Merging Assurance and the Capability Maturity Model Integration for Software: Efforts and Opportunities

Charles Muniak Ph.D. CSP

May 23, 2008

Agenda

- First a Story about the perception of risk
- What is Assurance?
- What is CMMI?
- Why is this important for safety practitioners?
- Is Safety in the Model?
- Status of present effort

Perception of Risk

What is Assurance?

- System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.
  - *Terms of Reference, ISO/IEC JTC1/SC7 WG9, System and Software Integrity*
- The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.
  - *CNSS Instruction No. 4009, "National Information Assurance Glossary," revised 2006*

The Assurance Problem

- There is a concern about the correct, predictable, safe, secure execution of complex software in distributed environments.
- In many cases there is inadequate attention given to total lifecycle issues, including impacts on lifecycle cost and risk associated with the use of commercial or reused products and components.

2007 Defense Science Board Findings

- Software industry is becoming increasingly global – trend is irreversible
- DoD is becoming increasingly dependent for mission-critical software that is highly interconnected, complex and globally sourced – quality, reliability and trustworthiness is highly variable
- There have been successful attacks upon sensitive but unclassified (SBU) systems by adversaries using low-level cyber attack techniques
- Information Technology (IT) is easy to exploit by nation states and hard to defend – trend will continue with more global sourcing

2007 Defense Science Board Findings

- DoD software continues to contain numerous vulnerabilities and weak information security design characteristics
- Present processes used by DoD for evaluation of commercial products are inadequate
- DoD does not consistently or adequately analyze and incorporate into its acquisition decisions the supply chain threat information that is available
- There is **no silver bullet** for vulnerability detection

Implications

- There is a serious problem with the security vulnerabilities of software acquired by the DoD – the acquisition process will probably be affected
- This represents an opportunity for astute corporations to place themselves in a position of competitive advantage – specifically at the forefront of the effort to add assurance to the CMMI model

"The current CMMI models are a good foundation for these new practices and building new practices on that foundation would help promote faster transition of the practices to the large and growing community of DoD contractors and other SW developers that already invest in adopting the CMMI models". [1]

1 – Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C. 20301-3140, page 35.

What is CMMI®,

- The Department of Defense (DOD) is the sponsor of CMMI®, an engineering and management ***model*** for assuring the quality of (typically information) systems throughout the Systems Development Life Cycle (SDLC).
- Life-cycle responsibility for CMMI® has been delegated to the Software Engineering Institute (SEI), a federally funded research and development center, hosted at Carnegie Mellon University.

Documented Benefits (median improvement 30 organizations)

- Cost - 34%
- Schedule - 50%
- Productivity – 61%
- Quality – 48%
- Customer Satisfaction -14%

Process Model

- A process model is a structured collection of practices that describe the characteristics of effective processes
- Practices included are those proven by experience to be effective

Process Management Premise

The quality of a system is highly influenced by the quality of the process used to acquire, develop and maintain it.

Maturity Level View

- ***Supplier Agreement Management, [ML 2]***
  The purpose of Supplier Agreement Management (SAM) is to manage the acquisition of products from suppliers.
- ***Measurement & Analysis, [ML 2]***
  The purpose of Measurement and Analysis (MA) is to develop and sustain a measurement capability that is used to support management information needs
- ***Requirements Management, [ML 2]***
  The purpose of Requirements Management (REQM) is to manage the requirements of the project's products and product components and to identify inconsistencies between those requirements and the project's plans and work products.
- ***Project Monitoring and Control, [ML 2]***
  The purpose of Project Monitoring and Control (PMC) is to provide an understanding of the project's progress so that appropriate corrective actions can be taken when the project's performance deviates significantly from the plan.
- ***Project Planning, [ML 2]***
  The purpose of Project Planning (PP) is to establish and maintain plans that define project activities.
- ***Process and Product Quality Assurance, [ML 2]***
  The purpose of Process and Product Quality Assurance (PPQA) is to provide staff and management with objective insight into processes and associated work products.
- ***Configuration Management, [ML 2]***
  The purpose of Configuration Management (CM) is to establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits.

Maturity Level View

- ***Validation, [ML 3]***
  The purpose of Validation (VAL) is to demonstrate that a product or product component fulfills its intended use when placed in its intended environment.
- ***Verification, [ML 3]***
  The purpose of Verification (VER) is to ensure that selected work products meet their specified requirements.
- ***Requirements Development, [ML 3]***
  The purpose of Requirements Development (RD) is to produce and analyze customer, product, and product component requirements.
- ***Risk Management, [ML 3]***
  The purpose of Risk Management (RSKM) is to identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.
- ***Technical Solution, [ML 3]***
  The purpose of Technical Solution (TS) is to design, develop, and implement solutions to requirements. Solutions, designs, and implementations encompass products, product components, and product-related lifecycle processes either singly or in combination as appropriate

Maturity Level View

- ***Decision Analysis & Resolution, [ML 3]***
  The purpose of Decision Analysis and Resolution (DAR) is to analyze possible decisions using a formal evaluation process that evaluates identified alternatives against established criteria.
- ***Integrated Project Management + IPPD, [ML 3]***
  The purpose of Integrated Project Management (IPM) is to establish and manage the project and the involvement of the relevant stakeholders according to an integrated and defined process that is tailored from the organization's set of standard processes.
- ***Organizational Training, [ML 3]***
  The purpose of Organizational Training (OT) is to develop the skills and knowledge of people so they can perform their roles effectively and efficiently.
- ***Product Integration, [ML 3]***
  The purpose of Product Integration (PI) is to assemble the product from the product components, ensure that the product, as integrated, functions properly, and deliver the product.

Maturity Level View

- ***Organizational Process Definition + IPPD, [ML 3]***
  The purpose of Organizational Process Definition (OPD) is to establish and maintain a usable set of organizational process assets and work environment standards.
- *IPPD Addition*
  For IPPD, Organizational Process Definition +IPPD also covers the establishment of organizational rules and guidelines that enable conducting work using integrated teams.
- ***Organizational Process Focus, [ML 3]***
  The purpose of Organizational Process Focus (OPF) is to plan, implement, and deploy organizational process improvements based on a thorough understanding of the current strengths and weaknesses of the organization's processes and process assets.
- ***Organizational Process Performance, [ML 4]***
  The purpose of Organizational Process Performance (OPP) is to establish and maintain a quantitative understanding of the performance of the organization's set of standard processes in support of quality and process-performance objectives, and to provide the process performance data, baselines, and models to quantitatively manage the organization's projects.
- ***Quantitative Project Management, [ML 4]***
  The purpose of Quantitative Project Management (QPM) is to quantitatively manage the project's defined process to achieve the project's established quality and process-performance objectives

Maturity Level View

- ***Causal Analysis & Resolution, [ML 5]***
  The purpose of Causal Analysis and Resolution (CAR) is to identify causes of defects and other problems and take action to prevent them from occurring in the future.
- ***Organizational Innovation and Deployment, [ML 5]***
  The purpose of Organizational Innovation and Deployment (OID) is to select and deploy incremental and innovative improvements that measurably improve the organization's processes and technologies. The improvements support the organization's quality and process performance objectives as derived from the organization's business objectives.

The Current Situation

- The “good” guys are independently working to address needs and standards
  - Duplicated cost and effort
  - Lots of standards and best practices
  - Inconsistent levels of detail
  - Build on Standard for Quality as Standard for Assurance

August 7, 2007 “Assurance” Workshop

- Objectives
  - Discuss “Best Practices” for Assurance
  - Identify sources of best practices for assurance
  - Understand Lessons Learned associated with use of assurance processes and practices
  - Understand stakeholder views for deploying practices and addressing assurance in CMMI®
- Participants
  - Government, Industry, Academia
  - Acquirers, vendors, developers, standards organizations, test labs, and research

Existing “Best Practices” for Assurance

- ISO/IEC 15408, Common Criteria for IT Security Evaluation
- ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE CMM)
- ISO/IEC SC22 – *OWG: Vulnerabilities* (OWGV) Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use
- ISO/IEC 15443 (FRITSA), A framework for IT security assurance
- ISO/IEC DTR 19791, Assessment of Operational Systems
- Capability Maturity Model Integration (CMMI®)
- Safety and Security Extensions for Integrated Capability Maturity Models
- And many more ….

Engineering Guidance and Certification Standards

- 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

Engineering Guidance and Certification Standards

- 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
- …

Concerns Expressed at Workshop

- If there is a one size fits all solution, it must be at a level of detail that the context is applicable in diverse contexts (Defense, National Security, Finance, Heath care, Aviations, Telecommunications)
- Implementation of the current model is costly – must be cognizant of increased size/scope of model
- Some individuals feel we don’t need another certification!

Assurance Working Group

- Formed with the objective to "Extend" the CMMI® to include assurance
  - Harmonize various assurance (first step is security) Models
  - Create an Assurance Focus Topic per CMMI® Steering Group Recommendation
- Approach
  - Leverage Security Capability Maturity Models (MSSDM, SSE-CMM) expertise and experience
  - Reference Assurance and Engineering Guidance for compatibility and adoptability
  - Establish a small team to "Harmonize" Assurance Models and perform a gap analysis
  - Engage a second small team to draft "Assurance Focus Topic"

Lockheed Martin's Move to Assurance: SW Safety and Security Certification Best Practices

- Description of the more common SW Safety and Security Engineering and Certification Processes Lockheed Martin programs encounter. Also "how to use" those processes.
- Documented processes apply to specific domains (e.g. Naval Weapon safety certification) some domains are not yet represented.
- 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.

Good Question

“ If your stuff is so important why isn’t it in the CMMI model?”

Claudio Pantaleo

Why Not work on Safety Alone

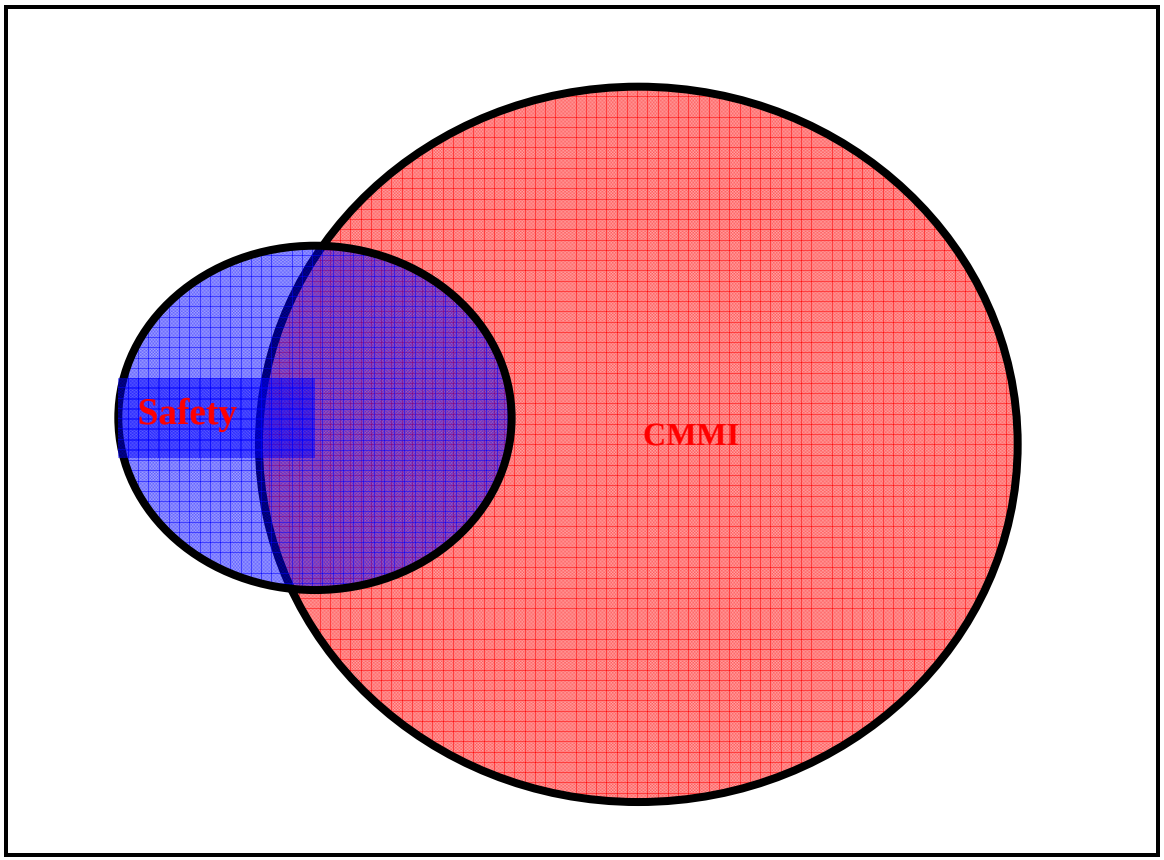
- Politics are complex.
- Thought that the assurance package (safety, security and reliability) will provide a united front and make a better argument for a model change.

How Much Safety is in the Model?

- Everything is already there
- Some is there
- There is nothing there
- Must remember this is a model not a standard

Supporting Material is in the Model - Not Specifics (According to CGM)

Venn Diagram CMMI and Safety practices

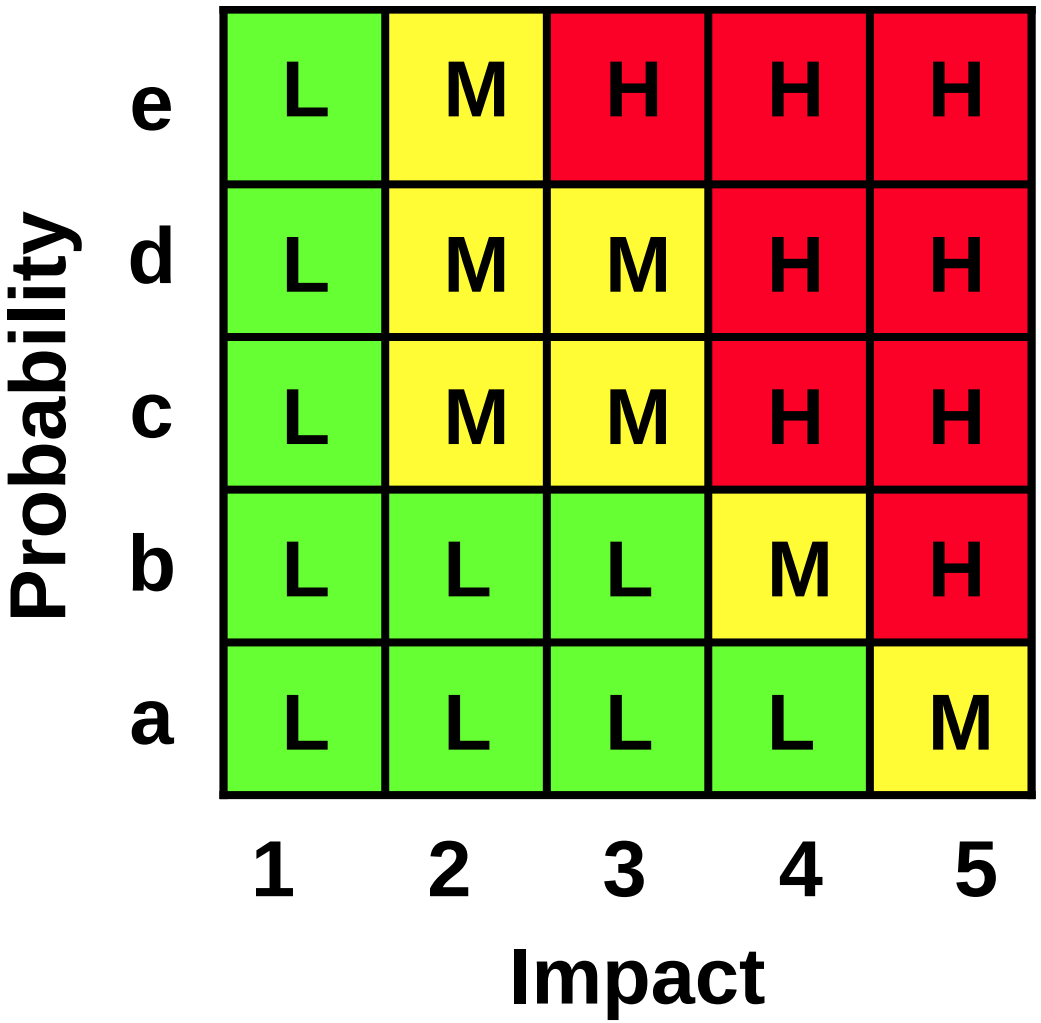


Safety Risk Matrix Example

	HAZARD SEVERITY CATEGORIES			
FREQUENCY OF OCCURRENCE	1 CATASTROPHIC	2 CRITICAL	3 MARGINAL	4 NEGLIGIBLE
A - FREQUENT	0	0	0	0
B - PROBABLE	0	0	0	0
C - OCCASIONAL	0	0	0	0
D - REMOTE	4 1 NSWC, 3 SYSTEM S/W	0	0	0
E - IMPROBABLE	64 7 NSWC, 8 HW, 5 HHA, 43 S/W	5 1 NSWC, 1 HW, 3 HHA	9 7HW, 2 HHA	0

Hazard Risk Index:	Risk Level & Acceptance Authority:
1A, 1B, 1C, 2A, 2B:	HIGH - Acceptance of Risk by the ASN(RDA).
1D, 2C, 3A, 3B:	SERIOUS – Acceptance of Risk by the Program Executive Officer (PEO).
1E, 2D, 2E, 3C, 3D, 3E, 4A, 4B:	MEDIUM – Acceptance of Risk by the Program Manager.
4C, 4D, 4E:	LOW – Acceptance of Risk by the Program Manager.

Project Risk Matrix Example



Results of Risk Comparison

- Perception of risk is different between program and safety (e.g. “don’t talk about anything that is less than 25%”)
- Probability scales are very different
- Descriptions of loss do not correspond very well
- CMMI RSKM should be augmented for safety

Benefits

- Competitive advantage for those with a good safety practice/process.
- Recognition of safety practice in companies.
- Confidence of customer in product.

Next Steps

- Develop Process Reference Model for Assurance.
- Map the Process Reference Model for Assurance to the CMMI-Dev1.2 – identify gaps.
- Make case to SEI for assurance addition to model.
- Streamline Assurance Practices into CMMI Implementations possibly through a Focus Topic.
  - SEI CMMI® Steering Committee Guidelines