INTEGRITY ASSURANCE: Safety/Security Extensions to CMMI® and iCMM®

Dr. Linda Ibrahim
Chief Engineer for Process Improvement
Federal Aviation Administration
Topics

- Background and Motivation
- Strategy
- What’s been done
- The Way Ahead
- Contact Information
Background

• CMMI and iCMM interest in safety/security
  – In December 2001, Australian Defence Materiel Organization, with the support of US DoD, developed +SAFE – A Safety Extension to CMMI
  – 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 3 years

• DoD and FAA decided to collaborate on developing safety/security extensions to both iCMM and CMMI
  – Joint FAA/DoD project launched in May 2002
  – Broad participation from government and industry
Motivation - 1

- 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

- Australian pilots concluded that safety is not adequately covered in CMMI
  - Risk that an organization appraised as capable under CMMI might be found lacking in safety process capability

- Analysis of current safety and security standards highlighted potential “gaps” in CMMI/iCMM coverage
Motivation - 2

• **CMMI:** CMMI-SE/SW/IPPD/SS, V1.1 mentions:
  – “Safety”: in 9 PAs
    • Project Planning, Risk Management, Requirements Development, Technical Solution, Product Integration, Configuration Management, Decision Analysis and Resolution, Organizational Environment for Integration, Causal Analysis and Resolution
  – “Security”: in 10 PAs
    • Project Planning, Project Monitoring and Control, Supplier Agreement Management, Risk Management, Requirements Development, Technical Solution, Product Integration, Configuration Management, Measurement and Analysis, Organizational Environment for Integration

• **Safety and security are only mentioned in informative components of the CMMI**
  – Not in *required* or *expected* components

• **The source material for CMMI did not include any specific safety or security references**
Motivation - 3

• iCMM: iCMM v2.0 includes:
  – For SECURITY – Normative material in 1 PA
    • Information Management
  – For SECURITY - Expected material in 6 PAs
    • Needs; Requirements; Deployment, Transition, and Disposal; Project Management; Configuration Management; Information Management
  – For SECURITY - Informative material in 11 PAs
    • Integrated Enterprise Management; Needs; Requirements; Design; Outsourcing; Evaluation; Deployment, Transition, and Disposal; Project Management; Integrated Teaming; Configuration Management; Information Management; Measurement and Analysis
  – For SAFETY – no Normative material
  – For SAFETY – Expected material in 4 PAs
    • Needs; Requirements; Integration; Deployment, Transition, and Disposal
  – For SAFETY - Informative material in 13 PAs
    • Integrated Enterprise Management; Needs; Requirements; Design; Alternatives Analysis; Integration; Evaluation; Deployment, Transition, and Disposal; Project Management; Integrated Teaming; Configuration Management; Training; Innovation

• iCMM v2.0 integrates 10 sources; some safety/security content
  – None of these sources are specific to safety or security
Overall Strategy to Develop Extension

1) Form Teams
2) Decide Source Material and Map Together at High Level
3) Develop/Synthesize Best Practice from Sources
4) Harmonize Safety and Security Practices
5) Review/Revise (external review)
6) Integrate/Align with the Reference Models
7) Perform Pilot Appraisals
8) Generate/Provide Training/Guidance
9) Review and Publish
Form Teams

Over 30 participants from FAA, OSD, Army, Navy, Air Force, NASA, DOE, Australian DMO, SEI and industry

Team structure:

• **Project Management**
  – co-leads with overall project responsibility

• **Safety Team**
  – co-leads, authors, and buddies responsible for safety best practices

• **Security Team**
  – co-leads, authors, and buddies responsible for security best practices

• **Model Team**
  – responsible for model knowledge, model placement, editing

• **Harmonization Team**
  – responsible for harmonization and vocabulary

• **Pilot Team**
  – responsible for planning pilot appraisals
Source Documents - 1

• Source documents are major, essential, widely recognized documents (3 to 5)

• Source documents used to synthesize “best practice”

• Bi-directional traceability required between new extension and source documents
  – Demonstrate coverage of source documents

• Reference documents also identified
  – Useful in developing best practices in certain areas, but full coverage and detailed mapping not required
  – E.g., +SAFE was used extensively as input to the safety component of the extension
### Source Documents - 2

- **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
Synthesizing Best Practice

- Source documents mapped together at high-level
- Natural groupings of subject matter identified
- Common objectives/outcomes identified
- Practices synthesized from similar practices/clauses/activities pertaining to common outcomes
- Practice level mappings to source material retained
Harmonization and Initial Review

- **Initial harmonization of the safety and security components occurred in October 02**
  - Safety and security harmonized into a single set of practices titled “Integrity Assurance”

- **Mapping maintained to the original safety and security source documents**
  - Important to demonstrate full coverage of the source documents

- **Common terms proposed for adoption**
  - Endeavor to use standard ISO terminology where possible

- **Review package released in November 2002, for broad review**
  - containing 26 harmonized integrity assurance practices
1. Establishing the Integrity Assurance Program
   - 1.1 Determine Regulatory Requirements, Legal Requirements and Standards
   - 1.2 Establish Integrity Assurance Objectives
   - 1.3 Establish an Integrity Assurance Organization Structure
   - 1.4 Establish an Integrity Assurance Plan

2. Managing the Integrity Assurance Program
   - 2.1 Conduct Reviews of Integrity Assurance Activities
   - 2.2 Monitor Integrity Assurance Incidents
   - 2.3 Establish and Control Integrity Assurance Repository
   - 2.4 Manage the Integrity Assurance Program
3. Managing Supplier Agreements
   - 3.1 Select Suppliers
   - 3.1 Establish Supplier Agreements
   - 3.2 Satisfy Supplier Agreements that Include Integrity Requirements

4. Determining and Applying Integrity Principles
   - 4.1 Determine Appropriate Integrity Principles, Measures and Tools
   - 4.2 Apply Integrity Principles, Measures and Tools

5. Identifying Threats
   - 5.1 Identify Likely Sources of Threats
   - 5.2 Document Threats and Incidents
6. Analyzing Integrity Risk
   - 6.1 Categorize Threats
   - 6.2 Prioritize Threats
   - 6.3 Identify Causal Factors
   - 6.4 Determine Risk Reduction Strategy

7. Developing and Allocating Integrity Requirements
   - 7.1 Develop Integrity Requirements
   - 7.2 Analyze Integrity Requirements
   - 7.3 Allocate Integrity Requirements
   - 7.4 Perform Impact Analysis of Changes

8. Determining Integrity Achievement
   - 8.1 Determine Compliance
   - 8.2 Assure Integrity
   - 8.3 Establish and Maintain Integrity Assurance Argument
Review/Revise

- Review package released for broader internal and external review
- 200+ review comments received
- Comments dispositioned
- Model placement in progress
Integration with CMMI & iCMM

- The goal is for common content to be integrated into both CMMI and iCMM

- The Model Team is
  - Analyzing and relating the harmonized practices to the content and structure of the existing integrated models
  - Determining placement of the material for both CMMI and iCMM, e.g., several of the harmonized practices are already covered to varying extents in existing PAs of the iCMM and CMMI

- Insufficient to use Integrity Assurance practices alone to conduct a safety or security appraisal
  - To be used in conjunction with other CMMI or iCMM PAs (with elaborations/amplifications)
  - Need to integrate with reference models
The Way Ahead

- **Pilot appraisals are being planned**
  - Appraisal feedback will be incorporated

- **Tech Note to be developed, including:**
  - Front matter
  - Integrity Assurance Process Area extension
  - Reference model integration – amplifications/elaborations to PAs
  - Guidance material
  - Mapping to source material

- **Tech Note to be distributed for review**

- **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
  – Matt Ashford: mashford@hq.dcma.mil

• Information available on-line at:
  http://www.acq.osd.mil/sts/sis/
  http://www.faa.gov/ipg
**Team Members – 1 of 2**

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Team/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ahern, Dennis</td>
<td>Northrop Grumman Electronic Systems</td>
<td>Model Team</td>
</tr>
<tr>
<td>Ashford, Matt</td>
<td>Australian Defence Materiel Organisation (DMO)</td>
<td>Safety Co-lead</td>
</tr>
<tr>
<td>Bate, Roger</td>
<td>Software Engineering Institute</td>
<td>Model Team</td>
</tr>
<tr>
<td>Coblentz, Brenda</td>
<td>US Department of Energy (DOE)</td>
<td>Safety Buddy Pilot Team</td>
</tr>
<tr>
<td>Conrad, Ray</td>
<td>Lockheed Martin Air Traffic Mgt (Safety)</td>
<td>Safety Buddy</td>
</tr>
<tr>
<td>Cooper, David</td>
<td>Praxis Critical Systems Ltd (UK)</td>
<td>Harmonization Team</td>
</tr>
<tr>
<td>Courington, Tim</td>
<td>FAA/Northrop Grumman</td>
<td>Security Co-lead</td>
</tr>
<tr>
<td>Croll, Paul</td>
<td>Computer Sciences Corporation (CSC)</td>
<td>Harmonization Lead</td>
</tr>
<tr>
<td>Dhami, Sartaj</td>
<td>FAA/Northrop Grumman</td>
<td>Security Author</td>
</tr>
<tr>
<td>Gill, Janet</td>
<td>US Navy, NAVAIR Software System Safety Lead</td>
<td>Safety Author</td>
</tr>
<tr>
<td>Henning, Ronda</td>
<td>Harris Corp</td>
<td>Security Co-lead</td>
</tr>
<tr>
<td>Horn, Mary</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>Ibrahim, Linda</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Project Co-Manager, Model Team Lead</td>
</tr>
<tr>
<td>Jackson, Tom</td>
<td>Lockheed Martin</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>Jarzombek, Joe</td>
<td>US Office of Secretary of Defense (OSD)</td>
<td>DoD Co-Sponsor, Project Co-Manager, Harmonization Team</td>
</tr>
</tbody>
</table>
## Team Members – 2 of 2

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Team/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keblawi, Faisal</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Co-Lead</td>
</tr>
<tr>
<td>Kemens, Victor</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>LaBruyere, Larry</td>
<td>FAA/Northrop Grumman</td>
<td>Pilot Team</td>
</tr>
<tr>
<td>Leonette, Martha J.</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Author</td>
</tr>
<tr>
<td>Miller, Gerald</td>
<td>FAA/Northrop Grumman</td>
<td>Security Author</td>
</tr>
<tr>
<td>Ming, Lisa</td>
<td>Defense Contract Management Agency</td>
<td>Safety Author</td>
</tr>
<tr>
<td>Patel, Raju B.</td>
<td>US Air Force, Wright Patterson AFB</td>
<td>Security Author</td>
</tr>
<tr>
<td>Pierson, Hal</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>Pyster, Art</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>FAA Co-Sponsor</td>
</tr>
<tr>
<td>Roseboro, Douglas</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>Sherer, Wayne</td>
<td>US Army, Picatinny Arsenal</td>
<td>Model Team</td>
</tr>
<tr>
<td>Simmons, Marty</td>
<td>Lockheed Martin Mission Systems</td>
<td>Security Buddy</td>
</tr>
<tr>
<td></td>
<td>(Security)</td>
<td></td>
</tr>
<tr>
<td>Stamnas, Les</td>
<td>SAIC</td>
<td>Pilot Team</td>
</tr>
<tr>
<td>Stroup, Ron</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Safety Co-lead</td>
</tr>
<tr>
<td>Stuart, Sandra</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Security Buddy</td>
</tr>
<tr>
<td>Terry, Ray C</td>
<td>US Navy, NAVAIR Systems Safety Division Head</td>
<td>Safety Buddy</td>
</tr>
<tr>
<td>VanBuren, Scott</td>
<td>US Federal Aviation Administration (FAA)</td>
<td>Harmonization Team</td>
</tr>
<tr>
<td>Wells, Curt</td>
<td>i-Metrics</td>
<td>Model Team</td>
</tr>
<tr>
<td>Wetherholt, Martha</td>
<td>NASA</td>
<td>Safety Author</td>
</tr>
</tbody>
</table>