

Unique CMMI® Challenges for Information Assurance Processes

Paul D. Nugent, Ph.D.
Lead Information Assurance Engineer
General Dynamics Advanced Information Systems
Paul.Nugent@gd-ais.com

Research Question

- Does the systems engineering discipline of Information Security have unique process implications for CMMI®

Philosophy

- Philosophy of Technology
 - ↗ Heidegger – *The Question Concerning Technology*
 - *Enframing*
 - ↗ Objects as “resources at hand”
 - ↗ Inauthentic way of being
 - Failure to conceive whole object (being)
 - Comparison to ancient Greeks
 - ↗ Ihde
 - Technology as extension of self
 - ↗ Extensions of capability to write, build, destroy, etc.
 - ↗ Implications for experience/identity

Capability and Vulnerability

- Philosophy of technology preoccupied with technology solely as a *capability*
- Fun with etymology
 - ↗ *capax* - “able to hold much”
 - ↗ *capare* - “to take, grasp”
- Yet what is grasping can be challenged, and whatever is held can be taken away
 - ↗ From *vulnerare* (“to wound”) and *vellere* (“pluck, tear”), we get the word *vulnerability*

Vulnerability

- Maple tree example
 - ↗ Capabilities: phloem, xylem, chlorophyll, etc.
 - ↗ Vulnerabilities: wind, flood, parasites, hot, cold, etc.
- Vulnerability inherent to systems
- With the conveniences of networks and Internet communications/services comes high risks
 - ↗ “Frankenstein’s *other* Monster”
- Relationship between capability and vulnerability
- Does vulnerability have special implications for CMMI processes?

Processes Addressing Capability

- Functional Requirements
- States and modes
- System Architecture

Processes addressing Vulnerability

- Are processes to build capability fundamentally different than those to address vulnerability?
 - Safety – vulnerable environment (personnel, cost, schedule, assets)
 - Understanding what the system can do to a passive environment
 - Stable environment
 - Minimal understanding of system by environmental actors
 - Reliability – vulnerability of system to failure
 - Understanding failure modes (properties of materials, stress environments)
 - Stable environment
 - Minimal understanding of system by environmental actors
 - Information Assurance – vulnerability of system to availability, integrity, confidentiality
 - Understanding threats
 - Maximum understanding of environmental actors
 - Example of system scanners – (sensitivity of information about vulnerabilities)
- **Information assurance requires organizational processes focused on understanding the system and understanding the environment**

Understanding

- Understanding the system
 - Special tools (scanners, sniffers, wire shark, etc.)
 - System configuration – accounting/management
- Understanding the environment
 - Information Assurance Vulnerability Management (IAVM)
 - Threat profiles, etc.

CMMI

- CMMI

- Capability Maturity Model Integration

- Processes can (and do) address vulnerability, but emphasis is on capability (documentation, peer reviews, etc.)

- How do you define measurable processes that achieve an understanding of information systems and threat environments?

- What is a defect in this process?
 - Proxies such as exploitable vulnerabilities found?
 - Number of known vulnerabilities/fixes analyzed and applied?

Measurement/Defects

- Is it a defect if a system or organization is not vulnerable at time T_1 , but is vulnerable at time T_2 ?
- A system/organization with no vulnerabilities would have crippled capabilities
 - Tolerance/acceptance of risk
- IA community moving toward “Risk Management” as overall philosophy
 - What is a risk management defect?

Conclusions/Recommendations

- Capability focus is amenable to efficiency
 - Ratio of inputs to outputs (defect rates)
- Vulnerability focus is better addressed by effectiveness
 - Degree to which defined goals are met
- Identify risk management processes/goals
- Migrate from defect focus to risk mitigation focus
- Measure success rate (risks mitigated per risks identified)

- Backup

CMMI Process Areas (Focus)

- Causal Analysis and Resolution Support
- Configuration Management Support
- Decision Analysis and Resolution Support
- Integrated Project Management Project Management
- Measurement and Analysis Support
- Organizational Process Definition Process Management
- Organizational Process Focus Process Management
- Organizational Performance Management Process Management
- Organizational Process Performance Process Management
- Organizational Training Process Management
- Product Integration Engineering
- Project Monitoring and Control Process Management
- Project Planning Process Management
- Process and Product Quality Assurance Process
- Quantitative Project Management Process Management
- Requirements Development Engineering
- Requirements Management Process Management
- Risk Management Process Management
- Supplier Agreement Management Process Management
- Technical Solutions Engineering
- Validation Engineering
- Verification Engineering