INTEGRITY ASSURANCE: Extending the CMMI[SM] & iCMM for Safety and Security

Linda Ibrahim
(Federal Aviation Administration)

Joe Jarzombek
(Office of the UnderSecretary of Defense)

Matt Ashford
(Australian Defence Material Organisation)

Topics

- Overview
  - Background
  - Motivation
- Strategy
  - Who's involved
  - Source Documents
  - Synthesis of best practice
  - Harmonization
- Overview of the Extension
- Integration with the Reference Models (CMMI / iCMM)
- The Current State of Play
- The Way Ahead
- Other Issues
- Conclusions

Background

- In December 2001, Australian DMO, with the support of US DoD, developed +SAFE – A Safety Extension to CMMI
- Initial release generated international interest, including US FAA and additional US DoD
- FAA approved a project to include both safety and security in FAA's integrated CMM (iCMM)
- CMMI SG have discussed addressing safety and security
- DoD and FAA decided to collaborate on developing safety/security extensions to both iCMM and CMMI
- Joint FAA/DoD project launched in May 2002
  - Participation from NASA, DOE and contractors
  - Experts from government and industry engaged

Motivation - 1

- Safety and security are critical to both DoD and FAA
- Both CMMI and iCMM provide a framework in which safety and security activities can take place
  - Yet some safety and security specific practices not addressed

Motivation - 2

- CMMI - The Facts:

  CMMI-SE/SW/IPPD/SS, V1.1 mentions:-

  - "Safe/Safety": 17 times 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": 19 times 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 – The Facts: 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

Motivation -4

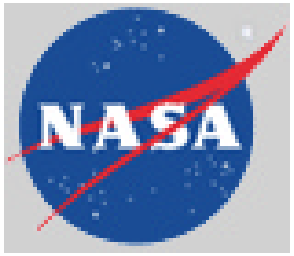
- On the safety side, Australian DMO trial concluded that safety is not adequately covered in CMMI
  - The coverage of safety within a CMMI based assessment was usually dependant on the assessment team's knowledge and experience
    - Independent of assessment method / model employed
    - Open to interpretation - weakens consistency and repeatability
  - Risk that an organization assessed as capable under CMMI might be found lacking in safety process capability
- Analysis of current safety standards highlighted potential "gaps" in CMMI/iCMM coverage, including:
  - Integrity requirements, that include "integrity levels"
  - Sliding scale of design and development rigor to address varying levels of system integrity
  - Hazard Log
  - Safety Argument and Supporting Evidence
  - Formal acceptance of residual safety risk
- Similar issues exist for security

Overall Strategy to Develop Extension

- Form Teams ☑
- Decide Source Material and Map Together at High Level ☑
- Develop/Synthesize Best Practice from Sources ☑
- Harmonize Safety and Security Practices ☑
  - Identify common goal and practices
- Review/Revise (external review)
- Integrate/Align with the Reference Models
- Perform Pilot Appraisals
- Generate/Provide Training/Guidance
- Publish

Who's Involved?
The Development Team...

TRW



HARRIS

NORTHROP GRUMMAN

LOCKHEED MARTIN

NAVAIR

SAIC
An Employee-Owned Company

CSC

I-metrics

Team Structure

Joe Jarzombek (OSD) Linda Ibrahim (FAA)
Joint Project Managers

Safety Team	Security Team	Harmonization Team	Model Team	Pilot Team
✓				✓
✓		✓		
	✓			
	✓		✓	✓
			✓	✓

Source Documents

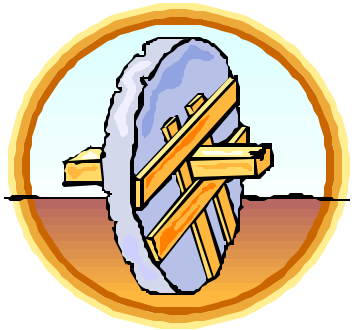
- Source documents are major, essential, widely recognized documents (3 to 5)
- Source documents used to synthesize “best practice”
- Bi-directional traceability required between new extension and source documents
  - Demonstrated coverage of source documents
- Reference documents also identified

- 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
  - Systems Security Engineering CMM (v2.0)
  - NIST 800-30: Risk Management Guide for Information Technology Systems

Source Documents -2

- 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

- What about +SAFE?
  - Australian DMO has already developed a CMMI safety extension
    - Lessons learnt for both content and CMMI integration
  - Although not a "source" document, +SAFE was used extensively as input to the safety component of the extension
    - Provided both content and structure
  - Didn't want to re-invent the wheel!



Synthesizing Best Practice

- Source documents mapped together at high-level
- Natural groupings of subject matter identified
  - "Information bins"
- Common objectives/outcomes identified
- Practices synthesized from similar practices/ clauses/activities pertaining to common outcomes

- Author guidelines developed by Model Team with a simple template provided, including:
  - Goal Name and Goal Statement
  - Practice Name and Practice Statement for practices related to each goal
  - Mapping to the source material

Harmonization

- Initial harmonization of the safety and security components occurred on 16/17 October 02
  - Safety and security harmonized into a single Process Area extension, titled “Integrity Assurance”
- Mapping maintained to the original safety and security source documents
  - Important to demonstrate full coverage of the source documents
- Common terms defined and adopted, e.g.
  - “Threat” (includes potential hazards and vulnerabilities)
  - “Integrity Level”
  - …
- Endeavor to use standard ISO terminology where possible

Integrity Assurance Process Area Structure -1

Process Area	Specific Goals (Note: DRAFT ONLY; subject to change)
Integrity Assurance	Establish an Integrity Assurance Program
	Manage the Integrity Assurance Program
	Manage Supplier Agreements
	Determine and Apply Integrity Principles Throughout Lifecycle
	Identify Threats
	Perform Integrity Risk Analysis
	Develop and Allocate Integrity Requirements
	Determine Integrity Achievement

Note: Some of the Goals/Practices will be implemented via amplifications and elaborations in the reference models (iCMM/CMMI)

Integrity Assurance Process Area Structure -2

- **SG 1. ESTABLISH AN INTEGRITY ASSURANCE PROGRAM**
  - **SP 1.1 Determine Regulatory Requirements, Legal Requirements and Standards**
  - **SP 1.2 Establish Integrity Assurance Objectives**
  - **SP 1.3 Establish an Integrity Assurance Organization Structure**
  - **SP 1.4 Establish an Integrity Assurance Plan**
- **SG 2. MANAGE THE INTEGRITY ASSURANCE PROGRAM**
  - **SP 2.1 Conduct Reviews of Integrity Assurance Activities**
  - **SP 2.2 Monitor Integrity Assurance Incidents**
  - **SP 2.3 Establish and Control Integrity Assurance Repository**
  - **SP 2.4 Manage the Integrity Assurance Program**

Integrity Assurance Process Area Structure -3

- **SG 3. MANAGE SUPPLIER AGREEMENTS**
  - **SP 3.1 Select Suppliers**
  - **SP 3.1 Establish Supplier Agreements**
  - **SP 3.2 Satisfy Supplier Agreements that Include Integrity Requirements**
- **SG 4. DETERMINE AND APPLY INTEGRITY PRINCIPLES THROUGHOUT LIFECYCLE**
  - **SP 4.1 Determine Appropriate Integrity Principles, Measures and Tools**
  - **SP 4.2 Apply Integrity Principles, Measures and Tools**
- **SG 5. IDENTIFY THREATS**
  - **SP 5.1 Identify Likely Sources of Threats**
  - **SP 5.2 Document Threats and Incidents**

Integrity Assurance Process Area Structure -4

- **SG 6. PERFORM INTEGRITY RISK ANALYSIS**
  - SP 6.1 Categorize Threats
  - SP 6.2 Prioritize Threats
  - SP 6.3 Identify Causal Factors
  - SP 6.4 Determine Risk Reduction Strategy
- **SG 7. DEVELOP AND ALLOCATE INTEGRITY REQUIREMENTS**
  - SP 7.1 Develop Integrity Requirements
  - SP 7.2 Analyze Integrity Requirements
  - SP 7.3 Allocate Integrity Requirements
  - SP 7.4 Perform Impact Analysis of Changes
- **SG 8. DETERMINE INTEGRITY ACHIEVEMENT**
  - SP 8.1 Determine Compliance
  - SP 8.2 Assure Integrity
  - SP 8.3 Establish and Maintain Integrity Assurance Argument

Integration with CMMI & iCMM

- Insufficient to use the Integrity Assurance PA, stand alone, to conduct a safety or security appraisal
  - To be used in conjunction with other CMMI or iCMM PAs
  - Minimal subset yet to be determined, however most likely to be the majority of the Level 2 and 3 Pas
  - Need to integrate with reference models
- The goal is for common content to be integrated into both CMMI and iCMM
- The Model Team will
  - Analyze and relate the harmonized goals and practices to the content and structure of the existing integrated models
  - Determine placement of the material for both CMMI and iCMM

Current State of Play

- Stand-alone safety and security extensions developed
  - Mapped to source documents
- Safety and security extensions harmonized, resulting in new “Integrity Assurance” Process Area
- Review package developed and ready to be released for broader internal and external review
  - Available on-line at: http://www.acq.osd.mil/sts/sis/

Who's Involved?
The Review Team...

The Way Ahead

- Collect, consolidate and incorporate review comments
- Validation program / pilot appraisals
- Tech Note, including:
  - Front matter
  - Integrity Assurance Process Area extension
  - Reference model integration
  - Guidance material
  - Mapping to source material
- Training
  - Initial training to be provided to appraisers during trial
  - More formal training material to be developed
- Configuration Control
  - iCMM and CMMI currently have different CCBs
- Stewardship/Maintenance
  - FAA to provide stewardship

Other Issues

- Product Vs Process
  - Process Model is different to Product Assessment
  - Designed to be used “up front” to address program risk, not at the end when system developed
- Capability Level • Integrity Level
  - No direct correlation between CMM capability/maturity levels and Integrity Levels / Levels of Assurance
  - Achieving a certain CMM capability/maturity level does not guarantee the ability to develop high integrity systems
- What about Certification?
  - Certification is an important component of a safety/security program, however is:
    - usually focussed on post-development test & evaluation; often too late
    - heavily reliant on the existence of regulations and standards to fully capture the safety and security “issues” – which is difficult to achieve
    - often different depending on what it’s for, where it’s done and who does it
  - As systems get more complex, process gets more important

Conclusions -1

- Why do we need to extend the integrated CMMs?
  - Aren't these models "big" enough already? Adding more will just confuse the issue!
  - What's so special about safety and security anyway?
  - Isn't safety and security already covered? If you do good requirements development, shouldn't it all flow from there.
  - If we add safety and security, what about all of the other "specialty" engineering disciplines (e.g. Reliability)?
  - We have a certification process, isn't that enough?

Conclusions -2

- Aren't these models "big" enough already? Adding more will just confuse the issue!
  - Current models inadequately address "integrity assurance"
  - By carefully adding the discipline extensions, new practices should only affect those interested in the discipline
- What's so special about safety and security anyway?
  - Critical to DoD, FAA, NASA, DOE and many others
  - Increasing reliance on high integrity systems
- Isn't safety and security already covered? If you do good requirements development, it should all flow from there.
  - "Goodness" aspect not well addressed in terms of safety/security
  - More to "Integrity Assurance" than just good requirements
  - Practices specific and essential to safety and security, but not already in the iCMM and CMMI will be added

Conclusions -3

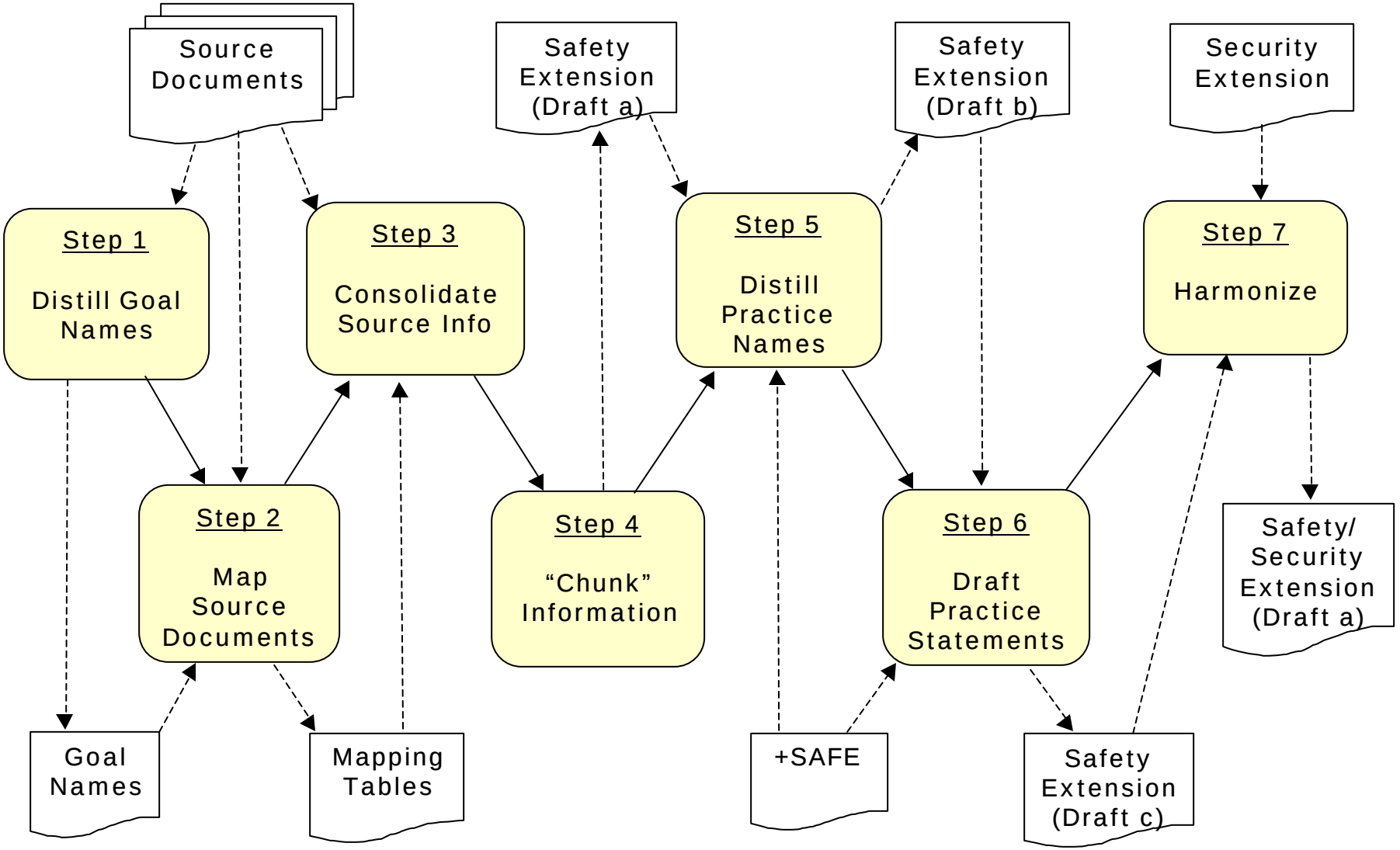
- If we add safety and security, what about all of the other "specialty" engineering disciplines (e.g. Dependability and Reliability)?
  - Although only mapped to the safety and security sources, the new Integrity Assurance PA may already encompass some of the other specialties, such as dependability and reliability
- We have a certification process, isn't that enough?
  - Certification is an important component of a safety/security program, however is:
    - usually focussed on post-development test & evaluation; often too late
    - heavily reliant on the existence of regulations and standards to fully capture the safety and security "issues" – which is difficult to achieve
    - often different depending on what it's for, where it's done and who does it
  - Certification is focussed on the end-game, where process models influence the design and development of a product and the institutionalization of applicable processes across an organization

Conclusions -4

- Initial draft of safety/security extension developed
  - Derived from and mapped to source documents
  - Harmonized into a single PA to encompass both safety and security
- We need your participation
- If interested in serving as a stakeholder/reviewer please contact the presenters:
  - Linda Ibrahim: linda.ibrahim@faa.gov
  - Joe Jarzombek: joe.jarzombek@osd.mil
  - Matt Ashford: matt.ashford@osd.mil
- Available on-line at: http://www.acq.osd.mil/sts/sis/

BACK-UP

Distilling Best Practice – Safety Example



Common Terms

- *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. [ISO/IEC 15026, 3.9]

  "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." [ISO/IEC 15026, 6.]

- *Threat*: A state of the system or system environment which can lead to adverse effect in one or more given risk dimensions. [ISO/IEC 15026, 3.21]

- *Risk Dimension*: A perspective from which risk assessment is being made for the system (eg safety, economic, security). [ISO/IEC 15026, 3.12]

Team Members -1

Name	*Organization*	*Team / Role*
Ahern, Dennis	Northrop Grumman Electronic Systems	Model Team
Ashford, Matt	Australian Defence Materiel Organisation (DMO)	Safety Co-lead
Bridges, Kevin	US Federal Aviation Administration (FAA)	Safety Buddy
Coblentz, Brenda	US Department of Energy (DOE)	Safety Buddy
Conrad, Ray	Lockheed Martin Air Traffic Mgt (Safety)	Safety Buddy
Courington, Tim	FAA/TRW Systems	Security Co-lead
Croll, Paul	CSC	Harmonization
Dhami, Sartaj		Security Buddy
Gill, Janet	US Navy, NAVAIR Software System Safety Lead	Safety Buddy
Henning, Ronda	Harris Corp	Security Co-lead
Ibrahim, Linda	US Federal Aviation Administration (FAA)	Project Co-Manager / Model Team
Jarzombek, Joe	US Office of Secretary of Defense (OSD)	DoD Co-Sponsor / Project Co-Manager / Harmonization Team
Keblawi, Faisal	US Federal Aviation Administration (FAA)	Security Co-Lead
Kemens, Victor	US Federal Aviation Administration (FAA)	Security Buddy

Team Members -2

Name	*Organization*	*Role*
LaBruyere, Larry	FAA/TRW	Pilot Team
Leonette, Martha J.	US Federal Aviation Administration (FAA)	Security Author
Miller, Gerald	FAA TRW	Security Author
Ming, Lisa	Defense Contract Management Agency	Safety Author
Pierson, Hal	US Federal Aviation Administration (FAA)	Security Buddy
Pyster, Art	US Federal Aviation Administration (FAA)	FAA Sponsor
Rierson, Leanna	US Federal Aviation Administration (FAA)	Safety Buddy
Sherer, Wayne	US Army, Picatinny Arsenal	Model Team
Simmons, Marty	Lockheed Martin Mission Systems (Security)	Security Buddy
Stamnas, Les	SAIC	Pilot Team
Stroup, Ron	US Federal Aviation Administration (FAA)	Safety Co-lead
Terry, Ray C	US Navy, NAVAIR Systems Safety Division Head	Safety Buddy
VanBuren, Scott	US Federal Aviation Administration (FAA)	Harmonization Team
Wells, Curt	i-Metrics	Model Team
Wetherholt, Martha	NASA	Safety Author