Safety and Security Process Measurement

Paul Caseley - DSTL Information Management, UK
Graham Clark, John Murdoch, Tony Powell - Department of Management Studies, University of York, UK

PSM Conference, Denver, 15-17 July 2003
Overview

• Safety and security processes, what are they?
• Why bother measuring these processes?
• Who benefits from safety and security process measures?
• Examples of Safety Measurement
  • A language-based measurement instrument
  • Comparing analysis
  • Potential Indicators
• CMMI and PSM - what’s the future?
Safety and Safety Processes

• Measurement of Safety
  – Concerned with assessing the safety-related risk of operating a product system; assessed throughout the product lifecycle
  – Essentially a risk assessment task, where acceptable residual risk levels are included in specifications and applicable standards
  – Identification and mitigation of Hazards

• Measurement of Safety Processes
  – Concerned with assessing the efficiency and effectiveness of safety processes, e.g. cost of certification following a change
  – Need for more detailed information on performance of safety assessment work
Security and Security Processes

• Measurement of Security
  – Similar to safety, assessing the security-related risk of operating a product system; assessed throughout the product lifecycle
  – Just like safety it is a risk assessment task, where acceptable residual risk levels are included in specifications and applicable standards
  – Identification and mitigation of Vulnerabilities

• Measurement of Security Processes
  – Concerned with assessing the efficiency and effectiveness of security processes
  – Need for more detailed information on performance of security analysis
Who uses safety process measures?

- Business/ organisation senior managers: (Business viewpoint)
  - investment, performance
  - integrated capabilities
  - inter-organisational collaboration,
- Projects: (System development viewpoint)
  - planning, estimating, integration with other processes
  - progress monitoring and management
- Safety Engineers: (Capability viewpoint)
  - efficiency and effectiveness of safety techniques
  - appropriateness of techniques across lifecycle
  - safety process improvement

Equally applicable to Security
An organic approach to measuring

- Effort \(\rightarrow\) Hrs
- Cost \(\rightarrow\) $ 
- Timescale \(\rightarrow\) days
- Quality \(\rightarrow\) defects
- Quantity \(\rightarrow\) LoC

Sub-product

Process

Lifecycle

Technique

Product

Representation

Sub-product
Language based measurement

“Today I checked the prelim HAZOP report for the EF ejection seat, computer”

From a simple language statement up to 18 base measures with context!
Statement construction

<table>
<thead>
<tr>
<th>Process</th>
<th>Action</th>
<th>Representation</th>
<th>LRI/Unit</th>
<th>Sub-Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Contract Support</td>
<td>CLAWZ files</td>
<td>Software-Builds, e.g.</td>
<td>CSCIs, e.g.</td>
</tr>
<tr>
<td>Develop</td>
<td>Compliance Process</td>
<td>X1</td>
<td>Y1</td>
<td></td>
</tr>
<tr>
<td>Identify</td>
<td>Compliance Script</td>
<td>X2</td>
<td>Y2</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Milestone Report</td>
<td>X3</td>
<td>Y3</td>
<td></td>
</tr>
<tr>
<td>Produce</td>
<td>Modified Ada Files</td>
<td>:</td>
<td>:</td>
<td></td>
</tr>
<tr>
<td>Re-Witness</td>
<td>Process Input Ada Files,</td>
<td>:</td>
<td>:</td>
<td></td>
</tr>
<tr>
<td>Run</td>
<td>Staff</td>
<td>:</td>
<td>:</td>
<td></td>
</tr>
<tr>
<td>Witness</td>
<td>tools</td>
<td>:</td>
<td>:</td>
<td></td>
</tr>
<tr>
<td>Tutoring</td>
<td>Z procedure Specifications,</td>
<td>:</td>
<td>:</td>
<td></td>
</tr>
</tbody>
</table>

“In the **Compliance Process**, **Witness the Modified Ada files** for **X2, Y3** “

A record of what actually happened from the person who did it!
An individual engineer’s distribution of activity

Seven Different Projects

Nine Different Processes

226 Measures Ranging from 0.25 to 47.5 hours

Time (Duration of 50 weeks)

Effort (Hours)
- Two or more companies develop the user and system requirement and initial designs.
- After demonstration a company is selected to further develop and manufacture the product
Measuring the processes

• Both teams used the same safety standard
  – Process is risk management (Security/Safety)
  • Hazard Identification
  • Risk Analysis (severity),
  • Risk Assessment (likelihood*Severity = Risk)
  • Risk Reduction
    – Identify security/safety requirements
    – Mitigation identification
    – Implement and verify
Comparing the Hazard Identification Processes

• The hazards from both teams were compared and equivalents identified
  – Using “data sleuthing” comparison method, e.g.
    • Group 1 have 20 hazards, Group 2 have 30 hazards
    • Common hazards = 15
    • proportion of hazards captured $15/30 = 0.5$
    • Possible total hazards $20/0.5 = 40$
  – Note: not the actual data! Results yet to be released.
  – Simple analysis gives some confidence in the quality of the identification process
  – Assumes processes are truly independent
Typical Indicators - requirement effects

- Identify Hazard
- Risk Evaluation
- Risk Assessment
- Risk Reduction
- Mitigation

Derived Requirement Growth

SRD

PHL

PHA

SHA

Project Weeks
Standardized software safety certification methodology for use within the US Navy for all weapon systems, Navy's Weapon System Explosives and Safety Review Board.
# ICM Table: Augmentations v2

<table>
<thead>
<tr>
<th>Common Issue Area</th>
<th>Measurement Category</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule and Progress</td>
<td>Milestone Performance</td>
<td>Milestone Dates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical Path Performance</td>
</tr>
<tr>
<td>Work Unit Progress</td>
<td>Requirements Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Problem Report Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Request Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Component Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Test Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action Item Status</td>
<td></td>
</tr>
<tr>
<td>Incremental Capability</td>
<td>Increment Content - Components</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increment Content - Functions</td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td>Effort</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff Experience</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff Turnover</td>
<td></td>
</tr>
<tr>
<td>Financial Performance</td>
<td>Earned Value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cost</td>
<td></td>
</tr>
<tr>
<td>Environment and Support Resources</td>
<td>Resource Availability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resource Utilization</td>
<td></td>
</tr>
</tbody>
</table>

Minor modifications to the existing ICM descriptions
<table>
<thead>
<tr>
<th>Product Quality</th>
<th>Functional Correctness</th>
<th>Defects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Technical Performance</td>
</tr>
<tr>
<td></td>
<td>Supportability</td>
<td>Time to Restore</td>
</tr>
<tr>
<td></td>
<td>Maintainability</td>
<td>Cyclomatic Complexity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance Actions</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>Utilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Throughput</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timing</td>
</tr>
<tr>
<td></td>
<td>Portability</td>
<td>Standards Compliance</td>
</tr>
<tr>
<td></td>
<td>Usability</td>
<td>Operator Errors</td>
</tr>
<tr>
<td></td>
<td>Dependability - Reliability</td>
<td>Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td>Dependability - Safety</td>
<td></td>
<td>Hazards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hazard Scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure Modes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety Assessments &amp; Assumptions</td>
</tr>
<tr>
<td>Assurance - Safety</td>
<td></td>
<td>Mitigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety Incidents &amp; Accidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety Argument</td>
</tr>
</tbody>
</table>
Conclusion

- Discussed the measurement of safety/security processes
- Identified who would benefit
- Looked at a language/organic based method of measurement
- Discussed the value of comparing processes
- Looked at potential indicators and how they would benefit a project
- A sketched future development for PSM
Contact points:

Dr. John Murdoch  
Department of Management Studies, University of York, UK  
+44 1904 434893  
jm48@york.ac.uk

Paul Caseley  
DSTL Information Management, UK  
+44 1684 77 1476  
prcaseley@dstl.gov.uk