Integration of Common Criteria into the Systems Engineering Process

A developer’s perspective on the application of Common Criteria

29th September 2011
Alexander Haferland, Bundesdruckerei GmbH
Objectives

Motivation for product certification:

- Customer requirements
- Commercial use/ selling point

Challenges for vendors:

- Synchronize with (multiple) Projects
  - Time & costs → sponsorship, time to market
  - Coordination → multiple projects, multiple certifications

- Synchronize with Product Portfolio
  - Customized solutions → re-use of certified products
  - Product changes → Maintenance vs. Re-certification
Common Criteria case example:
Shared responsibilities between developer & supplier

Using external TOE components

**Sponsor**
in-house

**Developer**
in-house, TOE

**Supplier**
external, TOE parts

**Manufacturer**
external

<table>
<thead>
<tr>
<th>ADV, ATE, AGD</th>
<th>ADV, ATE, AGD</th>
<th>ALC</th>
<th>ADV, ATE, AGD</th>
<th>ALC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST</td>
<td>ALC</td>
<td></td>
<td>ST</td>
<td>ALC</td>
</tr>
</tbody>
</table>

Supplying TOE components

**Sponsor**
external

**Developer**
external, TOE

**Supplier**
in-house, TOE parts

**Manufacturer**
external

<table>
<thead>
<tr>
<th>ADV, ATE, AGD</th>
<th>ADV, ATE, AGD</th>
<th>ALC</th>
<th>ADV, ATE, AGD</th>
<th>ALC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALC</td>
<td>ALC</td>
<td></td>
<td>ALC</td>
<td>ALC</td>
</tr>
</tbody>
</table>

Integration of CC into the SEP | 3
Common Criteria case example:
Both scenarios within the same project

Using external TOE components

- **Sponsor**
  - in-house

- **Developer**
  - in-house, TOE

- **Supplier**
  - external, TOE parts

- **Manufacturer**
  - external

- **TOE components**: ADV, ATE, AGD

Supplying TOE components

- **Sponsor**
  - external

- **Developer**
  - external, TOE

- **Supplier**
  - in-house, TOE parts

- **Manufacturer**
  - external

- **TOE components**: ADV, ATE, AGD

ALC
ADV
ATE
AGD
ST
ALC
ADV
ATE
AGD
ST
Common Criteria case example:
Challenges and Pitfalls

- Synchronize ‘document silos’
  - System requirements and SFR
  - System architecture and TSFI, sub-systems and modules
  - Test cases and traceability

- Product Configurations
  - Ensure control of product branches
  - Mapping CC documents to product versions

- Site Visits
  - Different evaluators for same life-cycle documentation
  - Prepare supplier for CC site visits
## Systems Engineering Process: Typical phases and relation to CC artifacts

<table>
<thead>
<tr>
<th>Analysis</th>
<th>Design</th>
<th>Implementation</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define/Refine System</td>
<td>Define/Refine Functional</td>
<td>Technical Realization of Architecture</td>
<td>Build Test Environment</td>
</tr>
<tr>
<td>Requirements</td>
<td>Functional Architecture (Decomposition)</td>
<td>Define/Refine Physical</td>
<td>Functional Testing</td>
</tr>
<tr>
<td>Define/Refine Use Cases</td>
<td>Define/Refine Functional</td>
<td>Interfaces (Internal/External)</td>
<td>Performance Testing</td>
</tr>
<tr>
<td>System Scope &amp; Context</td>
<td>Define/Refine Functional</td>
<td>Control Configuration Items</td>
<td>Regression Testing</td>
</tr>
<tr>
<td>Define/Refine Constraints</td>
<td>Define/Refine Data Flow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>Define/Refine Data Flow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diagram**

- SFR
- TSFI
- Subsystem, Module
- Implementation Representation
- Test Environment
- Test Case
- Test Result
Automation and Integration with Tools

- **Issue Tracking Tools**
  - Documentation tasks, Evaluator comments
  - Testing and bug fixing

- **Source Code Scans (Software)**
  - Source code scan integrated with build system
  - Potential runtime errors & vulnerabilities → Issue Tracker

- **Document Management**
  - Manage information for re-use (Configuration Items)
  - Tools for automation and synchronization
  - Example: ATE document
Project Management Support

- **Evaluation Support Teams**
  - Cross-functional teams for Evaluation support (e.g. for ALC and ATE / AVA)
  - Provide information, address technical issues, etc.
  - Controlled communication between Evaluators and technical experts

- **Multi-Project Coordination**
  - Establish role ‘Project Coordinator’
  - Coordinate across project borders
  - Ensure reporting through metrics
Summary

[Integrate evaluation activities into Systems Engineering Process]
- Combine activities and documentation
- Manage CC artifacts as data objects
- Use tools for support and automation

[Support certifications in multi-project scenarios]
- Reduce manual effort of synchronization and maintenance
- Ensure effective communication of appropriate parties
- Control time and costs through metrics

[Quo Vadis, CC?]
- Support commercial use of CC?
- Database CC part 2 (and 3)?
Thank you!

Do you have any questions