Open source workbench for safety case development.

Matt Barry
Kestrel Technology LLC
Palo Alto, CA
Background

* Trend toward explicit certification approach using arguments over critical system properties, rather than implicit approach of merely following standards and processes
* Need for new tool suites to support argument development and verification
* Safety, assurance, dependability cases
Supporting Experience

* "We’re willing to try this new explicit approach, but..."
* We don’t know cost and effort
* We don’t have examples to follow
* We don’t have integrated tools
* We don’t know if we can trust it
Suite Motivations

- Project management support for case cost, schedule, and resource planning
- Variety of argumentation styles
- Variety of evidence styles
- Case verification and validation analysis support
Approach

* Adopt and implement support for standard meta-models
* Adopt popular feature libraries
* Provide APIs for external tools
* Integrate into Eclipse workbench as either a feature or stand-alone product
* Release to open source community
Tree-based argument editors: outlines, diagnostics, etc.
Graphical argument editors: outlines, diagnostics, etc.
Examples wizard installs copies of useful patterns

Example Details

Contributed Examples

Select a category or example for details

- Pattern
  - Industrial Press p.1
  - Bluetooth p.1
  - Industrial Press p.1
  - Bluetooth p.1
  - Bluetooth p.1
- High-Level Software Safety Argument Pattern 08/06/09
- Software Contribution Safety Argument Pattern 08/06/09
- SSR Identification Software Safety Argument Pattern 08/06/09
- Hazardous Contribution Software Safety Argument Pattern 08/06/09
- Argument Justification Software Safety Argument Pattern 08/06/09
- EUROCONTROL Preliminary Safety Case Model EUROCONTROL S
- EUROCONTROL Preliminary Safety Case Diagram EUROCONTROL

- Document
- Checklist
  - EUROCONTROL SCDM Checklist SCDM 2.1 2006

Example Details

Properties established by example contribution

- Name: CertWare Software Project Management Metrics
- Version: CW SPM 2.3.2011
- Author: Matt Barry
- Applicability: CertWare SPM
- Motivation: Capturing product quality and in-progress indicators for safety case projects
- Intent: Initialize a typical structure of the SPM metrics
- Consequences: Populated model with placeholder data, ready for reapplication and computation
- Implementation: Edit file to populate with change repository, time-keeping, and change order data.

Contributed Resources

Resources to copy into workspace container

- Resource | Description
- Metrics.spm | Metrics model file

Related Documents
Dynamic, Context-Sensitive Help Built-In
Change order model collects statistics for PM metrics
PM metrics captures statistics, trends, and results.
### Commit Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrap Ratio</td>
<td>0.11</td>
</tr>
<tr>
<td>Maturity Ratio</td>
<td>0.89 hr/order</td>
</tr>
<tr>
<td>Maturity Trend</td>
<td>14.29 hr/SLOC-hr</td>
</tr>
<tr>
<td>Maintainability</td>
<td>1890.00</td>
</tr>
<tr>
<td>Rework Ratio</td>
<td>0.06</td>
</tr>
<tr>
<td>Rework Stability</td>
<td>1100.00 SLOC</td>
</tr>
<tr>
<td>Rework Backlog</td>
<td>2.20</td>
</tr>
<tr>
<td>Modularity Trend</td>
<td>14.29</td>
</tr>
<tr>
<td>Modularity Trend</td>
<td>14.29 SLOC/order-hr</td>
</tr>
<tr>
<td>Adaptability Ratio</td>
<td>0.45 hr/SLOC</td>
</tr>
<tr>
<td>Adaptability Trend</td>
<td>0.45 hr/SLOC-hr</td>
</tr>
</tbody>
</table>

### Raw Statistics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Defect Change Orders</td>
<td>12.00 orders</td>
</tr>
<tr>
<td>Normal Defect Change Orders</td>
<td>33.00 orders</td>
</tr>
<tr>
<td>Improvement Change Orders</td>
<td>44.00 orders</td>
</tr>
<tr>
<td>New Feature Change Orders</td>
<td>2.00 orders</td>
</tr>
<tr>
<td>Total Case Size</td>
<td>12000.00 SLOC</td>
</tr>
<tr>
<td>Broken Case Size</td>
<td>1300.00 SLOC</td>
</tr>
<tr>
<td>Fixed Case Size</td>
<td>200.00 SLOC</td>
</tr>
<tr>
<td>Baselined Case Size</td>
<td>500.00 SLOC</td>
</tr>
<tr>
<td>Usage Time</td>
<td>40.00 hrs</td>
</tr>
<tr>
<td>Repair Time</td>
<td>20.00 hrs</td>
</tr>
<tr>
<td>Development Effort</td>
<td>350.00 hrs</td>
</tr>
</tbody>
</table>

**PM metrics view provides values; XML export**
Custom DSL integrates argument items with PM data

```plaintext
argumnetmodel "Industrial Press.arm"
argumnetmodel "Bluetooth.arm"

// roll-up placeholder
plan "line1" element C1 estimated () actual ()

// adding a facility resource to a node
plan "line2" element C1
  estimated (team 'testing' facility "wind tunnel")
  actual (team "testing")

//
plan "line3" element Confidentiality estimated ()
  actual ()
```

- cost
- duration
- facility
- team

- Model Object Planning Notation
- Model Element ID: C1
- Content: C/S logic is fault free

- Description: 41M of 81M
Semi-Formal Proof DSL Provides Another Argument Style
### Statement Validation

Evaluate the statement's validity according to its logical elements below:

<table>
<thead>
<tr>
<th>Premises</th>
<th>Inference</th>
<th>Valid Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConP(x, i) holds by application of either rule 1, or rule 2 with n=0</td>
<td>Hence j1∧...∧jn → x is true</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Premises</th>
<th>Inference</th>
<th>Valid Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppose ConP(x, j1, ..., jn) is gotten by rule 1</td>
<td>Suppose ConP(x, j1, ..., jn) is gotten by application of rule 1 and hypothesis imply &amp; imply implies</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Premises</th>
<th>Inference</th>
<th>Valid Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppose ConP(x, j1, ..., jn) is gotten by rule 2 with n=0</td>
<td>Suppose ConP(x, j1, ..., jn) is gotten by application of rule 2 with n=0 implies &amp; imply implies</td>
<td></td>
</tr>
</tbody>
</table>

### Entailments

<table>
<thead>
<tr>
<th>Deduction entailments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppose ConP(x, j1, ..., jn) is gotten by application of rule 1 and hypothesis imply &amp; imply implies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deduction entailments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppose ConP(x, j1, ..., jn) is gotten by application of rule 2 with n=0 implies &amp; imply implies</td>
</tr>
</tbody>
</table>

### Deduction

<table>
<thead>
<tr>
<th>Deduction given the above entailments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hence j1∧...∧jn → x is true</td>
</tr>
</tbody>
</table>

### Validation

Validate the statement:

- Valid
- Invalid
- Unknown

Previous Author: mb T Time Stamp: Tue Dec 28 18:56:56 CST 2010
Verification Checklist Models Support Case Review
Life-Cycle Integration

Example from: EUROCONTROL SCDM

Example life-cycle requiring tooling integration
Credits

NASA Contract #NNL10AA08C
NASA Langley Research Center
Kestrel Technology LLC