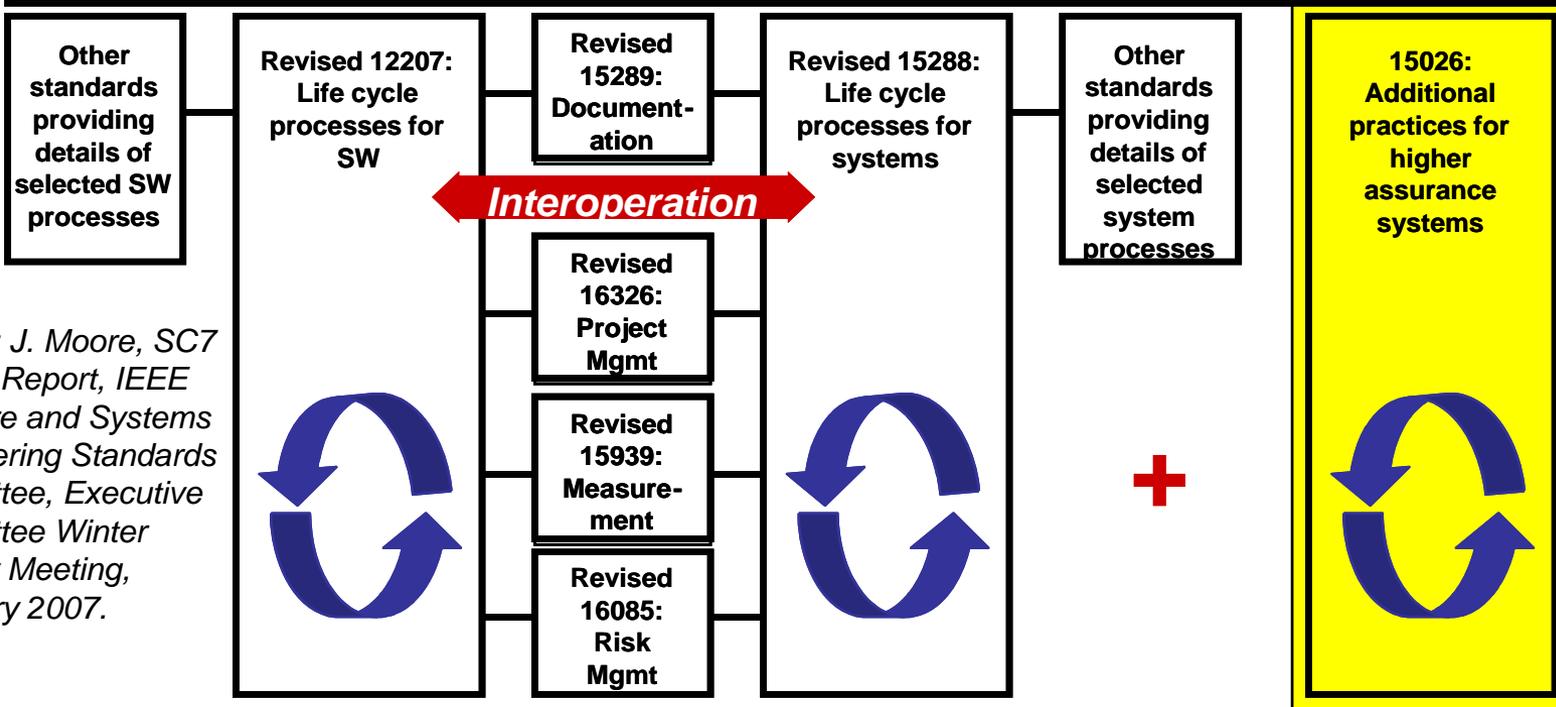


# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

### 15026 in the System and Software Life Cycles

24748: Guide to Life Cycle Management



Common vocabulary, process architecture, and process description conventions

ISO/IEC/IEEE 15026, System and Software Assurance

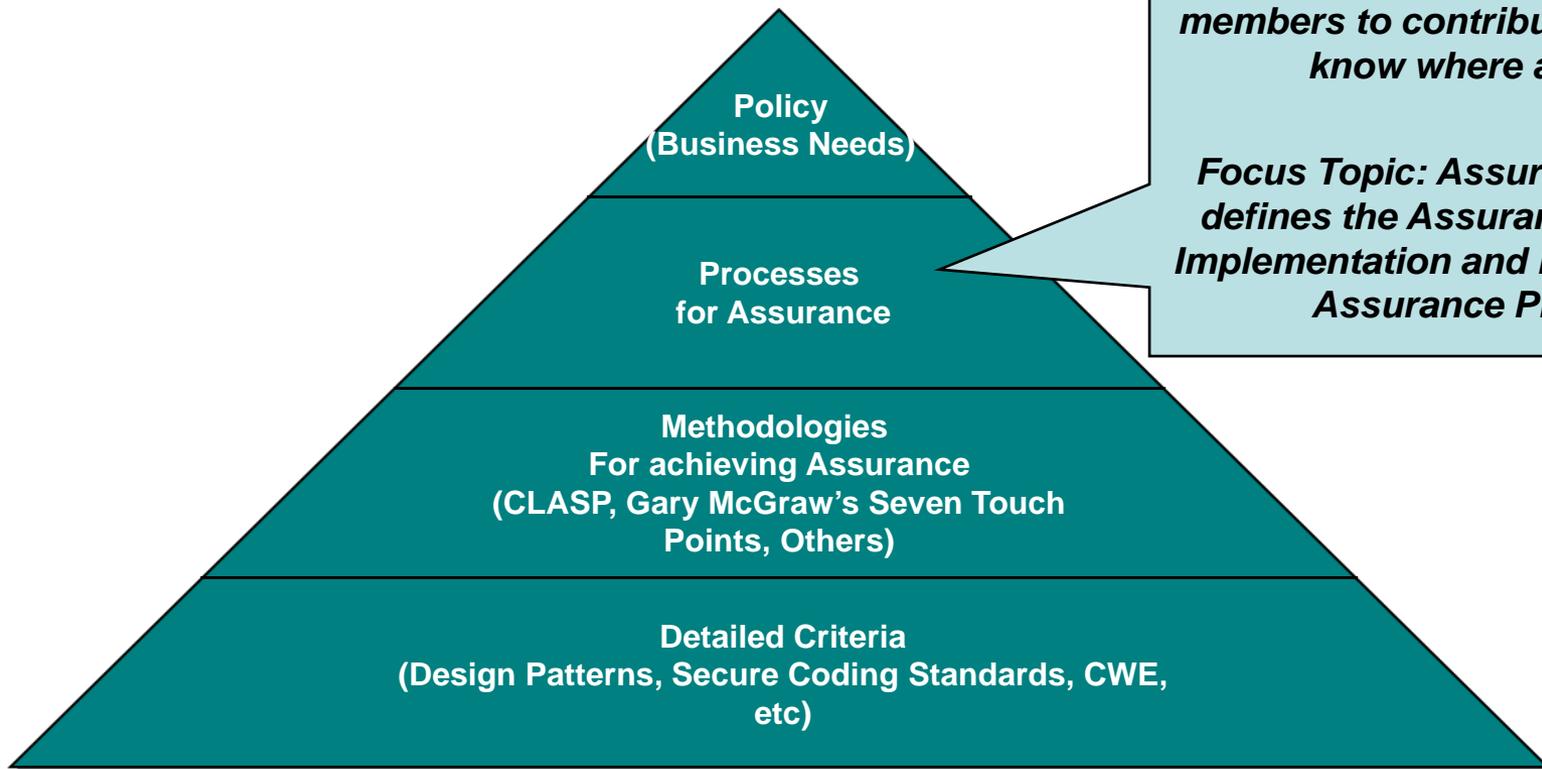
Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

### *Assurance for CMMI*



*For project leadership and team members to contribute they need to know where and how*

*Focus Topic: Assurance for CMMI defines the Assurance Thread for Implementation and Improvement of Assurance Practices*



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

### *Progress Update*

- March 2007: SEPG Birds of a Feather
- August 7, 2007: Industry Assurance for CMMI Meeting
- September 2007: Motorola, Lockheed Martin and Booz Allen form Assurance Working Group
- October 2007 – present: Assurance Harmonization Working Group
- January 2008 – present: Assurance Focus Topic Working Group
- July 16, 2008: Gained CMMI Steering Group approval to create Focus Topic for Assurance
- Today
  - Working with CMMI Architecture Team to develop a Focus Topic that documents the assurance thread through the CMMI
  - Refining practices and mapping to CMMI as necessary



# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

### *What can you do?*

- Use “Draft Practices” to identify gaps in your Assurance Practices
- Watch for updates <https://buildsecurityin.us-cert.gov/swa/procesrc.html>
- Share your Lessons Learned (swawg-process @ cert.org)



# **SOFTWARE ASSURANCE FORUM**

## **BUILDING SECURITY IN**

***For More Information . . .***

**Paul R. Croll**  
**CSC**  
**17021 Combs Drive**  
**King George, VA 22485**

**Phone: +1 540.644.6224**  
**Fax: +1 540.663.0276**  
**e-mail: [pcroll@csc.com](mailto:pcroll@csc.com)**

**Michele Moss**  
**Booz Allen Hamilton**  
**8283 Greensboro Drive**  
**McLean, VA 22102**

**Phone: +1 703.377.1254**  
**Fax: +1 703.902.3595**  
**e-mail: [moss\\_michele@bah.com](mailto:moss_michele@bah.com)**