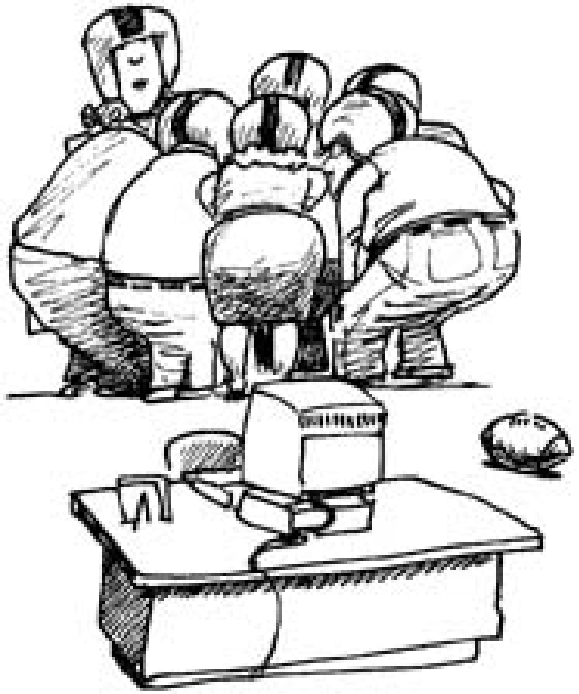
LOCKHEED MARTIN

Engineering Process Improvement Center

Lockheed Martin's Move to Assurance: Software Safety and Security Certification Best Practices (BP)



Dennis Beard, CISSP
Lockheed Martin – Syracuse, NY
August 7, 2007

Agenda

LOCKHEED MARTIN

Engineering Process Improvement Center

- **Best Practices Guidebook**
- **Context**
- **Guidebook Specifics**
- **Structure and Content**
- **Development of Guidebook**
- **Safety and Security for Integrated Capability Maturity Models**
- **Guidebook Promotion**
- **Target Audience**

CMMI® and Assurance - What Started This Discussion ???

LOCKHEED MARTIN

Dennis Beard leads an internal LM SW Subcouncil WG relating to SW Safety and Security certification. This group produced a corporate-wide SW Certification Best Practices (BP) Guidebook.

In November 2006, presented the BP to a joint meeting with the SW Engineering Institute (SEI) and the Corporate VP for Engineering and his staff.

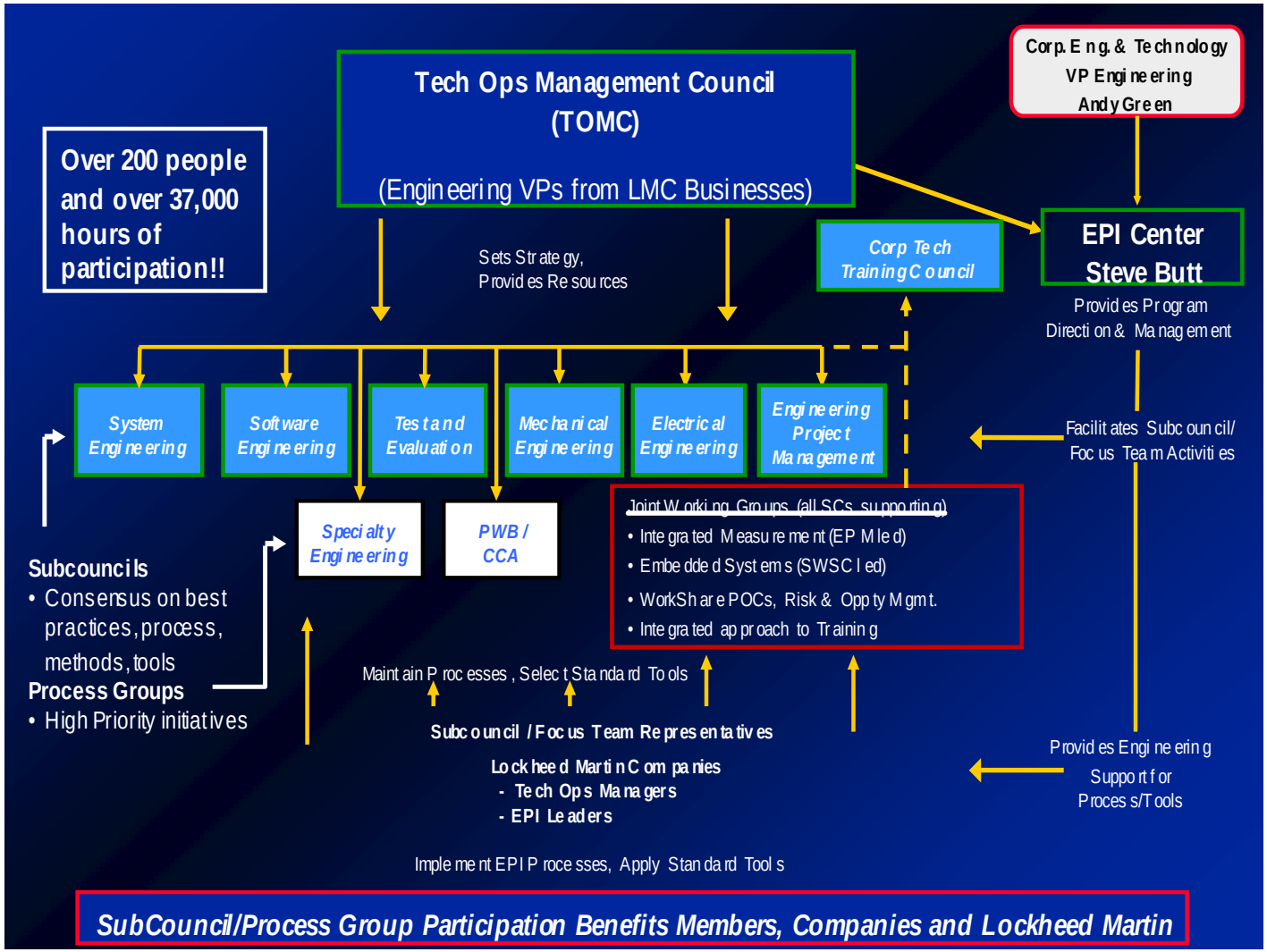
Suggestion was raised by LM management that we pursue the furthering of these Best Practices concepts via a Security "extension" to the CMMI.

® CMMI is register in the U.S. Patent and Trademark Office by Carnegie Mellon University

Context – SW Subcouncil

LOCKHEED MARTIN

Engineering Process Improvement Center



Completed a joint Safety and Security guidebook entitled:

Software Safety & Security:
A Guidebook for Engineering Best Practices and Certification & Accreditation Requirements

EPI 260-19 Version 1.0 completed July 2006.

Continuous content development has been maintained since July 2006 –

Version 2.0 was released end of July 2007.

Best Practices Specifics

Description of the more common SW Safety and Security Engineering and Certification Processes LM programs encounter. Also "how to use" those processes.

Intended for those not fully knowledgeable with a particular certification process – program management / technical / business development.

Built in an electronic format as a web-based document.

- but many people still want / need paper version

Section I Overview

- DoD 8570 - Information Assurance Workforce Improvement Program.
- Anti Tamper – A high level awareness summary of the:

  Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs*

*Issued by Dr. Gansler, Under Secretary of Defense, in May 2000

Section II – Engineering Guidance

- DOD-I- 8500.2- Information Assurance Implementation
- Safety & Security Extensions for Integrated Capability Maturity Models
- Key Practices for Engineering Security Mission-critical Systems
- ISO/IEC 27002: 2005 - Code of Practice for Information Security Management *(formerly ISO-IEC 17799)*
- NIST 800-53 - Security Controls for Federal Information Systems & Appendices
- NIST 800-30 - Risk Management Guide for Information Technology Systems
- NASA-GB-8719.13: Software Safety Guidebook Security Engineering Checklists

Section III – Certification Standards

- DITSCAP
- DIACAP
- (MIL-STD-882) Standard Practice for System Safety
- DO178B - Software Considerations in Airborne Systems and Equipment Certification
- C&A Methodologies Overview – developed by Systems Software Consortium
- ISO-IEC 27001: 2005 - Information Security Management Systems - Reqs;

  (27001 requires the use of 27002 which provides the needed guidance.)
- Common Criteria, ISO 15408, Information technology - Security Techniques - Evaluation criteria for IT security
- DCID 6/3 - Protecting Sensitive Compartmented Information Within Information Systems

BP Development Concept

- **Very aggressive schedule**
  - Started late September 2005
  - Draft of BP completed at the end of March 2006
  - Review cycle with our Pilot Partners completed late June 2006
  - Delivered to the SW Subcouncil on June 23, 2006
  - SW Subcouncil provided feedback completed July 2006
  - BP became EPI 260-19 in August 2006

- **First Version - developed 3 engineering and 3 certification processes documents in parallel**
  - Each document led by a SME
  - SME created synopsis of reference guidance with appropriate links to source(s)
  - SME solicited and selected pilot project partner
  - SME worked with pilot project partner to validate the guidance

- **Second version added additional relevant processes to sections II and III.**

A relevant component of section II of our Guidebook is a summary description of the Safety and Security Extension for Integrated Capability Maturity Models*.

- **Section II – Engineering Guidance**
  - DOD-I- 8500.2
  - **Safety & Security Extensions for Integrated Capability Maturity Models**
  - Key Practices for Engineering Security Mission-critical Systems

S & S Extensions are viewed as important to LM programs. Within our Best Practices, the Extensions are described and organized as:

Background - Section 2: Overview / Status / Evaluation

Structure – Section 3: Application Area / Work Environment

*Safety and Security Extensions for Integrated Capability maturity Models, September 2004, L. Ibrahim, J. Jarzombek, M. Ashford, et al.

CMMI* Section 2: *draws from existing and established Safety and Security sources – many which are pertinent to LM programs

Safety:

- ***MIL_STD 882D****
- ***DEF STAN 00-56***

Security:

- ***ISO 17799****
- ***ISO 15408 Common Criteria****
- **ISO 21827 (Sys Sec Eng CMM)**
- **NIST 800-30 Risk Management***

*Certifications and processes covered in Best Practices v1.0 and its revisions.

BP Promotion and Use

With the release of Version 2.0 – content development gives way to promoting the use of the Best Practices so that . . . .

Better SW assurance is the result by changing behavior in new programs to consider safety and security certification requirements up front.

Management has to be aware of the Best Practices in order to use them effectively.

Promotion Tasks

LOCKHEED MARTIN

Working with the LM Business Areas management leaders:

- Brief BP to Program Management Councils
- Identify to leaders SMEs (the authors) who can be help in specific certification areas
- Monitor which programs are using the BP
- Maintain the document via its built-in reader comment capability
- Continue to add new and relevant engineering and certification processes to the BP

Who is our Target Audience?

LOCKHEED MARTIN

Primarily we seek to promote the use of these Best Practices for Safety and Security assurance among program managers at project inception.

Best Practices (BP) serves front line engineers who have limited knowledge of assurance or certification processes

BP has easy-to-use reader to SME contact capability for each given Safety or Security topic.

Summary

Within LM we are taking an active role to foster a development environment that promotes Safety and Security Assurance from program inception. The Certification Best Practices Guidebook is an important part of that strategy.

We welcome the opportunity to promote and extend this level of assurance awareness out to the larger community of practice via the CMMI Model or other well recognized standards organizations.

Contact Information

LOCKHEED MARTIN

Engineering Process Improvement Center

Dennis J. Beard , CISSP
Systems Engineer (IT Security) Senior Staff
MS2 – Syracuse
315-456-3236
dennis.j.beard@lmco.com