Open source workbench for safety case development.

Matt Barry
Kestrel Technology LLC
Palo Alto, CA

IEEE Aerospace Conference 2001 - 13.0413 - #1182

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

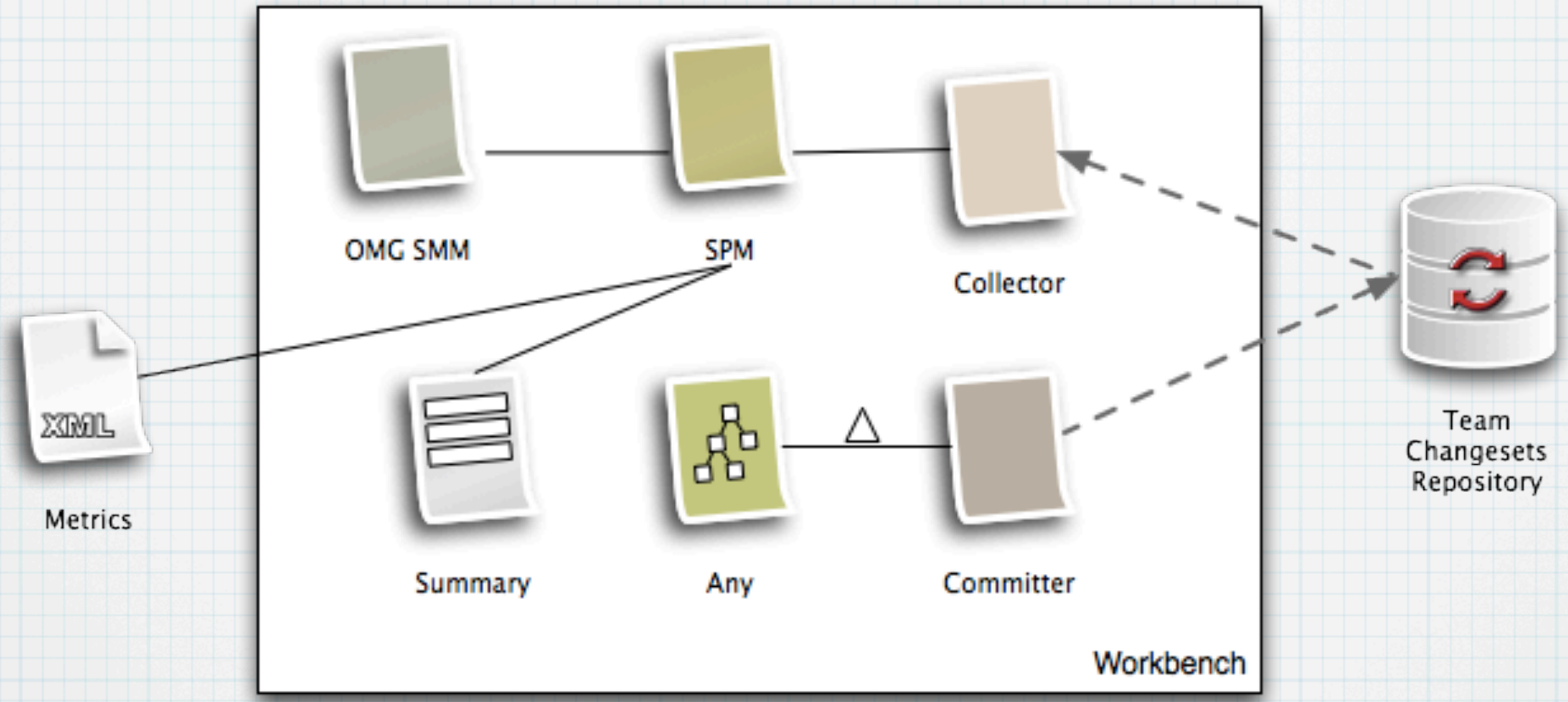
* Adopt and implement support for standard meta-models
* Adopt popular feature libraries
* Provide APIs for external tools
* Integrate into Eclipse workbench as either a feature or stand-alone product
* Release to open source community

OMG SAEM
Evidence
ARM
OMG ARM
GSN-ARM
AML
EUR
CAE
GSN
Export PDF
SFP DSL
EUR Graph
CAE Graph
GSN Graph
GSN DSL
Workbench
Export Word

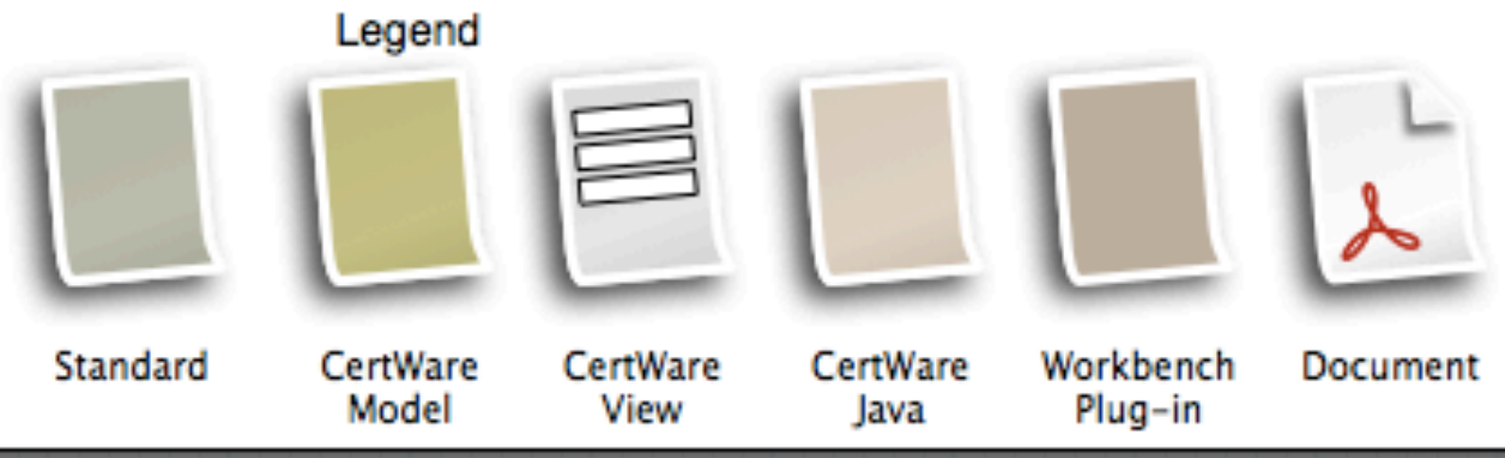
AML: Argument Markup Language
ARM: Argumentation Metamodel
ATL: Atlas Transformation Language
CAE: Claim, Argument, Evidence
DSL: Domain-Specific Language
EUR: EUROCONTROL
GSN: Goal Structuring Notation
M2M: Model-to-Model
SAEM: Software Assurance Evidence
SFP: Semi-Formal Proof

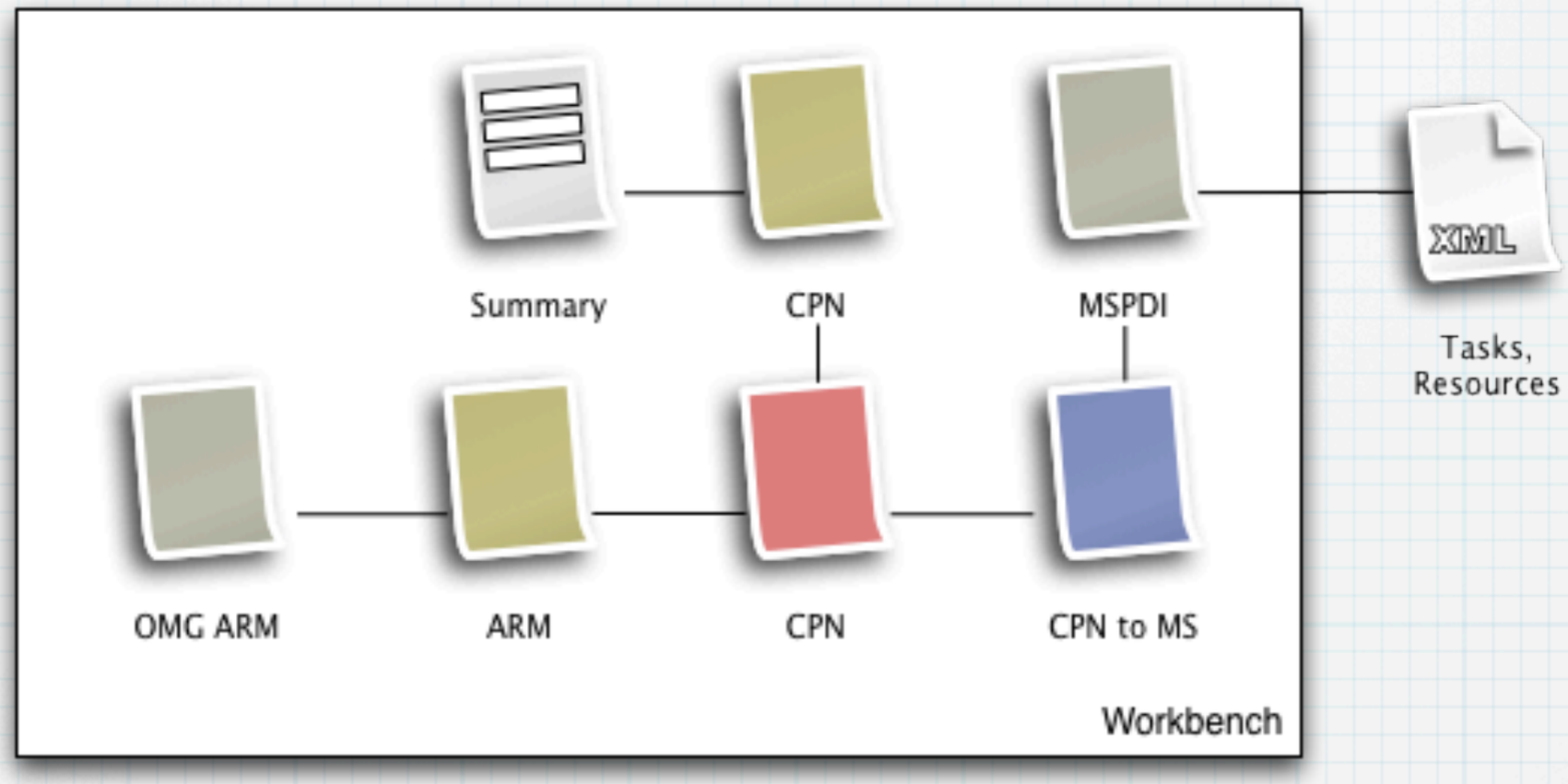
Legend

Standard
CertWare Model
CertWare ATL M2M
CertWare DSL
Document

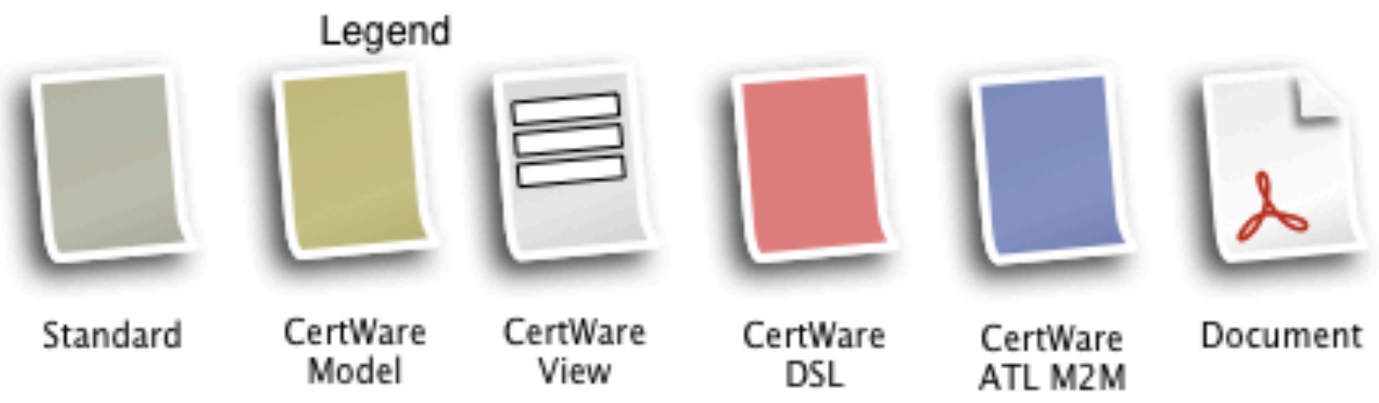


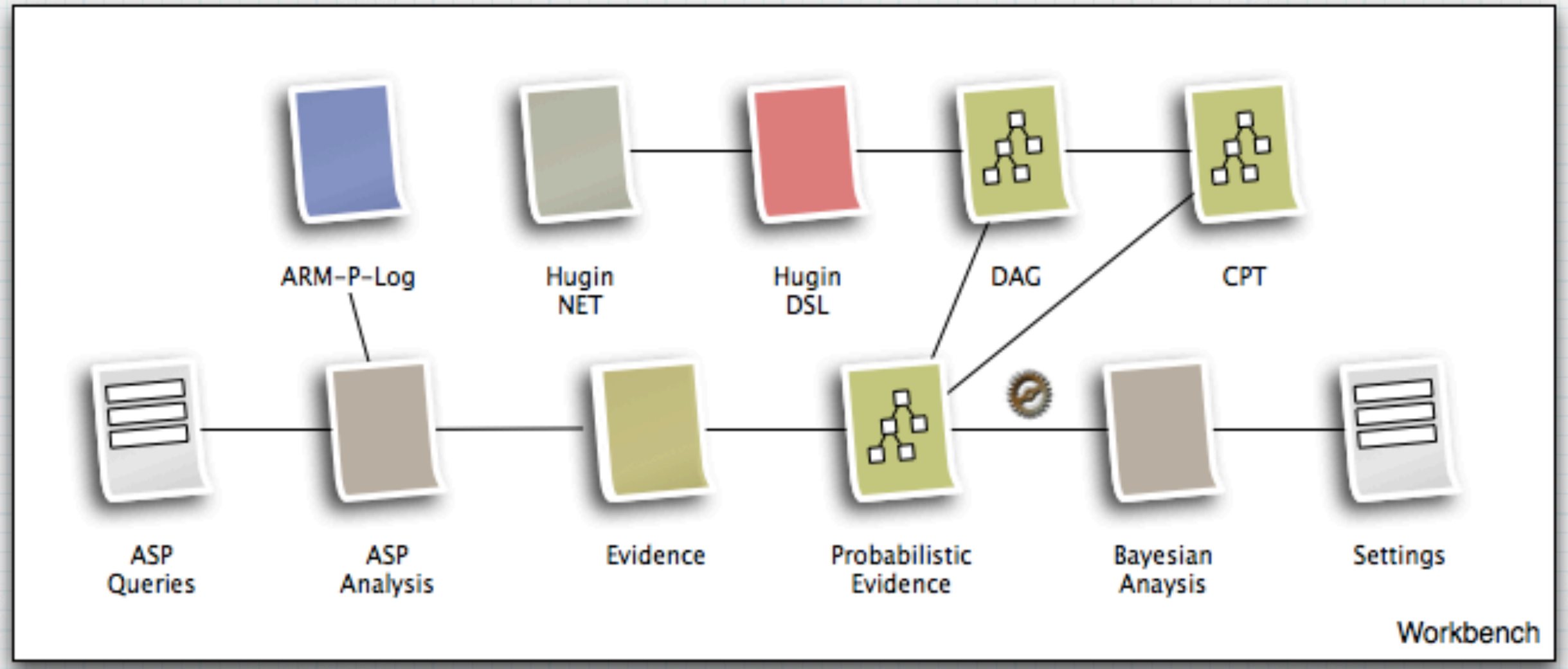
ARM: Argumentation Metamodel
ATL: Atlas Transformation Language
CPN: CertWare Planning Notation
DSL: Domain-Specific Language
GSN: Goal Structuring Notation
M2M: Model-to-Model
SMM: Software Measurement Metamodel
SPM: Software Project Management
XML: Extensible Markup Language



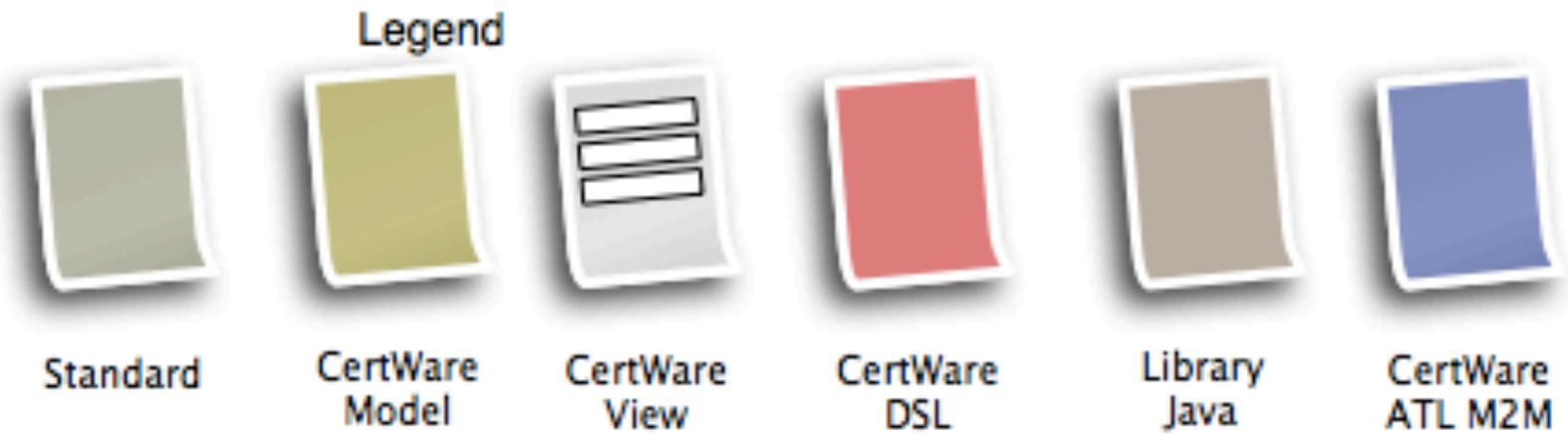


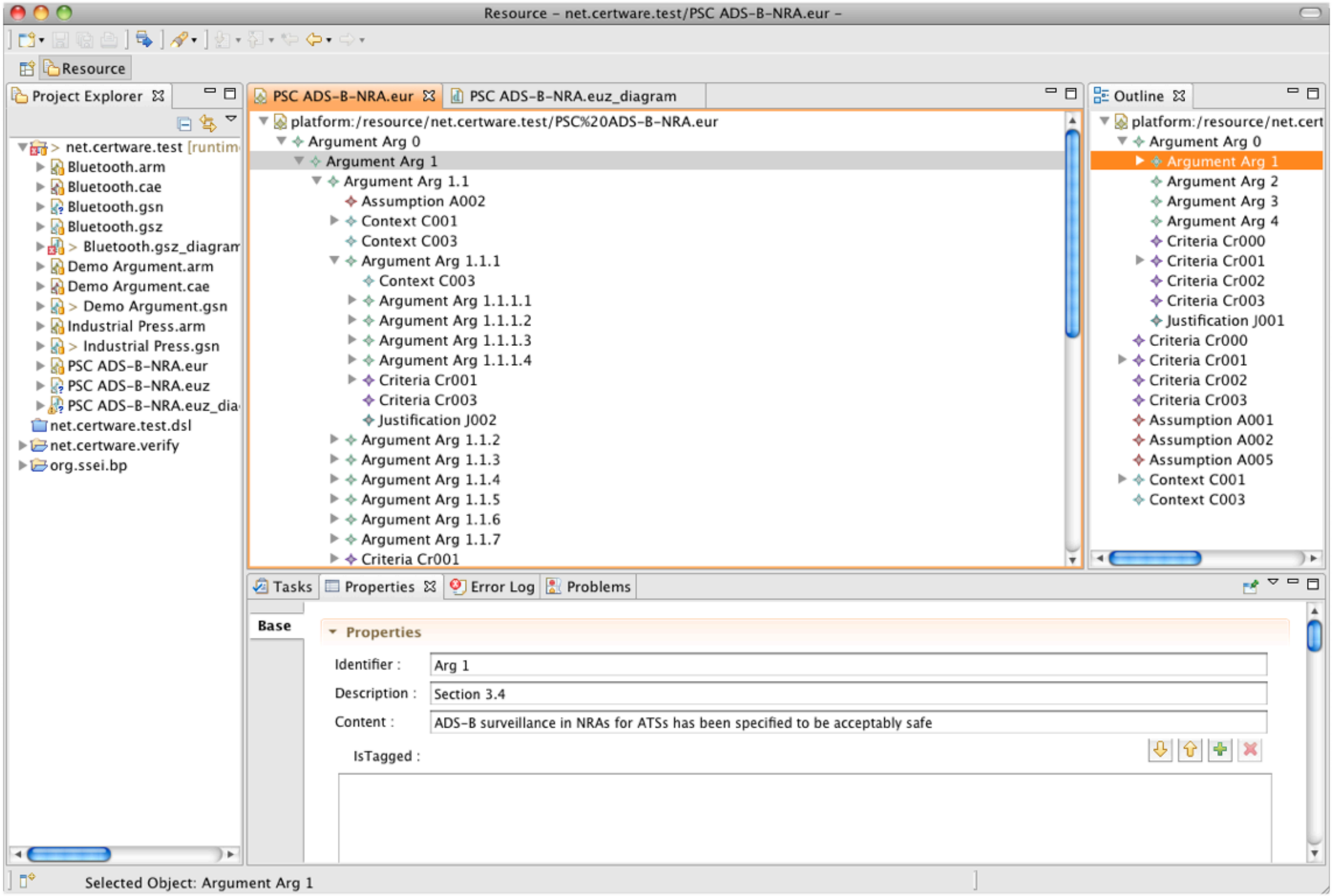
ARM: Argumentation Metamodel
ATL: Atlas Transformation Language
CPN: CertWare Planning Notation
DSL: Domain-Specific Language
GSN: Goal Structuring Notation
M2M: Model-to-Model
SMM: Software Metrics Metamodel
SPM: Software Project Management
XML: Extensible Markup Language



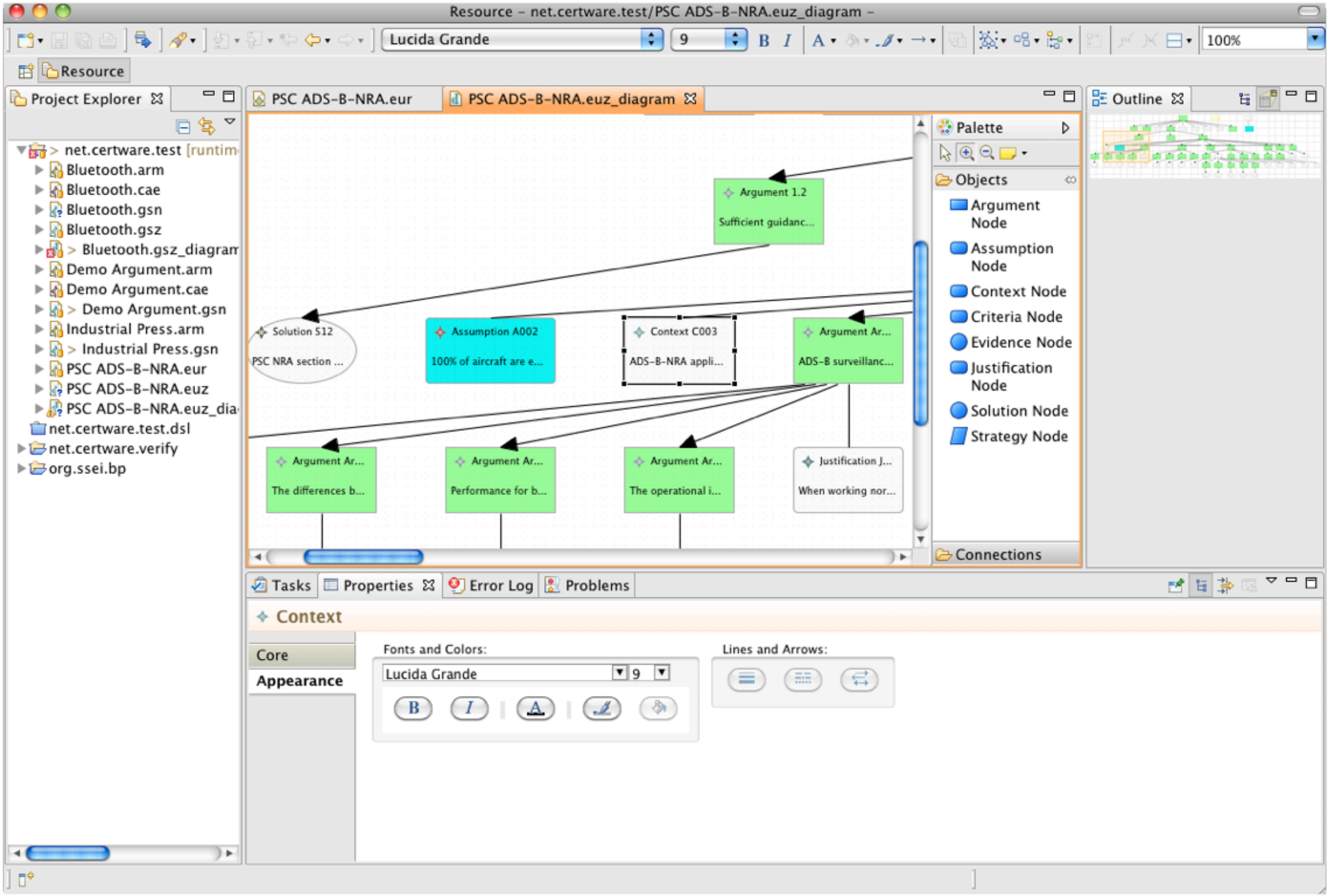


ASP: Answer Set Programming
CPT: Conditional Probability Table Model
DAG: Directed Acyclic Graph Model
DSL: Domain-Specific Language
M2M: Model-to-Model Transformation
NET: Hugin NET File API
P-Log: ASP with Probabilities

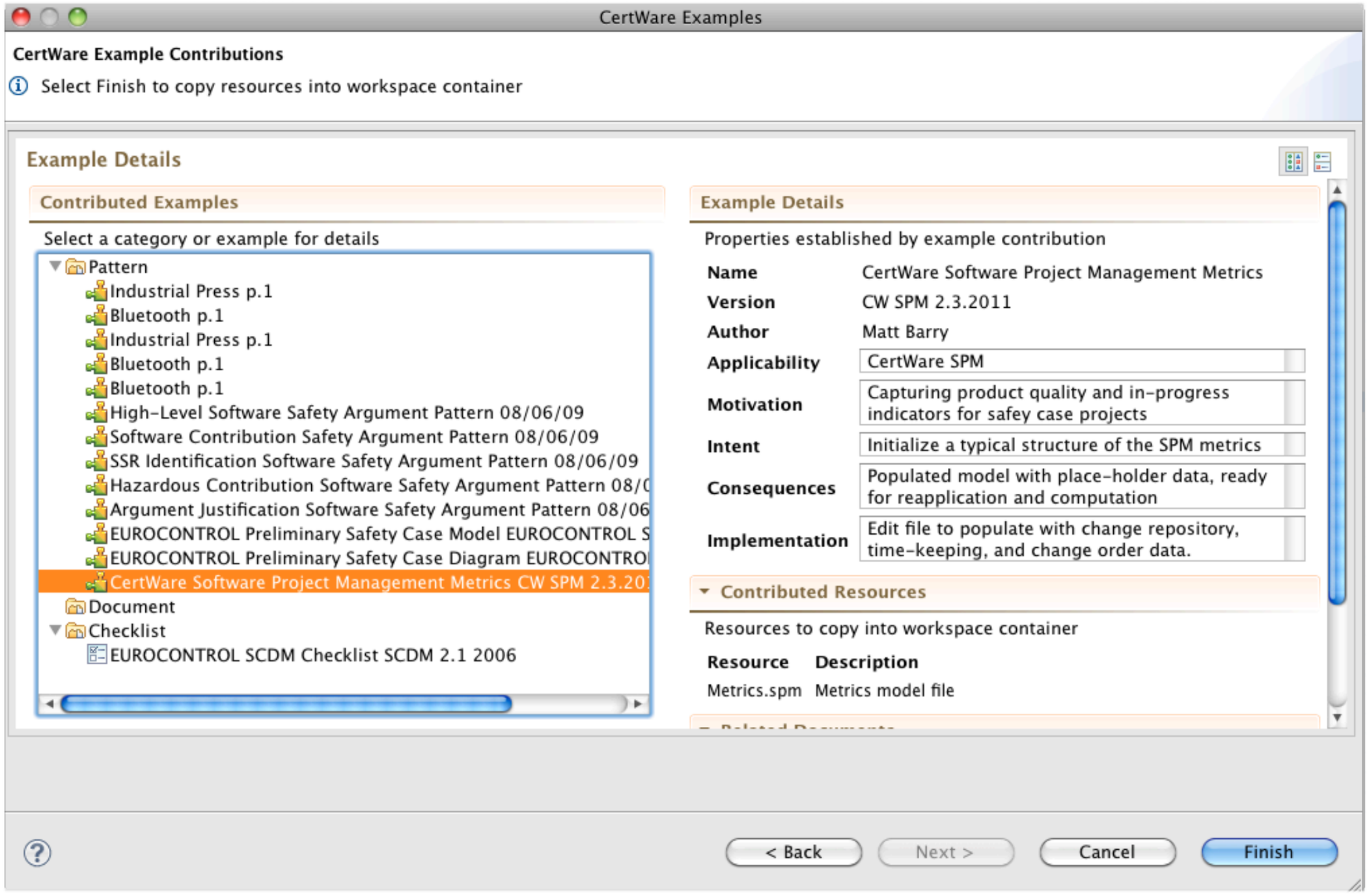




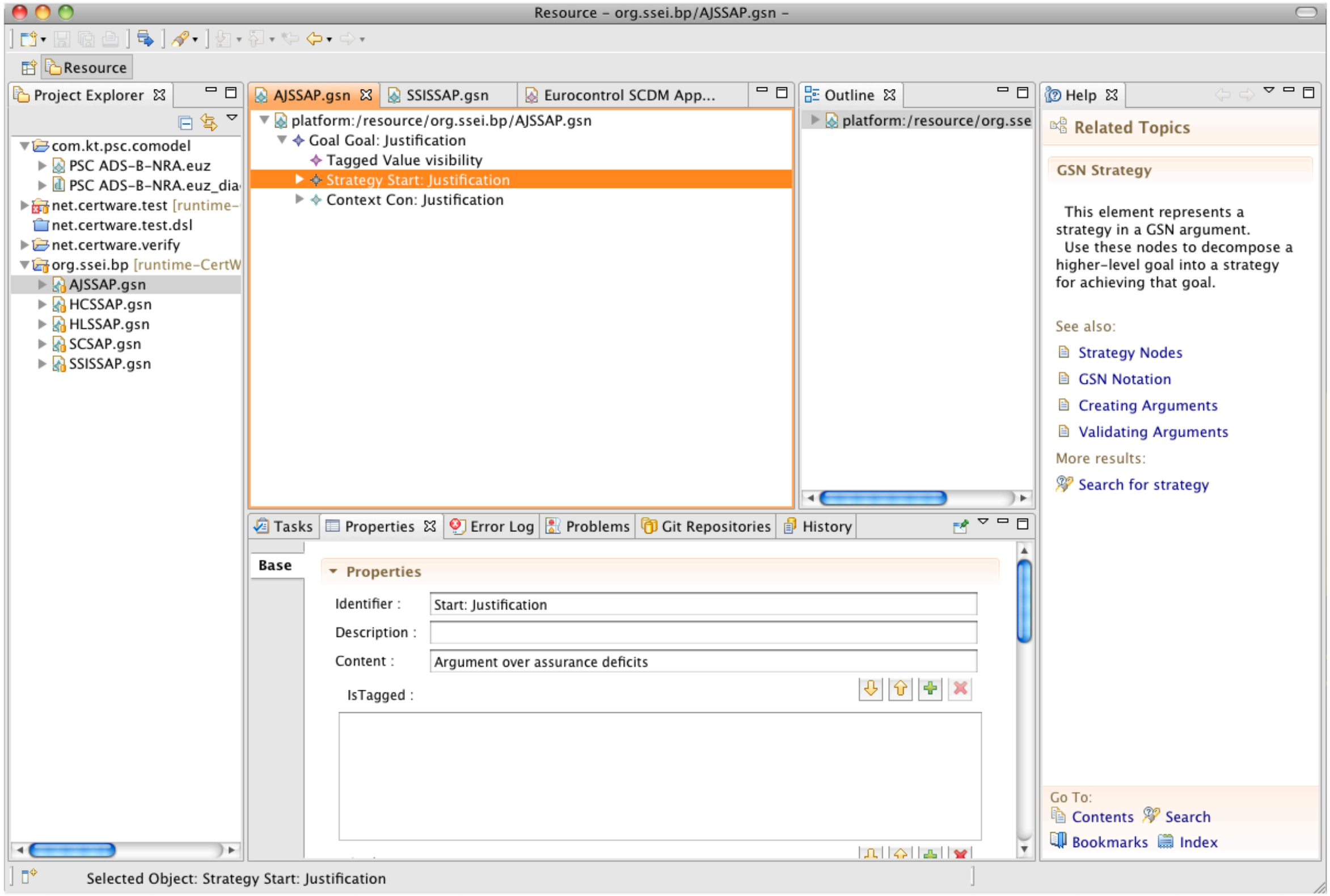
Tree-based argument editors: outlines, diagnostics, etc.



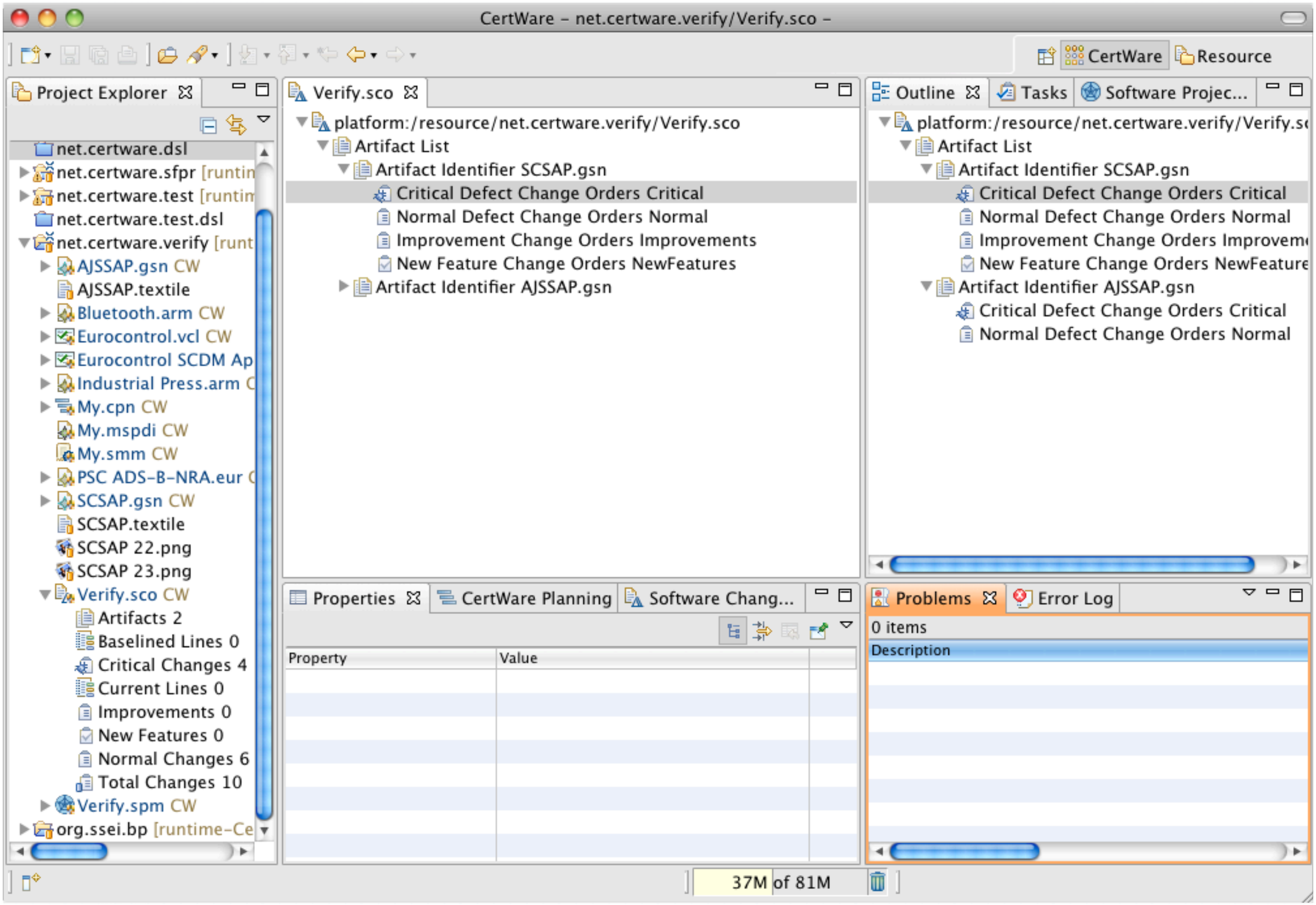
Graphical argument editors: outlines, diagnostics, etc.



Examples wizard installs copies of useful patterns



Dynamic, Context-Sensitive Help Built-In



Change order model collects statistics for PM metrics

CertWare – net.certware.verify/Verify.spm –

CertWare | Resource

Project Explorer

- net.certware.test [runtime-CertWar
- net.certware.test.dsl
- net.certware.verify [runtime-CertW
  - AJSSAP.gsn CW
  - AJSSAP.textile
  - Bluetooth.arm CW
  - Eurocontrol.vcl CW
  - Eurocontrol SCDM AppC.vcl CW
  - Industrial Press.arm CW
  - My.cpn 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.sco CW
  - Verify.spm CW
    - 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
- org.ssei.bp [runtime-CertWare_Edi

Verify.sco | Verify.spm

- Critical And Normal Change Order Count Total Count
- End Product Quality End Product Quality
  - Project Commit
  - Adaptability Ratio Measure Adaptability Ratio
  - Rework Ratio Measure Rework Ratio
  - Scrap Ratio Measure Scrap Ratio
  - Modularity Measure Modularity Ratio
  - Maturity Ratio Measure Maturity Ratio
  - Maintainability Measure Maintainability Ratio
- In Progress Indicator In-Progress Indicator
  - Project Commit
  - Rework Stability Measure Rework Stability
  - Rework Backlog Measure Rework Backlog
  - Modularity Trend Modularity Trend
  - Adaptability Trend Adaptability Trend
  - Maturity Trend Maturity Trend
- Case Scope CertWare SPM
- Project Scope CertWare SPM
- Change Scope CertWare SPM

Outline | Tasks

- platform:/resource/net.certware.ver
  - Project Model
    - Project Commit
      - Project Model
      - Total Case Size Measure Tot
      - Baseline Case Size Measure
      - Critical Defect Change Orde
      - Normal Defect Change Orde
      - Improvement Change Order
      - New Feature Change Order
      - Total Change Order Count T
      - Broken Case Size Measure B
      - Fixed Case Size Measure Fix
      - Repair Effort Measure Repai
      - Usage Time Measure Usage
      - Annotation Commit ID
      - Development Effort Measure
      - Critical And Normal Change
      - End Product Quality End Pro

Properties | Software... | CertWar... | Software...

tware Project Management Metrics

Commits

roject comm

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

Problems | Error Log

0 items

Description

Selected Object: platform:/resource/net.certware.verify/Verify.spm

43M of 81M

PM metrics captures statistics, trends, and results

Tasks | Properties | Software Project Management Metrics

Software Project Management Metrics

Project Commits

Project commit (N/A)

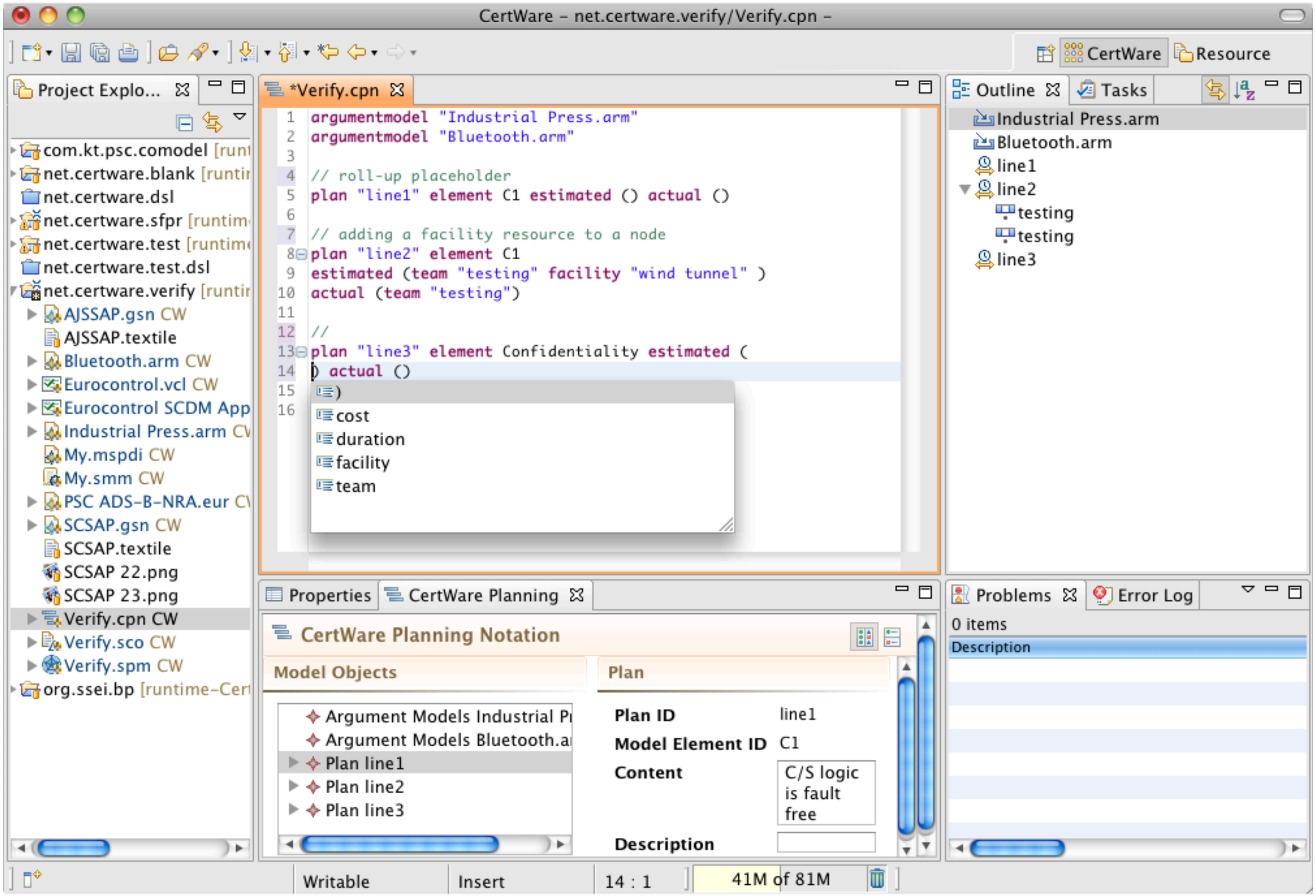
Commit Metrics

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

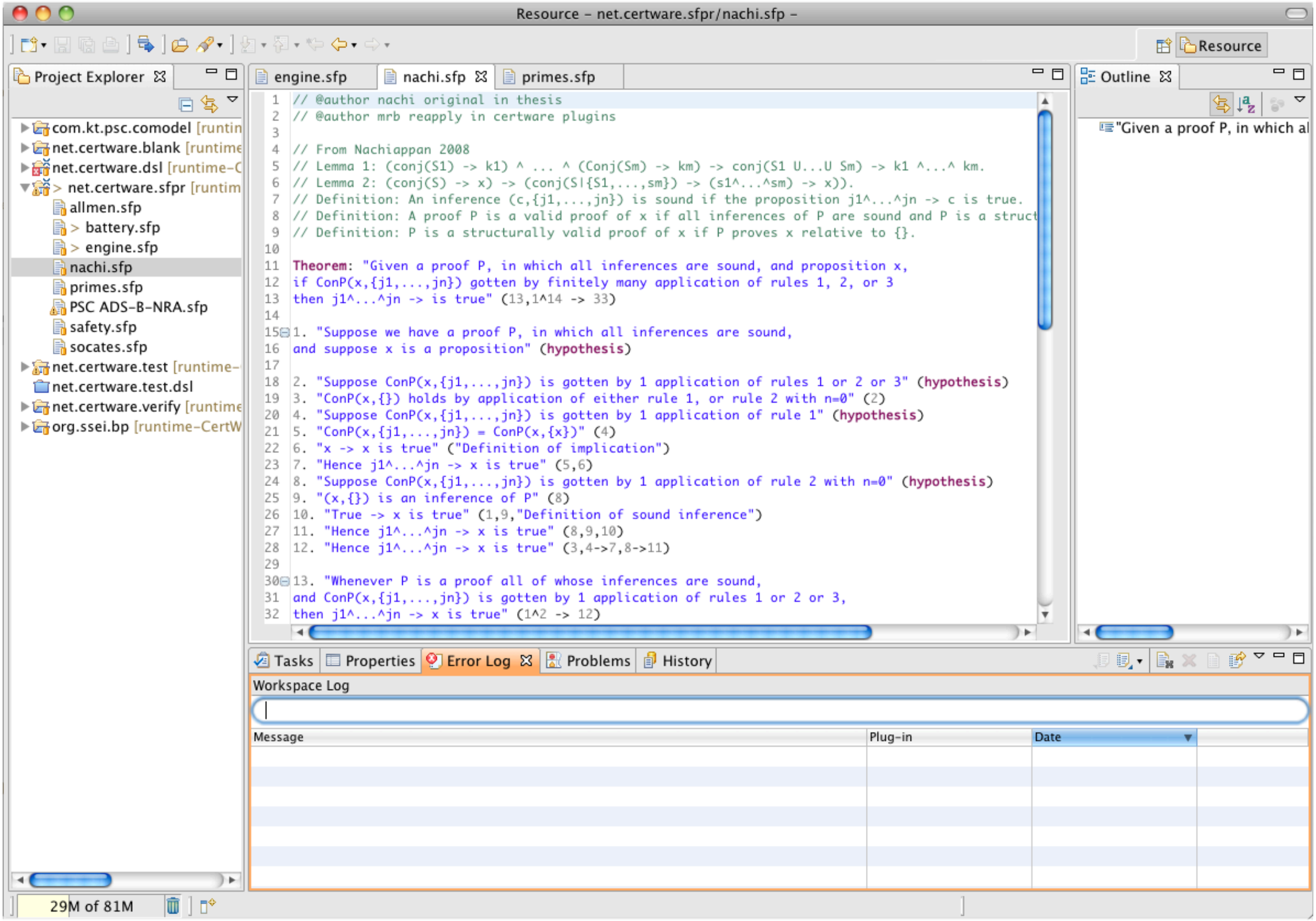
Raw Statistics

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



Custom DSL integrates argument items with PM data



Semi-Formal Proof DSL Provides Another Argument Style

CertWare Semi-Formal Proof Review

CertWare Semi-Formal Proof Review

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 ConP(x,{j1,...,jn}) is gotten by 1 application of rules 1 or 2 or 3" (hypothesis
  - 3. "ConP(x,{}) holds by application of either rule 1, or rule 2 with n=0"
  - 4. "Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 1" (hypothesis)
  - 5. "ConP(x,{j1,...,jn}) = ConP(x,{x})"
  - 6. "x -> x is true"
  - 7. "Hence j1^...^jn -> x is true"
  - 8. "Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 2 with n=0" (hypothesis)
  - 9. "(x,{}) is an inference of P"
  - 10. "True -> x is true"
  - 11. "Hence j1^...^jn -> x is true"
  - 12. "Hence j1^...^jn -> 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 s
  - 15. "Suppose ConP(x,{j1,...,jn}) is gotten by N+1 application of rules 1 or 2 or 3" (hypot
  - 16. "Suppose ConP(x',{j1,...,jn}) is gotten by N+1 application of rules 1 or 2 or 3" (hypot
  - 17. "ConP(x',{j1,...,jn}) = ConP(x',{x'})"
  - 18. "x' -> x' is true"
  - 19. "Hence j1^...^jn -> x' is true"
  - 20. "Suppose ConP(x',{j1,...,jn}) is gotten by N+1 applications,
  - 21. "(X1,{j1,...,jm}) is a sound inference of P, and ConP(Ji,Si)
  - 22. "j1^...^jm -> x'"
  - 23. "(conj(S1) -> j1) ^ ... ^ (conj(Sm) -> jm) is true"
  - 24. "conj(S1 U...U Sm) -> j1 ^...^ jm"
  - 25. "conj(S1 U...U Sm) -> x' is true"
  - 26. "Hence j1 ^ ... ^ jm -> x' is true"
  - 27. "Suppose ConP(x',{j1,...,jn}) is gotten by N+1 applications,
  - 28. "There exists {s1,...,sn}, S and proposition x, where x' is
  - 29. "conj(S) -> x is true"
  - 30. "conj(S|{s1,...,sn}) -> (s1^...^sn -> x) is true"
  - 31. "Hence j1^...^jn -> x' is true"
  - 32. "Hence j1^...^jn -> x1 is true"
  - 33. "Whenever ConP(x,{j1,...,jn}) 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
☑	ConP(x,{}) holds by application of either rule 1, or rule 2 with n=0	

Inference

Inference given the above premises:

Valid	Statement	Comment
✗	Hence j1^...^jn -> x is true	

Entailments

Deduction entailments:

Valid	Statement	Comment
☑	Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 1	hypothesis
⇨	Implies	
☑	Hence j1^...^jn -> x is true	

Valid	Statement	Comment
☑	Suppose ConP(x,{j1,...,jn}) is gotten by 1 application of rule 2 with n=0	hypothesis
⇨	Implies	
☑	Hence j1^...^jn -> x is true	

Deduction

Deduction given the above entailments:

Valid	Statement	Comment
✗	Hence j1^...^jn -> x is true	

Validation

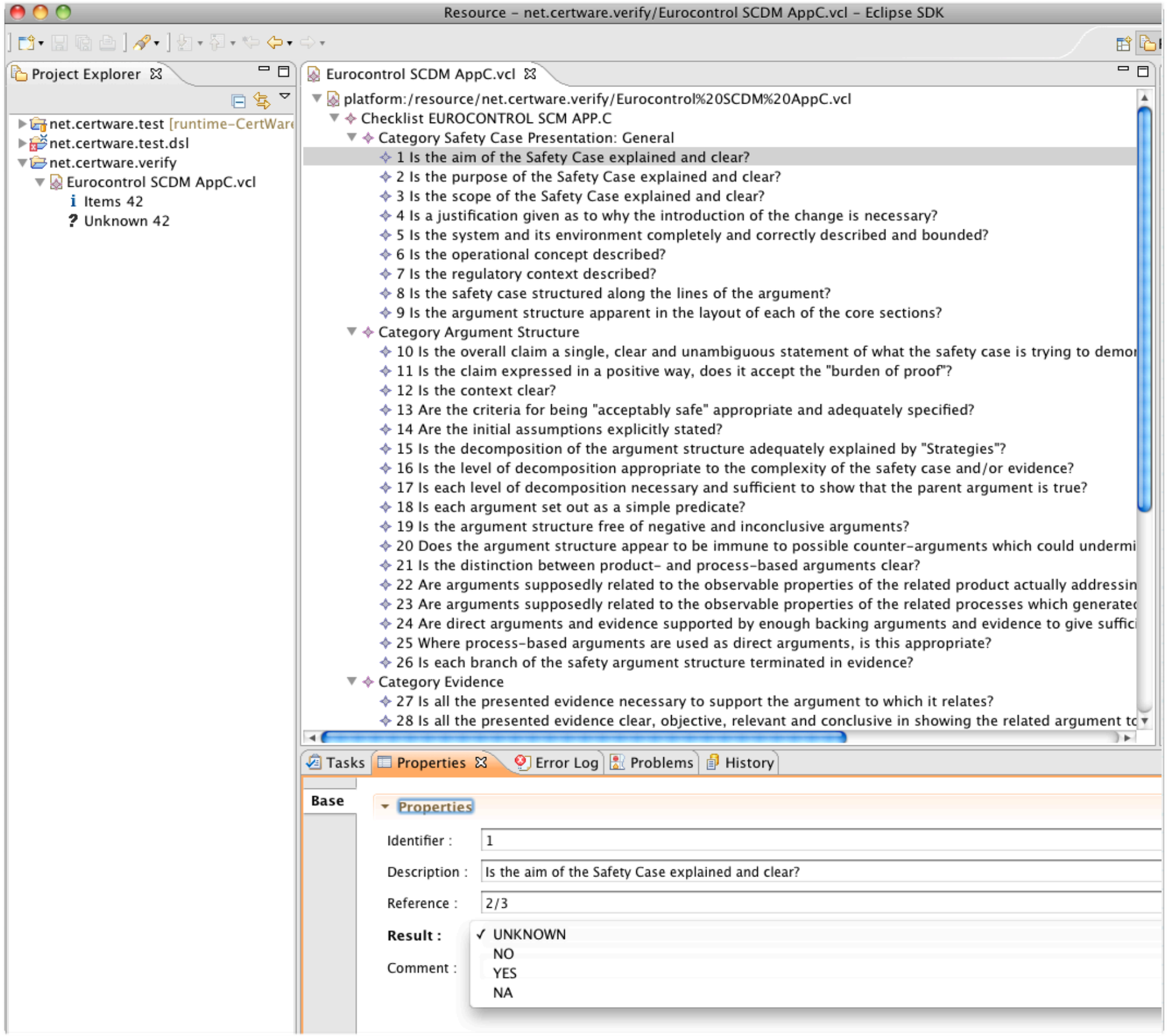
Validate the statement:

Valid | Invalid | Unknown

Previous Author mrb Time Stamp Tue Dec 28 18:50:56 CST 2010

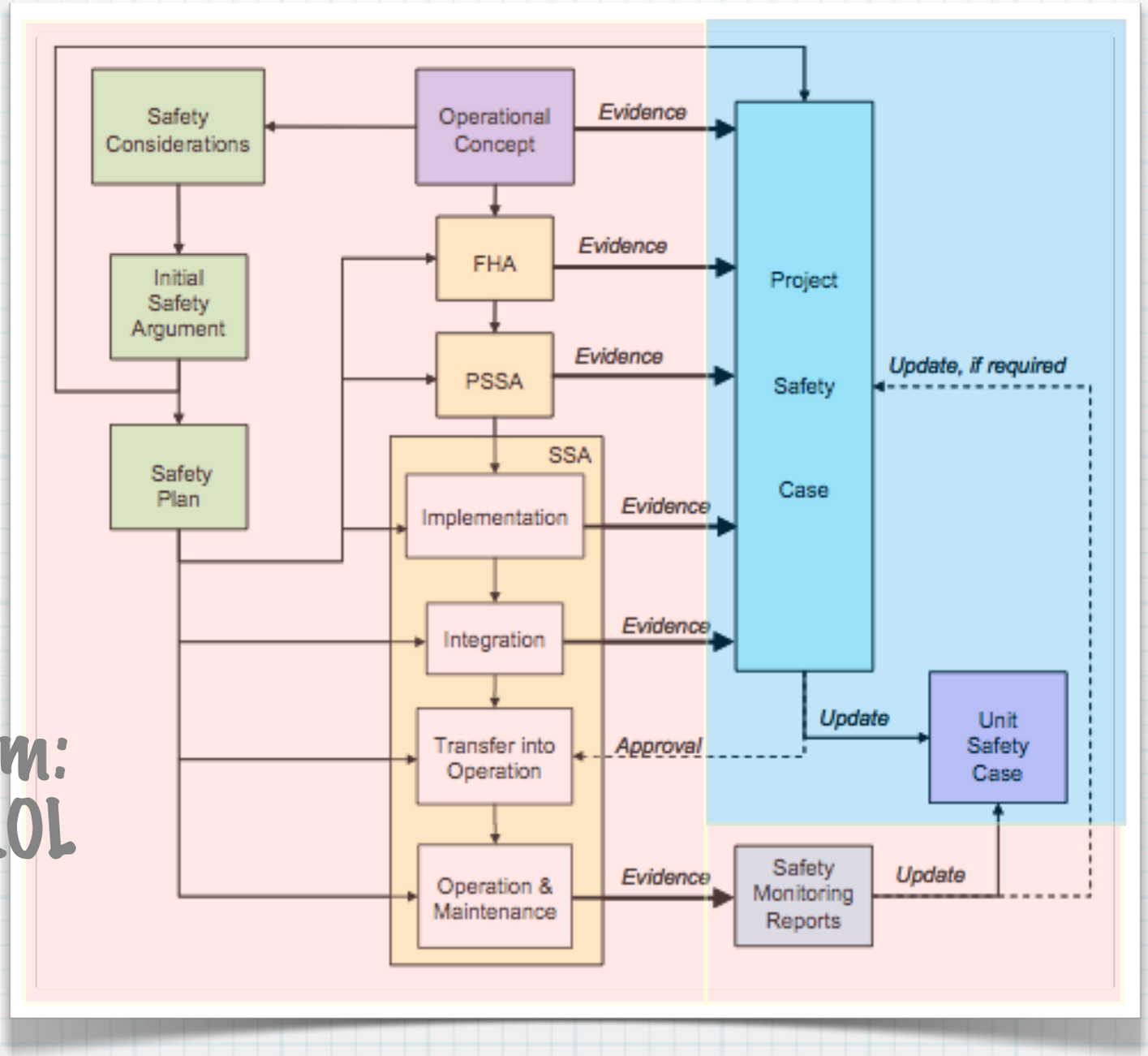
Help | < Back | Next > | Cancel | Finish

Semi-Formal Proof Review Wizard Facilitates V&V



Verification Checklist Models Support Case Review

Life-Cycle Integration



Current Focus

Future Focus

Example from: EUROCONTROL SCDM

Example life-cycle requiring tooling integration

Credits

NASA Contract #NNL10AA08C
NASA Langley Research Center
Kestrel Technology LLC