



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

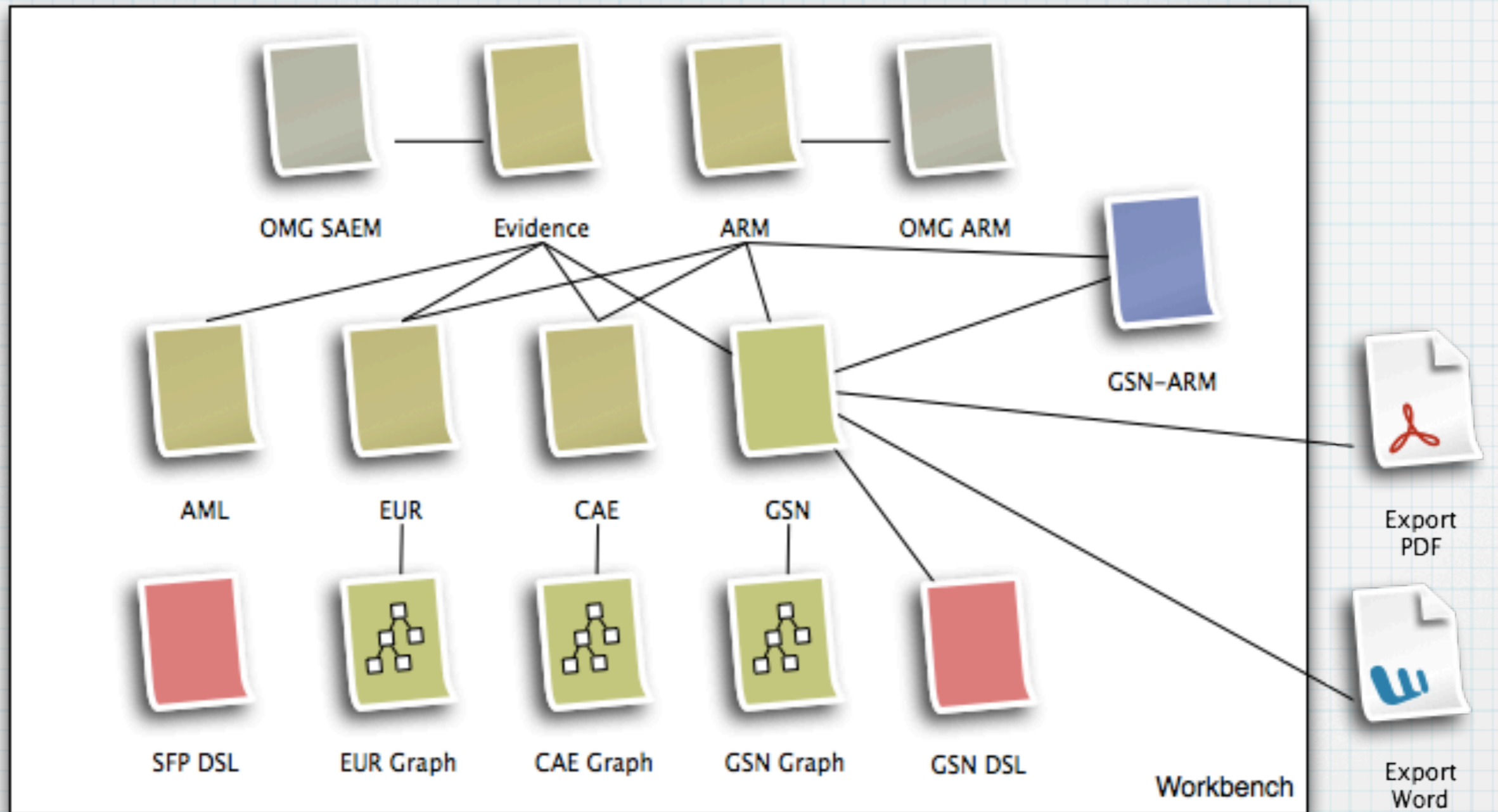
- * “We’re willing to try this new explicit approach, but...”
- * We don’t know cost and effort
- * We don’t have examples to follow
- * We don’t have integrated tools
- * We don’t know if we can trust it

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

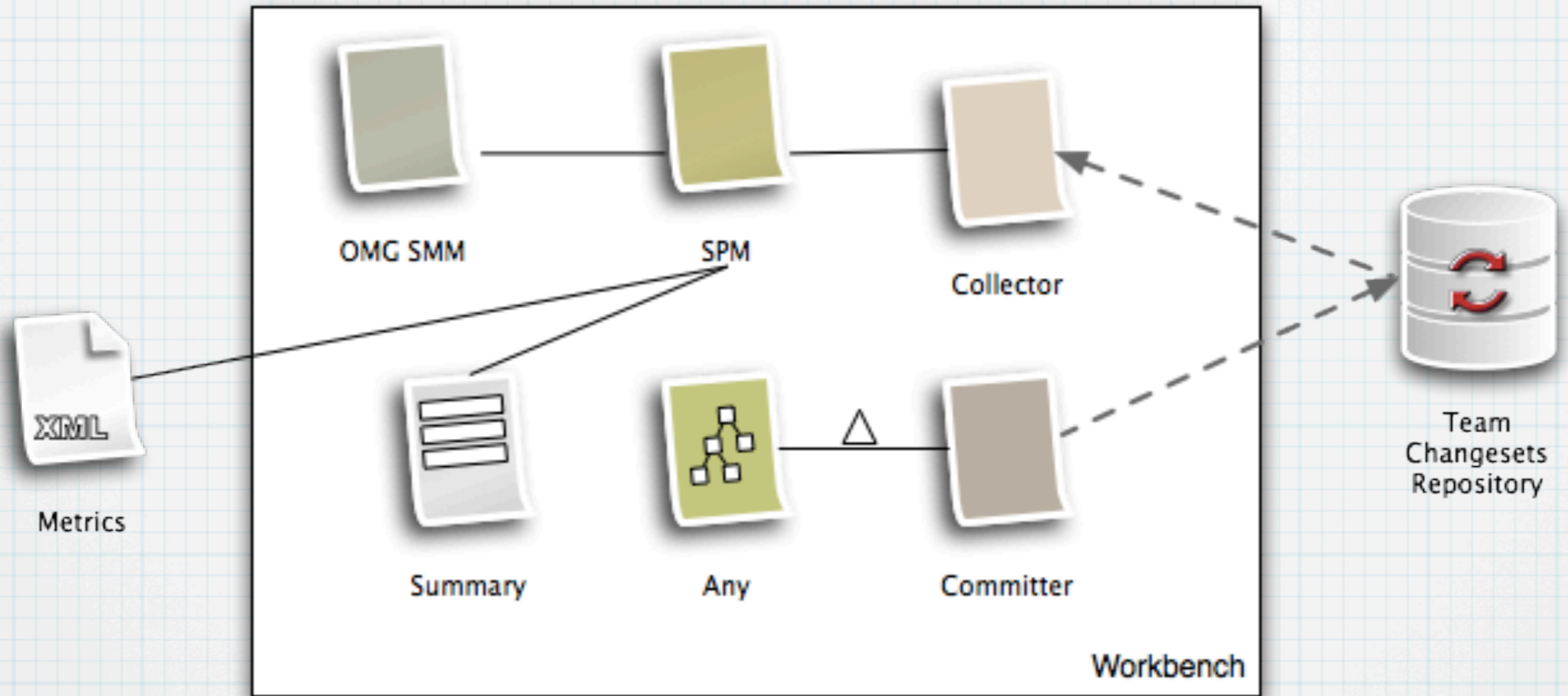
- * Adopt and implement support for standard meta-models
- * Adopt popular feature libraries
- * Provide APIs for external tools
- * Integrate into Eclipse workbench as either a feature or stand-alone product
- * Release to open source community



Legend

- AML: Argument Markup Language
- ARM: Argumentation Metamodel
- ATL: Atlas Transformation Language
- CAE: Claim, Argument, Evidence
- DSL: Domain-Specific Language
- EUR: EUROCONTROL
- GSN: Goal Structuring Notation
- M2M: Model-to-Model
- SAEM: Software Assurance Evidence
- SFP: Semi-Formal Proof

Standard CertWare Model CertWare ATL M2M CertWare DSL Document



ARM: Argumentation Metamodel
 ATL: Atlas Transformation Language
 CPN: CertWare Planning Notation
 DSL: Domain-Specific Language
 GSN: Goal Structuring Notation
 M2M: Model-to-Model
 SMM: Software Measurement Metamodel
 SPM: Software Project Management
 XML: Extensible Markup Language

Legend



Standard



CertWare Model



CertWare View



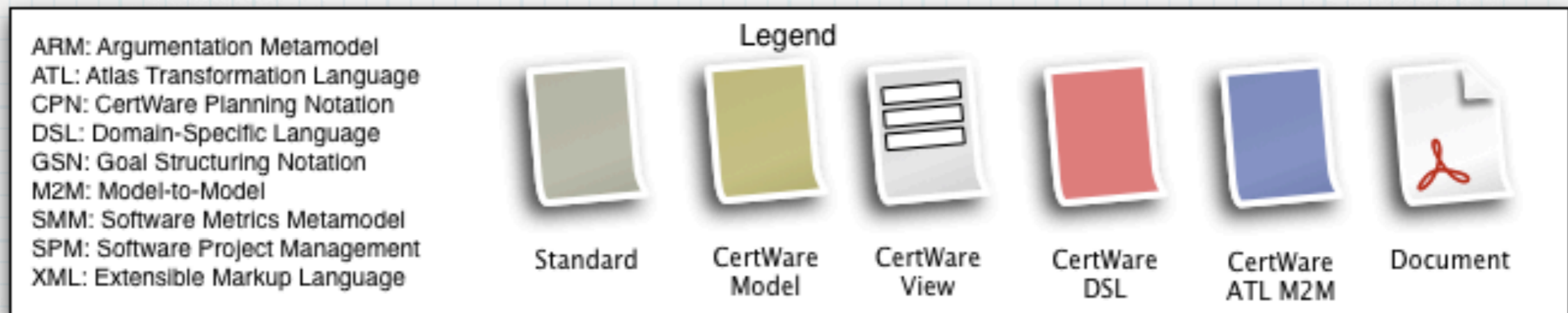
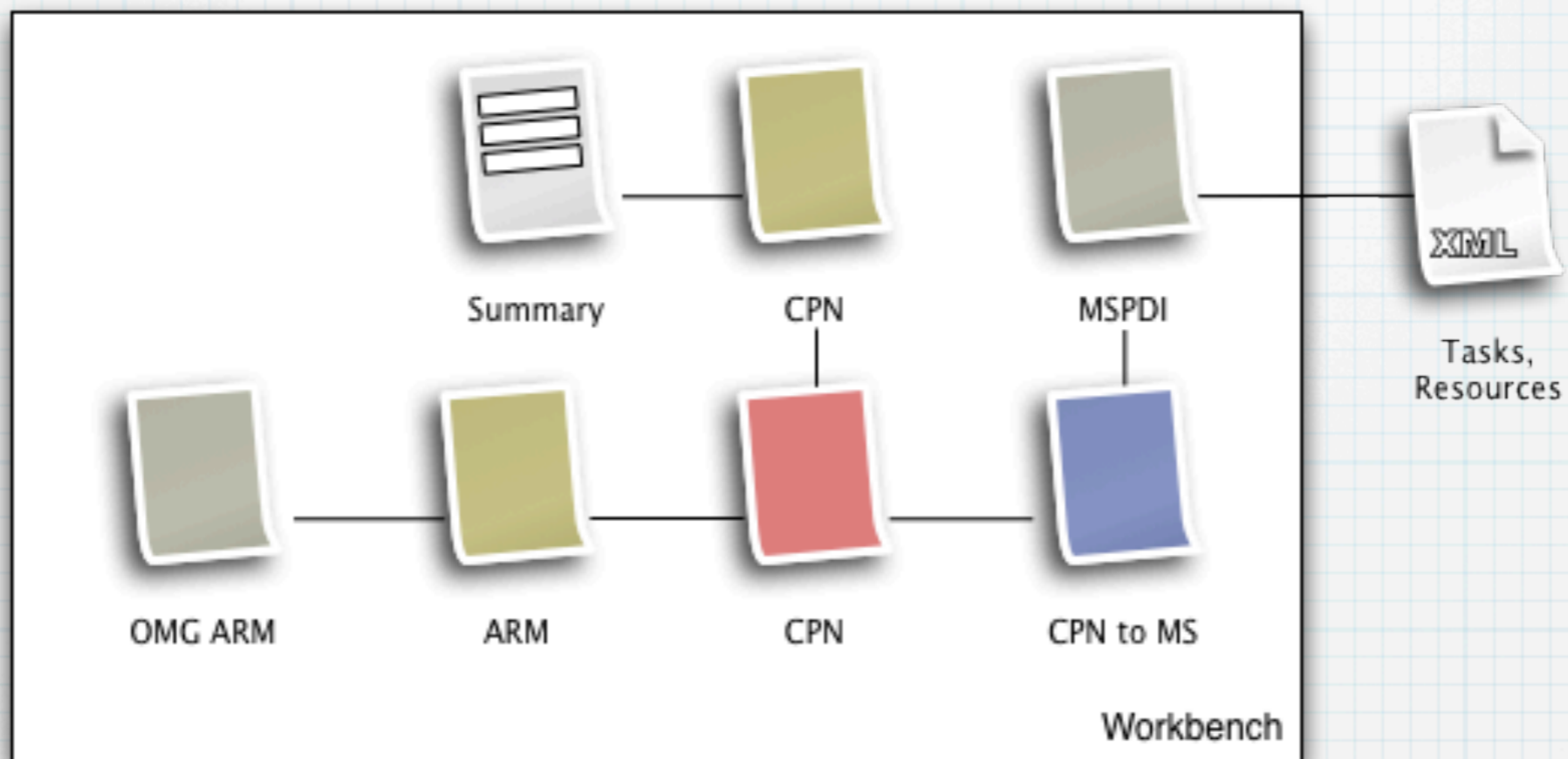
CertWare Java

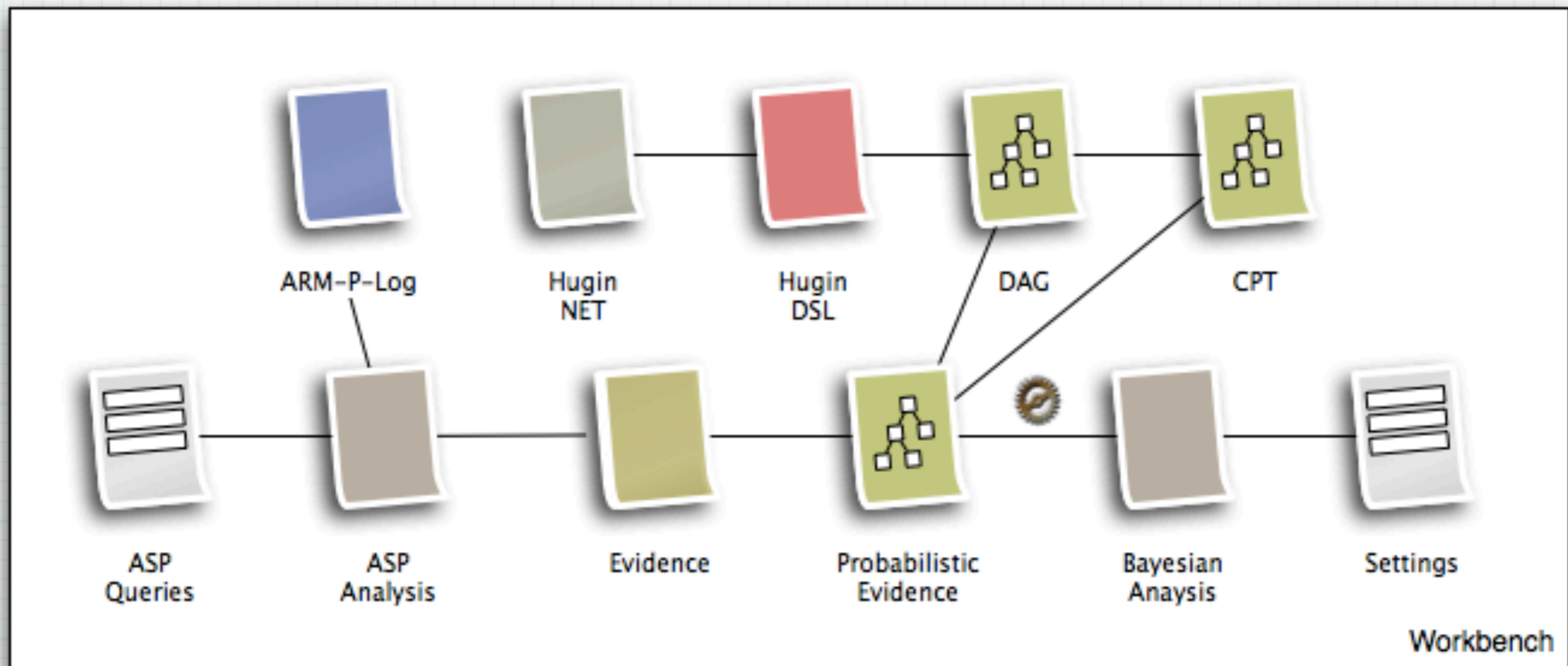


Workbench Plug-in



Document





Legend

- ASP: Answer Set Programming
- CPT: Conditional Probability Table Model
- DAG: Directed Acyclic Graph Model
- DSL: Domain-Specific Language
- M2M: Model-to-Model Transformation
- NET: Hugin NET File API
- P-Log: ASP with Probabilities

- Standard
- CertWare Model
- CertWare View
- CertWare DSL
- Library Java
- CertWare ATL M2M

The screenshot displays a software interface for editing arguments in a tree-based structure. The window title is "Resource - net.certware.test/PSC ADS-B-NRA.eur".

- Project Explorer (Left):** Shows a hierarchical view of the project files, including folders like "net.certware.test" and "org.ssei.bp", and files such as "Bluetooth.arm", "PSC ADS-B-NRA.eur", and "PSC ADS-B-NRA.euz_diagram".
- Main Tree View (Center):** Displays a detailed tree structure of the argument hierarchy. The root is "platform:/resource/net.certware.test/PSC%20ADS-B-NRA.eur". It branches into "Argument Arg 0", "Argument Arg 1", and "Argument Arg 1.1". "Argument Arg 1.1" further branches into "Assumption A002", "Context C001", "Context C003", "Argument Arg 1.1.1", "Argument Arg 1.1.2", "Argument Arg 1.1.3", "Argument Arg 1.1.4", "Argument Arg 1.1.5", "Argument Arg 1.1.6", "Argument Arg 1.1.7", "Criteria Cr001", "Criteria Cr002", "Criteria Cr003", and "Justification J002".
- Outline View (Right):** Provides a condensed overview of the tree structure, listing all nodes from "Argument Arg 0" down to "Context C003".
- Properties Panel (Bottom):** Shows the properties for the selected object, "Argument Arg 1". The fields are:
 - Identifier: Arg 1
 - Description: Section 3.4
 - Content: ADS-B surveillance in NRAs for ATSS has been specified to be acceptably safe
 - IsTagged: (with expand/collapse, add, and delete icons)

At the bottom of the window, a status bar indicates "Selected Object: Argument Arg 1".

Tree-based argument editors: outlines, diagnostics, etc.

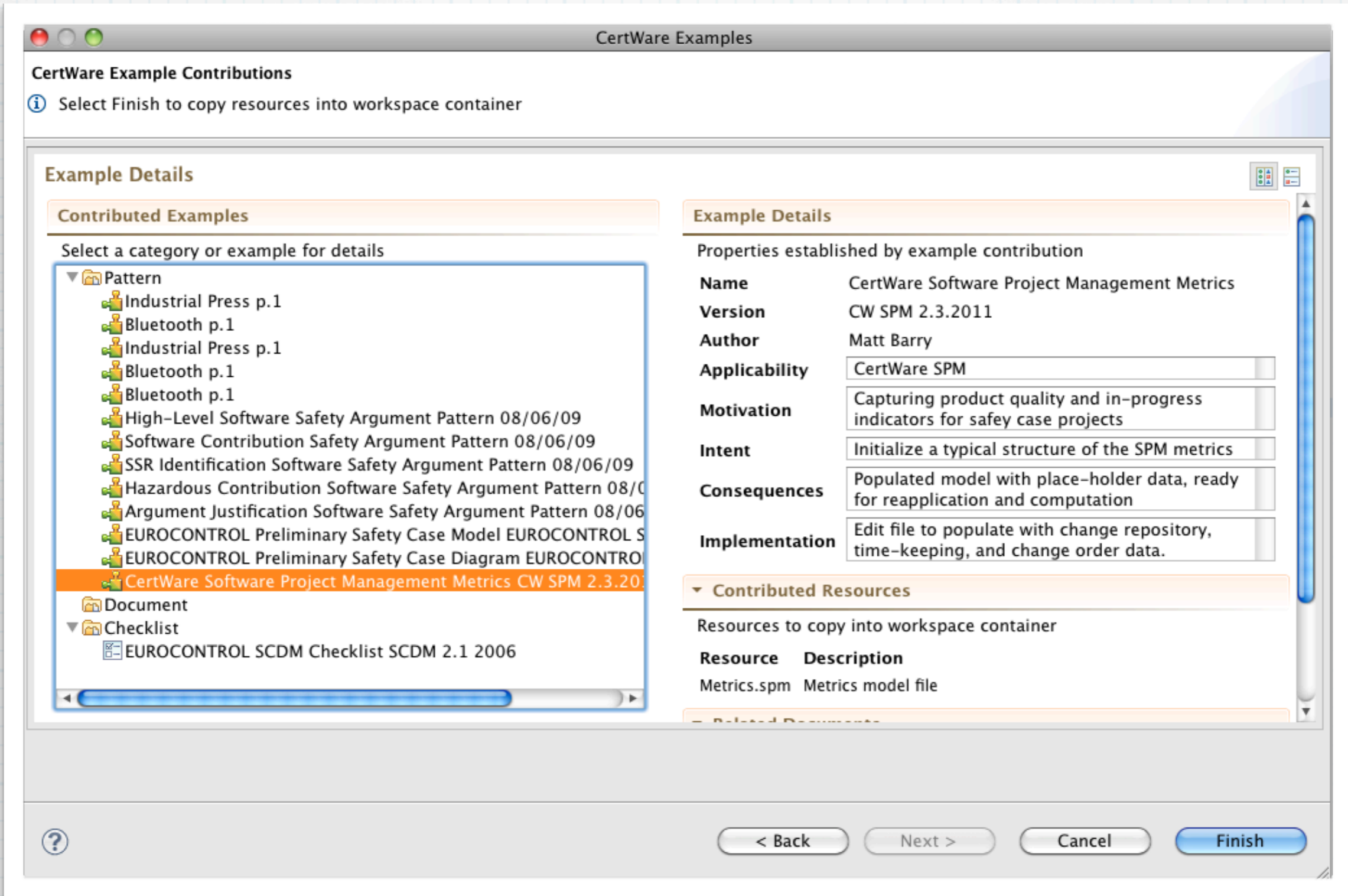
The screenshot displays a graphical argument editor interface. The main workspace shows a diagram with several nodes and their relationships:

- Solution S12** (oval): "PSC NRA section ..."
- Assumption A002** (red diamond): "100% of aircraft are e..."
- Context C003** (dashed box): "ADS-B-NRA appli..."
- Argument Ar...** (green diamonds):
 - "Sufficient guidanc..." (top right)
 - "ADS-B surveillanc..." (middle right)
 - "The differences b..." (bottom left)
 - "Performance for b..." (bottom middle)
 - "The operational i..." (bottom right)
- Justification J...** (white diamond): "When working nor..."

The interface includes several panels:

- Project Explorer** (left): Shows a tree view of project files, including "net.certware.test" and "PSC ADS-B-NRA.eur".
- Palette** (right): Lists node types: Argument Node, Assumption Node, Context Node, Criteria Node, Evidence Node, Justification Node, Solution Node, and Strategy Node.
- Outline** (top right): Shows a small overview of the diagram.
- Properties** (bottom): Shows settings for the selected "Context" node, including "Core" and "Appearance" sections. The "Appearance" section includes "Fonts and Colors" (Lucida Grande, size 9) and "Lines and Arrows" (with icons for line styles and arrowheads).

Graphical argument editors: outlines, diagnostics, etc.



Examples wizard installs copies of useful patterns

The screenshot displays an IDE window titled "Resource - org.ssei.bp/AJSSAP.gsn". The interface includes a Project Explorer on the left, a central editor showing a GSN model tree, and a Help sidebar on the right. The model tree shows a hierarchy: platform:/resource/org.ssei.bp/AJSSAP.gsn > Goal Goal: Justification > Tagged Value visibility > Strategy Start: Justification (selected). The Help sidebar shows "Related Topics" for "GSN Strategy", including a description and a list of links: Strategy Nodes, GSN Notation, Creating Arguments, and Validating Arguments. Below the main editor, there are tabs for Tasks, Properties, Error Log, Problems, Git Repositories, and History. The Properties tab is active, showing fields for Identifier (Start: Justification), Description, Content (Argument over assurance deficits), and IsTagged. A status bar at the bottom indicates "Selected Object: Strategy Start: Justification".

Dynamic, Context-Sensitive Help Built-In

The screenshot displays the CertWare application interface. On the left, the Project Explorer shows a tree view of project files, including 'net.certware.verify' and 'Verify.sco'. The main workspace is divided into several panes: 'Verify.sco' showing an 'Artifact List' with items like 'Critical Defect Change Orders Critical', 'Normal Defect Change Orders Normal', 'Improvement Change Orders Improvements', and 'New Feature Change Orders NewFeatures'; 'Outline' showing a hierarchical view of the same artifacts; 'Properties' showing a table with 'Property' and 'Value' columns; 'CertWare Planning' and 'Software Chang...' tabs; and 'Problems' and 'Error Log' panes, both showing '0 items'. At the bottom, a status bar indicates '37M of 81M'.

| Property | Value |
|----------|-------|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Change order model collects statistics for PM metrics

The screenshot displays the CertWare IDE interface with several panels:

- Project Explorer:** Shows a tree view of project files, including 'Verify.spm' and 'Verify.spm CW'.
- Verify.spm View:** A hierarchical tree of project metrics, with 'Adaptability Ratio Measure Adaptability Ratio' selected.
- Properties Panel:** Displays 'Software Project Management Metrics' for the selected object, showing a table of metrics.
- Outline Panel:** Shows the overall project structure, including 'Project Model' and 'Project Commit'.
- Problems/Errors Panel:** Currently empty, showing '0 items'.

Software Project Management Metrics Table:

| Commit Metrics | |
|-----------------|------------------|
| Scrap Ratio | 0.11 |
| Maturity Ratio | 0.89 hr/order |
| Maturity Trend | 14.29 hr/SLOC-hr |
| Maintainability | 1890.00 |
| Rework Ratio | 0.06 |

Verify.spm CW Properties Table:

| | |
|-----------------------|---------|
| Adaptability Ratio | 0.45 |
| Adaptability Trend | 0.45 |
| Maintainability Ratio | 1890.00 |
| Maturity Ratio | 0.89 |
| Maturity Trend | 14.29 |
| Modularity Ratio | 14.29 |
| Modularity Trend | 14.29 |
| Rework Backlog | 2.20 |
| Rework Ratio | 0.06 |
| Rework Stability | 1100.00 |
| Scrap Ratio | 0.11 |

PM metrics captures statistics, trends, and results

Tasks Properties Software Project Management Metrics

Software Project Management Metrics

Project Commits

Project commit (N/A)

Commit Metrics

| | |
|--------------------|---------------------|
| Scrap Ratio | 0.11 |
| Maturity Ratio | 0.89 hr/order |
| Maturity Trend | 14.29 hr/SLOC-hr |
| Maintainability | 1890.00 |
| Rework Ratio | 0.06 |
| Rework Stability | 1100.00 SLOC |
| Rework Backlog | 2.20 |
| Modularity | 14.29 |
| Modularity Trend | 14.29 SLOC/order-hr |
| Adaptability Ratio | 0.45 hr/SLOC |
| Adaptability Trend | 0.45 hr/SLOC-hr |

Raw Statistics

| | |
|-------------------------------|---------------|
| Critical Defect Change Orders | 12.00 orders |
| Normal Defect Change Orders | 33.00 orders |
| Improvement Change Orders | 44.00 orders |
| New Feature Change Orders | 2.00 orders |
| Total Case Size | 12000.00 SLOC |
| Broken Case Size | 1300.00 SLOC |
| Fixed Case Size | 200.00 SLOC |
| Baselined Case Size | 500.00 SLOC |
| Usage Time | 40.00 hrs |
| Repair Effort | 20.00 hrs |
| Development Effort | 350.00 hrs |

PM metrics view provides values; XML export

CertWare - net.certware.verify/Verify.cpn -

Project Explorer

- com.kt.psc.comodel [runtime]
- net.certware.blank [runtime]
- net.certware.dsl
- net.certware.sfpr [runtime]
- net.certware.test [runtime]
- net.certware.test.dsl
- net.certware.verify [runtime]
 - AJSSAP.gsn CW
 - AJSSAP.textile
 - Bluetooth.arm CW
 - Eurocontrol.vcl CW
 - Eurocontrol SCDM App
 - Industrial Press.arm CW
 - My.mspdi CW
 - My.smm CW
 - PSC ADS-B-NRA.eur CW
 - SCSAP.gsn CW
 - SCSAP.textile
 - SCSAP 22.png
 - SCSAP 23.png
 - Verify.cpn CW
 - Verify.sco CW
 - Verify.spm CW
- org.ssei.bp [runtime-CertWare]

*Verify.cpn

```

1 argumentmodel "Industrial Press.arm"
2 argumentmodel "Bluetooth.arm"
3
4 // roll-up placeholder
5 plan "line1" element C1 estimated () actual ()
6
7 // adding a facility resource to a node
8 plan "line2" element C1
9   estimated (team "testing" facility "wind tunnel" )
10  actual (team "testing")
11
12 //
13 plan "line3" element Confidentiality estimated (
14   ) actual (
15   )
16
17   cost
18   duration
19   facility
20   team
  
```

Outline

- Industrial Press.arm
- Bluetooth.arm
- line1
- line2
 - testing
 - testing
- line3

Properties CertWare Planning

CertWare Planning Notation

| Model Objects | Plan |
|------------------------------|---------------------------------|
| Argument Models Industrial P | Plan ID line1 |
| Argument Models Bluetooth.a | Model Element ID C1 |
| Plan line1 | Content C/S logic is fault free |
| Plan line2 | Description |
| Plan line3 | |

Problems Error Log

0 items

Writable Insert 14 : 1 41M of 81M

Custom DSL integrates argument items with PM data

Project Explorer

- com.kt.psc.comodel [runtime-...]
- net.certware.blank [runtime-...]
- net.certware.dsl [runtime-...]
- net.certware.sfpr [runtime-...]
- allmen.sfp
- battery.sfp
- engine.sfp
- nachi.sfp
- primes.sfp
- PSC ADS-B-NRA.sfp
- safety.sfp
- socrates.sfp
- net.certware.test [runtime-...]
- net.certware.test.dsl
- net.certware.verify [runtime-...]
- org.ssei.bp [runtime-CertW...]

engine.sfp

```

1 // @author nachi original in thesis
2 // @author mrb reapply in certware plugins
3
4 // From Nachiappan 2008
5 // Lemma 1: (conj(S1) -> k1) ^ ... ^ (Conj(Sm) -> km) -> conj(S1 U...U Sm) -> k1 ^...^ km.
6 // Lemma 2: (conj(S) -> x) -> (conj(S1{S1,...,sm}) -> (s1^...^sm) -> x)).
7 // Definition: An inference (c,{j1,...,jn}) is sound if the proposition j1^...^jn -> c is true.
8 // Definition: A proof P is a valid proof of x if all inferences of P are sound and P is a struct
9 // Definition: P is a structurally valid proof of x if P proves x relative to {}.
10
11 Theorem: "Given a proof P, in which all inferences are sound, and proposition x,
12 if ConP(x,{j1,...,jn}) gotten by finitely many application of rules 1, 2, or 3
13 then j1^...^jn -> is true" (13,1^14 -> 33)
14
15 1. "Suppose we have a proof P, in which all inferences are sound,
16 and suppose x is a proposition" (hypothesis)
17
18 2. "Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rules 1 or 2 or 3" (hypothesis)
19 3. "ConP(x,{}) holds by application of either rule 1, or rule 2 with n=0" (2)
20 4. "Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 1" (hypothesis)
21 5. "ConP(x,{j1,...,jn}) = ConP(x,{x})" (4)
22 6. "x -> x is true" ("Definition of implication")
23 7. "Hence j1^...^jn -> x is true" (5,6)
24 8. "Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 2 with n=0" (hypothesis)
25 9. "(x,{}) is an inference of P" (8)
26 10. "True -> x is true" (1,9,"Definition of sound inference")
27 11. "Hence j1^...^jn -> x is true" (8,9,10)
28 12. "Hence j1^...^jn -> x is true" (3,4->7,8->11)
29
30 13. "Whenever P is a proof all of whose inferences are sound,
31 and ConP(x,{j1,...,jn}) is gotten by 1 application of rules 1 or 2 or 3,
32 then j1^...^jn -> x is true" (1^2 -> 12)

```

Outline

- "Given a proof P, in which all

Tasks Properties Error Log Problems History

Workspace Log

| Message | Plug-in | Date |
|---------|---------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

29M of 81M

Semi-Formal Proof DSL Provides Another Argument Style

Select a statement to review

Proof Statement Validation

Proof Statements

Select a statement to review

- ▼ Theorem: "Given a proof P, in which all inferences are sound, and proposition x,
 - 1. "Suppose we have a proof P, in which all inferences are sound,
 - 2. "Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by 1 application of rules 1 or 2 or 3" (hypothesis)
 - 3. " $\text{ConP}(x, \{j\})$ holds by application of either rule 1, or rule 2 with $n=0$ "
 - 4. "Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by 1 application of rule 1" (hypothesis)
 - 5. " $\text{ConP}(x, \{j_1, \dots, j_n\}) = \text{ConP}(x, \{x\})$ "
 - 6. " $x \rightarrow x$ is true"
 - 7. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true"
 - 8. "Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by 1 application of rule 2 with $n=0$ " (hypothesis)
 - 9. " $(x, \{j\})$ is an inference of P"
 - 10. "True $\rightarrow x$ is true"
 - 11. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true"
 - 12. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true"
 - 13. "Whenever P is a proof all of whose inferences are sound,
 - 14. "By induction hypothesis, we suppose that P is a proof all of whose inferences are so
 - 15. "Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by N+1 application of rules 1 or 2 or 3" (hypot
 - 16. "Suppose $\text{ConP}(x', \{j_1, \dots, j_n\})$ is gotten by N+1 application of rules 1 or 2 or 3" (hypot
 - 17. " $\text{ConP}(x', \{j_1, \dots, j_n\}) = \text{ConP}(x', \{x'\})$ "
 - 18. " $x' \rightarrow x'$ is true"
 - 19. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x'$ is true"
 - 20. "Suppose $\text{ConP}(x', \{j_1, \dots, j_n\})$ is gotten by N+1 applications,
 - 21. " $(X_1, \{j_1, \dots, j_m\})$ is a sound inference of P, and $\text{ConP}(j_i, S_i)$
 - 22. " $j_1 \wedge \dots \wedge j_m \rightarrow x$ "
 - 23. " $(\text{conj}(S_1) \rightarrow j_1) \wedge \dots \wedge (\text{conj}(S_m) \rightarrow j_m)$ is true"
 - 24. " $\text{conj}(S_1 \cup \dots \cup S_m) \rightarrow j_1 \wedge \dots \wedge j_m$ "
 - 25. " $\text{conj}(S_1 \cup \dots \cup S_m) \rightarrow x'$ is true"
 - 26. "Hence $j_1 \wedge \dots \wedge j_m \rightarrow x'$ is true"
 - 27. "Suppose $\text{ConP}(x', \{j_1, \dots, j_n\})$ is gotten by N+1 applications,
 - 28. "There exists $\{s_1, \dots, s_n\}$, S and proposition x, where x' is
 - 29. " $\text{conj}(S) \rightarrow x$ is true"
 - 30. " $\text{conj}(S | \{s_1, \dots, s_n\}) \rightarrow (s_1 \wedge \dots \wedge s_n \rightarrow x)$ is true"
 - 31. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x'$ is true"
 - 32. "Hence $j_1 \wedge \dots \wedge j_n \rightarrow x_1$ is true"
 - 33. "Whenever $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by N+1 application

Statement Validation

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

Premises

Inference Premise:

| | |
|---|----------------|
| Valid Statement | Comment |
| <input checked="" type="checkbox"/> $\text{ConP}(x, \{j\})$ holds by application of either rule 1, or rule 2 with $n=0$ | |

Inference

Inference given the above premises:

| | |
|--|----------------|
| Valid Statement | Comment |
| <input type="checkbox"/> Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true | |

Entailments

Deduction entailments:

| | |
|--|----------------|
| Valid Statement | Comment |
| <input checked="" type="checkbox"/> Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by 1 application of rule 1 | hypothesis |

Implies
 Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true

| | |
|---|----------------|
| Valid Statement | Comment |
| <input checked="" type="checkbox"/> Suppose $\text{ConP}(x, \{j_1, \dots, j_n\})$ is gotten by 1 application of rule 2 with $n=0$ | hypothesis |

Implies
 Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true

Deduction

Deduction given the above entailments:

| | |
|--|----------------|
| Valid Statement | Comment |
| <input type="checkbox"/> Hence $j_1 \wedge \dots \wedge j_n \rightarrow x$ is true | |

Validation

Validate the statement:

Valid Invalid Unknown

Previous Author Time Stamp



Help

< Back

Next >

Cancel

Finish

Semi-Formal Proof Review Wizard Facilitates V&V

Resource - net.certware.verify/Eurocontrol SCDM AppC.vcl - Eclipse SDK

Project Explorer

- net.certware.test [runtime-CertWare]
- net.certware.test.dsl
- net.certware.verify
 - Eurocontrol SCDM AppC.vcl
 - Items 42
 - Unknown 42

Eurocontrol SCDM AppC.vcl

- platform:/resource/net.certware.verify/Eurocontrol%20SCDM%20AppC.vcl
 - Checklist EUROCONTROL SCM APP.C
 - Category Safety Case Presentation: General
 - 1 Is the aim of the Safety Case explained and clear?
 - 2 Is the purpose of the Safety Case explained and clear?
 - 3 Is the scope of the Safety Case explained and clear?
 - 4 Is a justification given as to why the introduction of the change is necessary?
 - 5 Is the system and its environment completely and correctly described and bounded?
 - 6 Is the operational concept described?
 - 7 Is the regulatory context described?
 - 8 Is the safety case structured along the lines of the argument?
 - 9 Is the argument structure apparent in the layout of each of the core sections?
 - Category Argument Structure
 - 10 Is the overall claim a single, clear and unambiguous statement of what the safety case is trying to demonstrate?
 - 11 Is the claim expressed in a positive way, does it accept the "burden of proof"?
 - 12 Is the context clear?
 - 13 Are the criteria for being "acceptably safe" appropriate and adequately specified?
 - 14 Are the initial assumptions explicitly stated?
 - 15 Is the decomposition of the argument structure adequately explained by "Strategies"?
 - 16 Is the level of decomposition appropriate to the complexity of the safety case and/or evidence?
 - 17 Is each level of decomposition necessary and sufficient to show that the parent argument is true?
 - 18 Is each argument set out as a simple predicate?
 - 19 Is the argument structure free of negative and inconclusive arguments?
 - 20 Does the argument structure appear to be immune to possible counter-arguments which could undermine the argument?
 - 21 Is the distinction between product- and process-based arguments clear?
 - 22 Are arguments supposedly related to the observable properties of the related product actually addressing those properties?
 - 23 Are arguments supposedly related to the observable properties of the related processes which generated the product actually addressing those properties?
 - 24 Are direct arguments and evidence supported by enough backing arguments and evidence to give sufficient support to the claim?
 - 25 Where process-based arguments are used as direct arguments, is this appropriate?
 - 26 Is each branch of the safety argument structure terminated in evidence?
 - Category Evidence
 - 27 Is all the presented evidence necessary to support the argument to which it relates?
 - 28 Is all the presented evidence clear, objective, relevant and conclusive in showing the related argument to be true?

Tasks | Properties | Error Log | Problems | History

Base

Properties

Identifier : 1

Description : Is the aim of the Safety Case explained and clear?

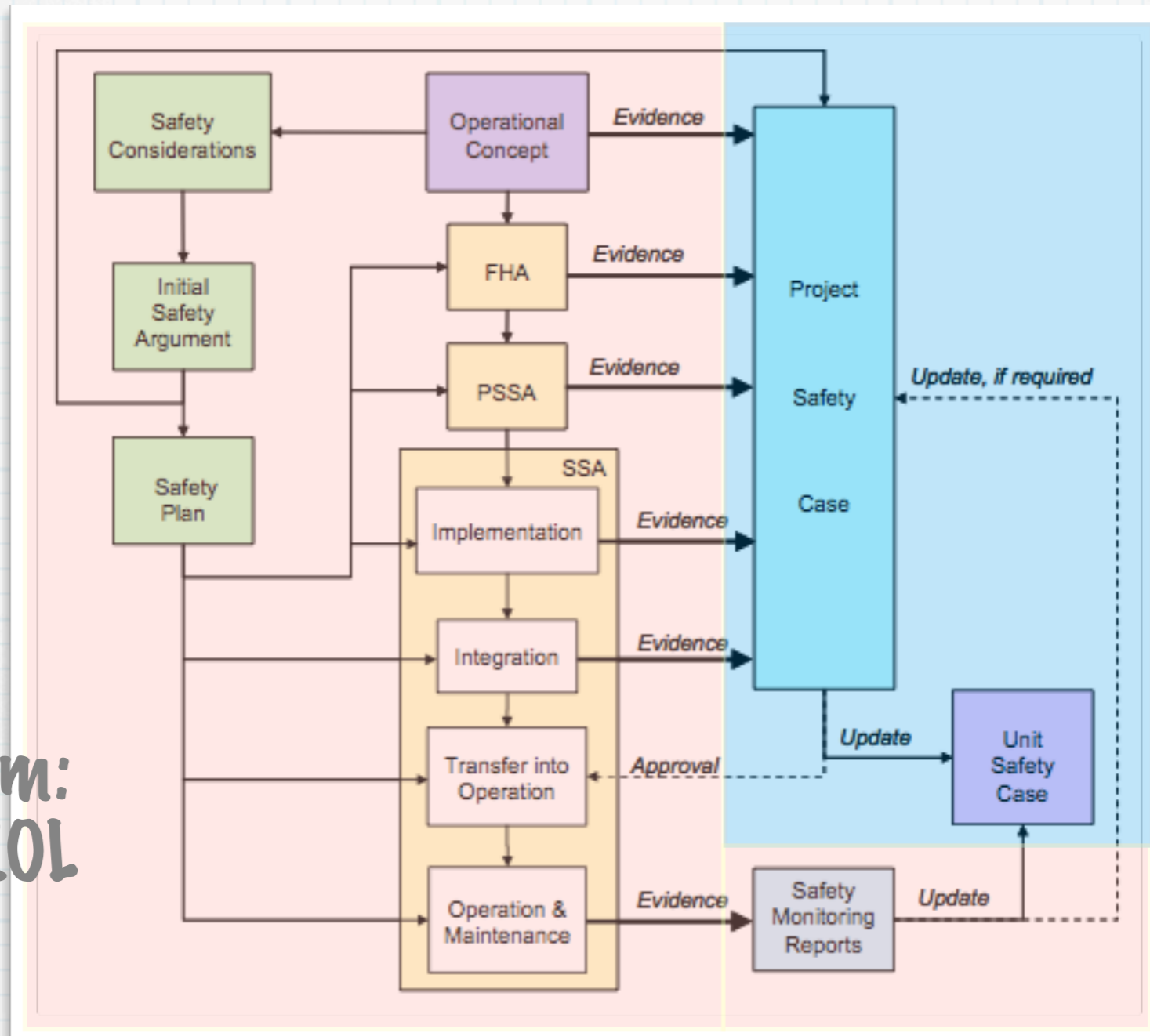
Reference : 2/3

Result : UNKNOWN
 NO
 YES
 NA

Comment :

Verification Checklist Models Support Case Review

Life-Cycle Integration



Example from:
EUROCONTROL
SCDM

Example life-cycle requiring tooling integration

Credits

**NASA Contract #NNL10AAA08C
NASA Langley Research Center
Kestrel Technology LLC**