Extending CMMI® and iCMM® for Safety and Security

Linda Ibrahim

Federal Aviation Administration

Joe Jarzombek

Office of Under Secretary of Defense

Presented at CMMI Technology Conference
November 2003; Denver, Colorado

®Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

Topics

- **Background and Motivation**
- **What's been done**
- **The Way Ahead**

Background

- **CMMI and iCMM interest in safety/security**
  - FAA approved a project to include both safety and security in FAA integrated CMM (iCMM)
  - CMMI Steering Group has discussed addressing safety and security; yet decided to stabilize CMMI at v1.1 for a few years
- **DoD and FAA decided to collaborate on developing safety/security extensions to both iCMM and CMMI**
  - Joint FAA/DoD project launched with broad participation including government, industry, and SEI
  - Objectives: identify best safety and security practices with intent that common content would be included in both models

Motivation

- **Safety and security are critical to both DoD and FAA, as well as other government and industry organizations**
- **Both CMMI and iCMM provide a framework in which safety and security activities can take place**
- **Analysis of current safety and security standards highlighted potential "gaps" in CMMI/iCMM coverage**

What's Been Done: Current Status

- **What produced so far**
  - Selection of source material for safety and for security
  - Development of integrated best practices from sources
  - Harmonization of safety and security practices
  - External review and subsequent revision
  - Initial packaging of revised practices for integration/ alignment with reference models
  - Pilot appraisals initiated

Source Documents Selected

- **Traceability required between extension and source documents**
  - Demonstrate coverage of source documents
- **Three Source Documents for safety**
  - *MIL-STD-882C:* System Safety Program Requirements
  - *IEC 61508:* Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems
  - *DEF STAN 00-56:* Safety Management Requirements for Defence Systems
- **Four Source Documents for security**
  - *ISO 17799:* Information Technology - Code of practice for information security management
  - *ISO 15408:* The Common Criteria (v 2.1) Mapping of Assurance Levels and Families
  - *SSE-CMM:* Systems Security Engineering CMM (v2.0)
  - *NIST 800-30:* Risk Management Guide for Information Technology Systems

Best Practices Synthesized, Harmonized and Reviewed

- **Safety and security practices synthesized**
  - Source documents for each area mapped together at high-level
  - Practices synthesized from similar practices/ clauses/activities pertaining to common outcomes
  - Practice level mappings to source material retained
- **Practices harmonized and reviewed**
  - Safety and security practices harmonized resulting in common set of practices
  - Distributed for external review
  - Over 200 comments received from ~35 reviewers in US, Australia, and various European countries
  - Comments dispositioned by team; practices revised

Initial Packaging of Revised Practices

- **Revised practices analyzed with respect to reference models**

- **Most of the harmonized safety and security practices are already addressed to varying extents in existing PAs of CMMI and/or iCMM**
  - They can be implemented by performing existing practices of iCMM and/or CMMI, with appropriate interpretation for safety and security assurance application
  - However, there is currently no easy mechanism to identify which practices are required for appraisal or process improvement purposes

- **Some practices need more focused coverage in both models**
  - Although there is some guidance, additional emphasis is desirable

- **Preliminary conclusion:**
  - A Safety and Security Assurance Application Area is proposed, and has been drafted
  - A Work Environment Process Area is proposed, and has been drafted

The Safety and Security Assurance Application Area

An Application Area:

- Identifies best practices (application practices) associated with the application, drawn from the source documents
  - Provides informative, interpretative information about each application practice
  - Identifies existing practices in one or both reference models that would be performed to implement the application practice
- Keeps the application practices visible for those pursuing the application, for both process improvement and appraisal purposes
- Draws on breadth and depth of the reference models for details of required application practices; avoids needless redundancy
- Is appraised by appraising the associated practices in the reference model, as interpreted by the application
  - An application area can be at any capability level

Safety and Security Assurance Application Practices - 1

The Safety and Security Assurance Application Practices

(NOTE: This is work in progress)

Practices related to capability

- **Assure Safety and Security Awareness**
- **Establish Qualified Work Environment:** Establish and maintain a qualified work environment that meets safety and security needs.
- **Control Information:** Establish and maintain storage, protection and access for safety and security assurance information.
- **Monitor Incidents:** Monitor, report, and analyze safety and security incidents and identify corrective action.

Practices related to threats and associated risks

- **Identify Threats:** Identify potential threats and likely sources of threats.
- **Analyze and Prioritize Threats:** For each potential treat, estimate the consequence and likelihood of an occurrence and determine relative priority.
- **Identify Causal Factors:** For each threat, determine the causal factors.
- **Determine, Implement and Monitor Threat Risk Reduction Strategy:** For each threat, determine, implement and monitor the risk reduction strategy to achieve an acceptable level of risk.

Safety and Security Assurance Application Practices - 2

Practices related to development and assurance

- **Determine Regulatory Requirements, Legal Requirements and Standards:** Identify and document regulatory requirements, legal requirements and standards.
- **Establish and Allocate Safety and Security Requirements:** Establish and maintain safety and security requirements, including associated integrity levels that address threats and threat risk reduction strategies, and design the product or service to meet them.
- **Objectively Evaluate Products:** Objectively verify and validate work products and delivered products and services to assure safety and security assurance requirements have been achieved and services fulfill intended use.
- **Establish Safety and Security Assurance Argument:** Establish and maintain a safety and security assurance argument and supporting evidence throughout the lifecycle.

Safety and Security Assurance Application Practices - 3

Practices related to management

- **Establish a Safety and Security Assurance Organization Structure:** Establish and maintain safety and security organization structure including specifying roles and duties of personnel and groups, providing reporting channels, and ensuring adequate levels of managerial and technical independence.
- **Establish a Safety and Security Assurance Plan:** Establish and maintain a safety and security plan to achieve overall safety and security assurance requirements and objectives.
- **Conduct Reviews of Safety and Security Activities:** Review progress of activities relative to safety and security plan both periodically and at selected milestones.

Practices related to suppliers

- **Select Suppliers:** Select suppliers based on evaluation of ability to meet specified safety and security requirements and criteria.
- **Establish Supplier Agreements:** Establish supplier agreements using criteria that include safety and security requirements.
- **Satisfy Supplier Agreements that include Safety and Security Requirements:** Execute supplier agreements and ensure that safety and security assurance is delivered with the product or service.

Safety and Security Assurance draws on Practices from the following PAs

iCMM PAs	CMMI PAs *(including extensions)*
PA 19 Work Environment *(NEW)*	Work Environment *(NEW)*
PA 10 Operation and Support	*Operation and Support (extended from iCMM)*
PA 01 Needs; PA 02 Requirements	Requirements Development *(with new practice to be added)*; Requirements Management
PA 13 Risk Management	Risk Management
PA 08 Evaluation	Verification; Validation
PA 00 Integrated Enterprise Management	*Integrated Enterprise Management (extended from iCMM)*
PA 11 Project Management	Project Planning; Project Monitoring and Control; Integrated Project Management
PA 05 Outsourcing; PA 12 Supplier Agreement Management	Supplier Agreement Management
PA 03 Design	Technical Solution
PA 17 Information Management	*Information Management (extended from iCMM)*
PA 16 Configuration Management	Configuration Management
PA 22 Training	Organizational Training
PA 15 Quality Assurance and Management	Process and Product Quality Assurance
PA 21 Process Improvement	Organizational Process Focus
PA 18 Measurement and Analysis	Measurement and Analysis

Work Environment Process Area

(NOTE: This is work in progress)

Goal: A work environment that meets stakeholder needs is established and maintained.

Practices:

- **Determine work environment needs:** Establish and maintain the needs and requirements to implement, operate and sustain work environments.
- **Establish work environment standards:** Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements.
- **Establish work environment:** Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs.
- **Maintain the qualification of components:** Maintain the required qualification of work environment components.
- **Maintain the qualification of personnel:** Assure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.
- **Maintain technology awareness:** Monitor, evaluate and insert, as appropriate, new technology for improving the work environment.
- **Assure continuity of work environment:**

The Way Ahead

- **Pilot appraisals have been initiated**
  - Two in FAA, one in Lockheed Martin, one may be initiated in Department of Energy
  - These are ARC Class C appraisals, for validation of practices
  - Appraisal feedback will be incorporated
- **Final packaging**
  - Safety and Security Assurance Application Area
  - Work Environment Process Area
  - Guidance material
  - Consolidated Glossary
  - Mapping to source material
- **Distribution for review**
- **Revision, Publication, and Use**

Contact Information

- **For more information, or to participate, please contact:**
  - Linda Ibrahim: linda.ibrahim@faa.gov
  - Joe Jarzombek: joe.jarzombek@osd.mil
- **Information available on-line at:**

  http://www.acq.osd.mil/sts/sis/

  http://www.faa.gov/ipg

Selected terminology - 1

RELATED DEFINITIONS (extracted from consolidated Safety/Security Glossary)

Assurance argument: A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

Integrity Level: A denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.

"The system integrity level corresponds to the tolerable level of risk that is associated with the system. A system can be associated with risk because its failure can lead to a threat, or because its functionality includes mitigation of consequences of initiating events in the system's environment that can lead to a threat."

Software safety integrity: Measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time

Software safety integrity level: Discrete level (one out of a possible four) for specifying the safety integrity of software in a safety-related system

Selected terminology - 2

Risk: Combination of the probability of occurrence of harm and the severity of that harm; The combination of the frequency, or probability, and the consequence of an accident; An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability; The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

Threat: A state of the system or system environment which can lead to adverse effect in one or more given risk dimensions; The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability; Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or a system.

Threat analysis: The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy; includes a weakness of an asset or group of assets which can be exploited by a threat

Hazard: Potential source of harm; A physical situation, often following from some initiating event, that can lead to an accident; A condition that is prerequisite to a mishap.

Hazard probability: The aggregate probability of occurrence of the individual events that create a specific hazard.

Hazard severity: An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.