

CCAIE Summary and Demonstration

Rance J. DeLong
John Rushby

HAMES Review
October 7, 2008



© 2008 SRI International

Agenda for CCAIE presentation

- Progress and Status Overview
- MILS, the Common Criteria, and the CCAIE
- CCAIE Concept of Operation Review
- CCAIE Architecture Review
- CCAIE Principles of Operation Overview
- CCAIE Prototype Demonstration Overview
- CCAIE Demonstration



© 2008 SRI International

CCAIE Progress and Status Overview . . .



© 2008 SRI International

Progress

- CCAE Documentation
 - Part 1 - Introduction and Concept of Operation
 - Part 2 - Architecture
 - Part 3 - Principles of Operation
- CCAE Implementation
 - Experimental and prototype new code
 - Stable older code (shortcomings fixed as they appear)
- AFRL Layered Assurance Workshop (2nd LAW) presentation
 - *High-Assurance Development and Evaluation: Rethinking the Common Criteria and EAL7*
- Digital Avionics Systems Conference (27th DASC) paper
 - *The MILS Component Integration Approach to Secure Information Sharing*
- International Common Criteria Conference (9th ICC) participation
 - Continuing our effort to influence future CC directions (like steering an oil tanker)



© 2008 SRI International

CCAE documentation overview

- Part 1 - Introduction and Concept of Operation
 - Chapter 1 - Executive Summary
 - Chapter 2 - Introduction
 - Chapter 3 - Concept of Operation
- Part 2 - Architecture
 - Chapter 4 - Architecture
- Part 3 - Principles of Operation
 - Chapter 5 - Functional Description
 - Chapter 6 - Theory of Operation
- Appendices
 - A - Glossary
 - B - Fuzzy Unification
 - C - Workflow Management Language
 - D - Definite Clause Translation Grammar Examples
 - E - Document Generator Sketch
 - F - Repository Documents
 - G - Importing the XML Version of the Common Criteria
 - H - Publishing with LaTeX
 - I - Functional Allocation
 - J - Prototype Demo
 - K - Development Plan

CURRENT



© 2008 SRI International

CCAE documentation overview

- Upcoming documentation tasks for coming year
 - Continue to keep Parts 1 - 3 current and in sync with implementation
 - Appendices of current Parts 1 - 3 are a "down payment" on Part 4
 - Loose collection of low-level topics
 - Will be made complete and uniformly developed in Part 4
 - Functional Allocation (Appendix I) and Functional Description (Chapter 5) expanded to include all CONOP referenced capabilities
 - Development Plan (Appendix K) will provide detail on the planned development of all the CONOP referenced capabilities
- Updated Part 2 - Architecture
 - Chapter 4 - Architecture updated to reflect system as (being) built
- Part 4 - Development
 - Chapter 7 - Detailed Design
 - Appendix K - Development Plan (updated)
- Part 5 - Implementation
 - Chapter 8 - Implementation Commentary
 - Appendix X - Implementation Code (assuming other detail appendices may be added)

FUTURE



© 2008 SRI International

CCAIE Technology

- Advances
 - Generates a PP in format and style that can be adjusted independent of the content
 - Guarantee the accuracy of normative Common Criteria material such as SFR/SAR
 - Automatically check CC dependencies and hierarchy
- Expected Advancements in Coming Work
 - Objective (and quantitative) assessment of PP quality and completeness
 - Representing and applying “fuzzy” expert knowledge
- Technical Risks
 - *None* in the core functional areas
 - Applying expert knowledge
 - Only the *degree* (somewhere between successful and “jaw-dropping” successful) of achievement in applying ontology, reasoning, and expert knowledge
- “Effort” Risks
 - Effort needed to import new versions of CC
 - Effort to encode expert knowledge and ontology



© 2008 SRI International

Status Summary

- CCAIE Document
 - Parts 1 through 3 DRAFT, undergoing continuing refinement
 - Parts 4 and 5 to come: detailed design and implementation commentary
- Implementation goals for this timeframe substantially achieved
 - see Appendix I: Functional Allocation, pp. 171-174
 - All code for demo goals in, at least, experimental phase (see description in Appendix K: Development Plan, section K.2, pp. 182-184)
 - Skeleton is in place, now for the body building
- Project a “usable” CCAIE by end 2009
 - Text-based User Interface Agent
 - Limited “intelligence” but good “organizational skills” and “attention to detail”
 - May have to contend with move to CC 3.1



© 2008 SRI International

Status Summary

- Next Steps
 - Complete Appendix I: Functional Allocation
 - Include all envisioned functions described in Concept of Operation
 - Give a better idea of work to come
 - Functionality needed for expert user to produce all aspects of a PP
- Plans
 - See Appendix K: Development Plan
 - Broad “stable” implementation by end-09
 - Encompassing all mechanical aspects of authoring
 - Usable by others
 - Then begin graphical user interface agent,
 - and add the “intelligence”
 - Ontology
 - Knowledge encoding
 - Reasoning
 - Expert advice



© 2008 SRI International

Objectives for 2009

- Establish concrete objectives and set dates for 2009 reviews and deliveries
- Tentative Objectives
 - “Stable”-ize current experimental and prototype code (see Appendix K)
 - User agent activities and UI interactions to include core PP creation and revision “therbligs”
 - Complete internal representations to accommodate *all parts* of a real example (SKPP)
 - Implement the relational model of T,P,A -> Objectives -> SFRs/SARs
 - Assessment of PPs using CC-based objective criteria, e.g., dependencies, hierarchy, EAL conformance, mapping and rationale, and presence of all required parts
 - Workflow Management
 - Complete integration of workflow management
 - Author and Reviewer Agents
 - Whiteboard
 - Control shell
 - Whiteboard interface rules to knowledge sources
 - Solidify CCAE’s role in MIPP conformance enforcement
- Questions?



© 2008 SRI International

Resources

- CCAE Development Resources (current)
 - Principals (current and future)
 - Rance DeLong, 80+ hours per month currently and in 2009
 - John Rushby, variable as needed
 - Other resources (medium term)
 - GUI designer when ready to begin that phase
 - Consulting from SRI's AI Center
 - Apprentice to work on CC 3.1 adaptation and knowledge encoding
 - Outside resources (long term)
 - Reviewers and users
 - Contributing experts

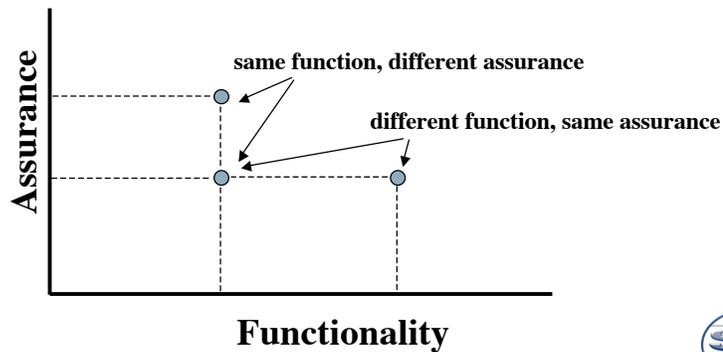


MILS, the Common Criteria, and the CCAE . . .



What CC protection profiles do: The CC provides us with

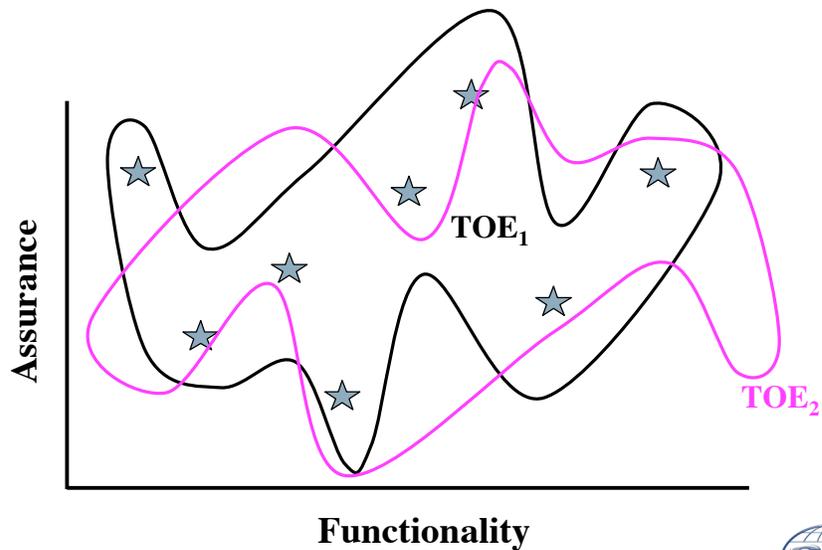
- A structure for the development of security requirements specifications
- Independent functional and assurance dimensions (like ITSEC, unlike TCSEC)



© 2008 SRI International

13

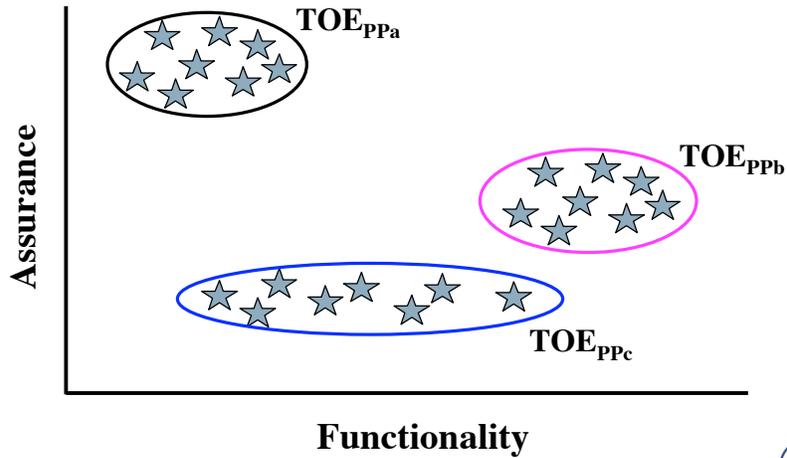
Unconstrained TOEs in Functionality \times Assurance



© 2008 SRI International

14

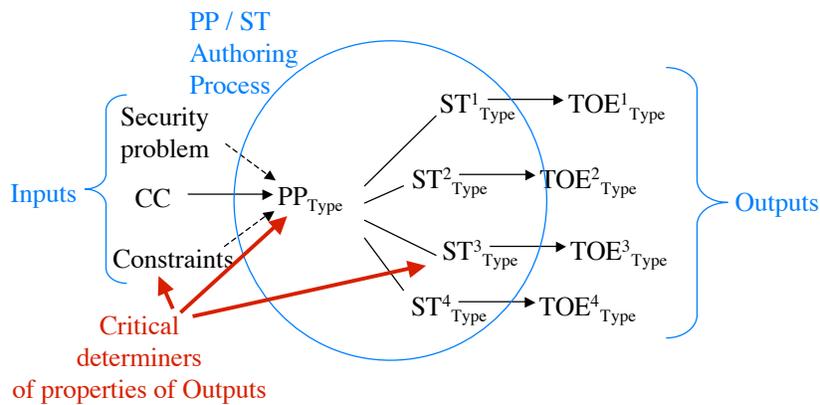
PPs Constrain TOEs in Functionality × Assurance



© 2008 SRI International

CC-based product (TOE) development

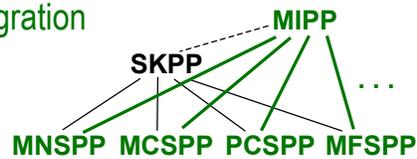
We expect multiple TOEs of each product type and have expectations of a relationship among instances of a type and with instances of other types



© 2008 SRI International

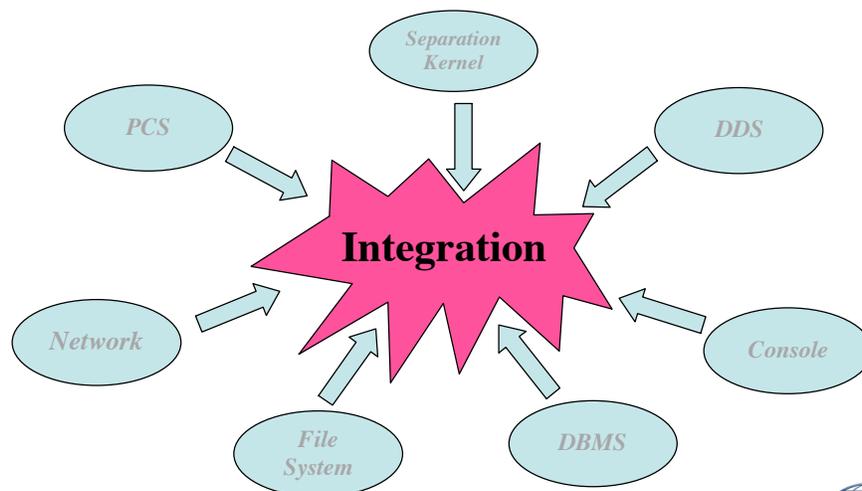
MILS is based on composition of cooperating products defined by related Protection Profiles

- Separation Kernel (SKPP)
- Partitioning Communication System (PCSP)
- MILS Console System (MCSP)
- MILS Network System (MNSP)
- MILS File System (MFSPP)
- ...
- MILS Integration Protection Profile (MIPP)
aka MILS Component Integration



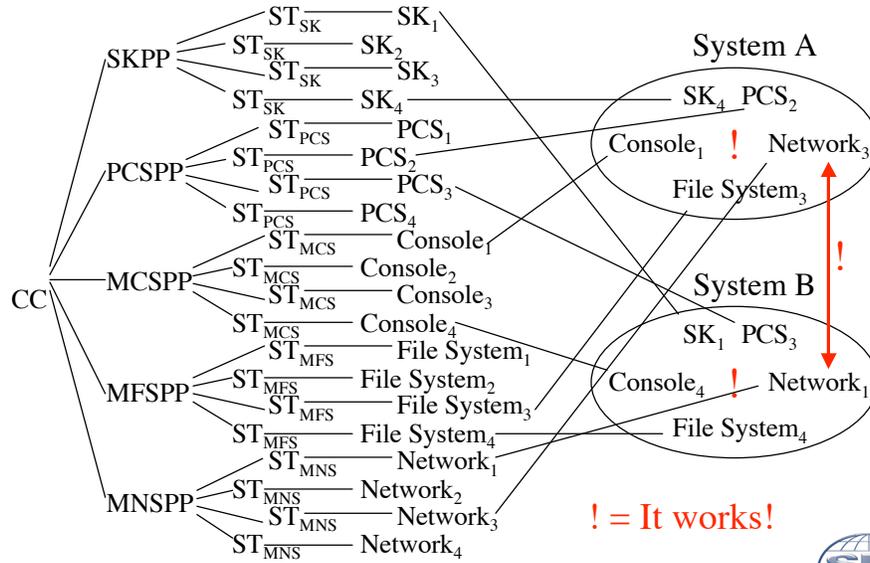
© 2008 SRI International

Need for MILS theory and an integration PP to coordinate component PPs and avoid integration blowup

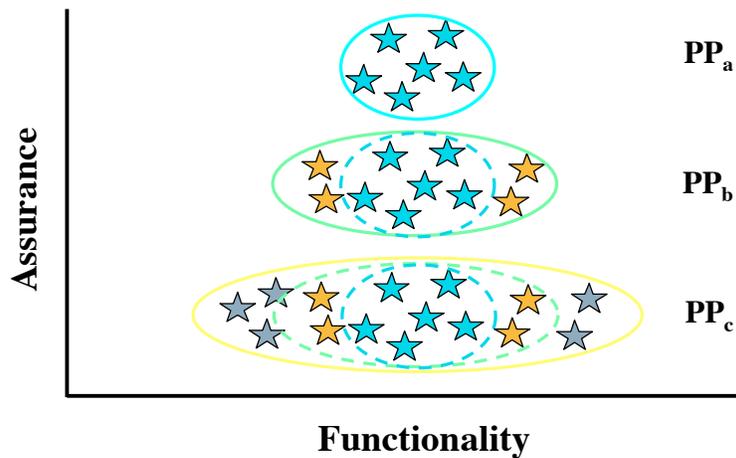


© 2008 SRI International

We Want MILS PPs to Achieve *This Goal!*

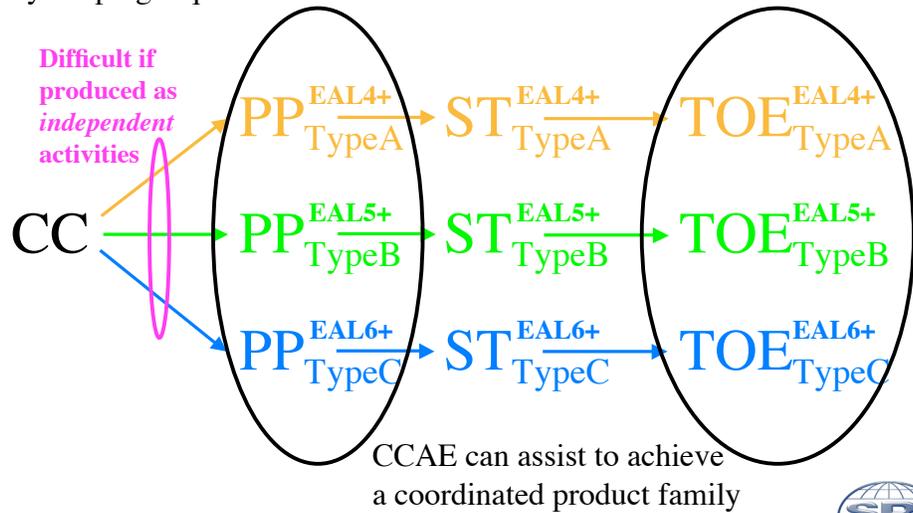


And, Have an Effective Approach to Product Families



Avoiding the potential problems with separate PPs for product family members

by keeping requirements well coordinated

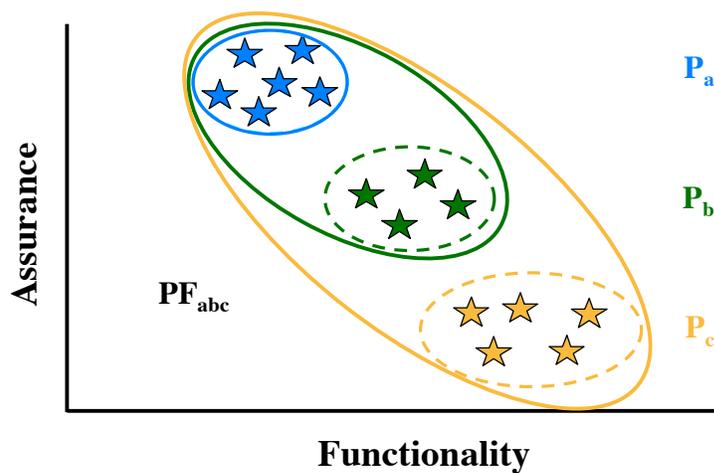


© 2008 SRI International



21

Define Configurations of a Product Family with Sub-Profiles and CCAE manages complexity



© 2008 SRI International



22

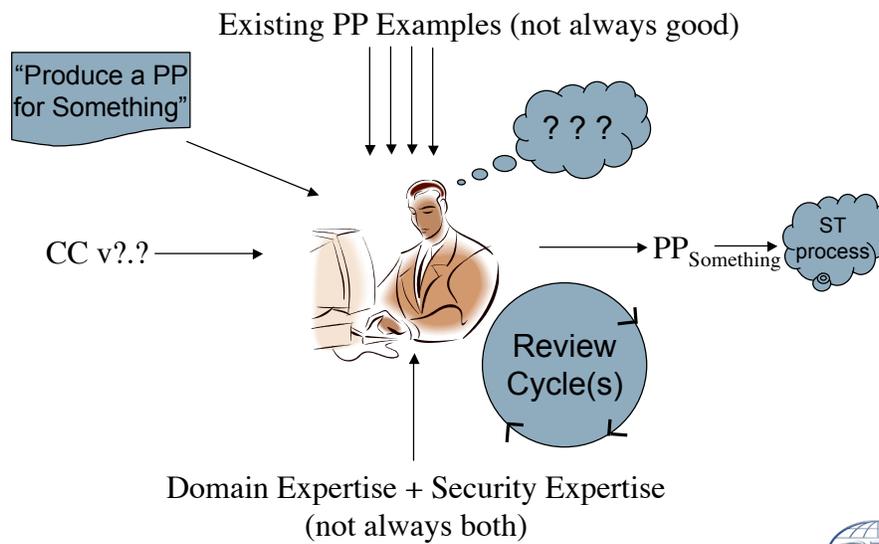
CCAIE Concept of Operation Review . . .



© 2008 SRI International

23

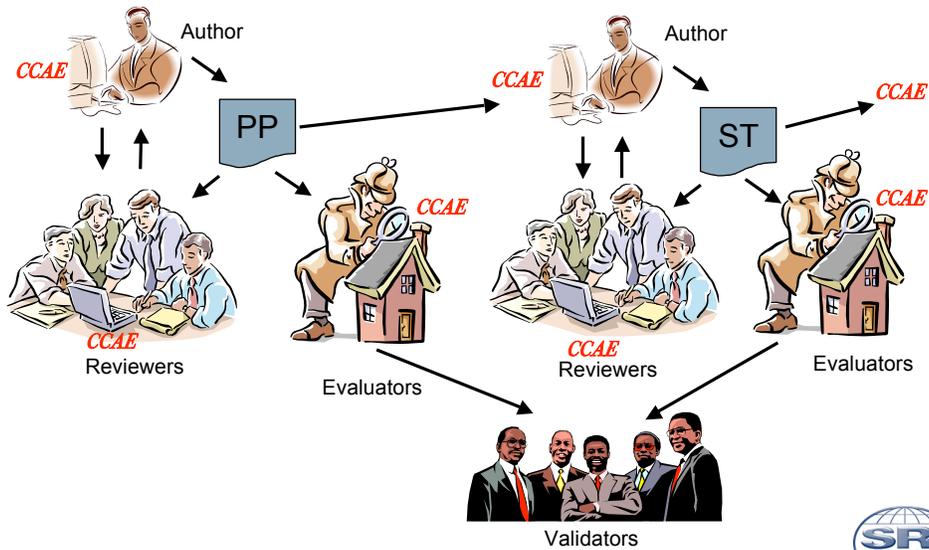
How MILS PPs Have Been Written



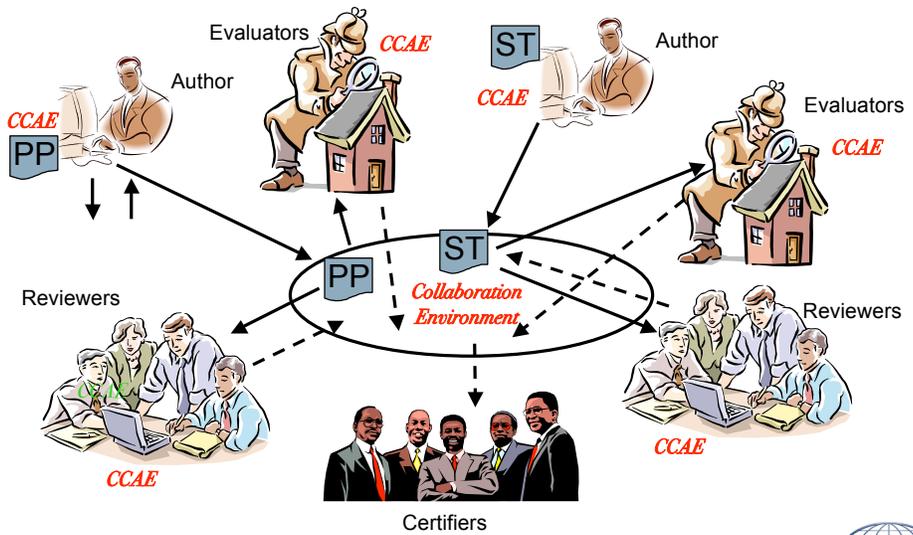
© 2008 SRI International

24

Applications of the CCAE



CCAe Collaborative Environment



CCAIE-supported author, reviewer, evaluator tasks

Choose security environ threats, policies, assumptions	Ontology provides a common framework
Derive security objectives	Ontology and expert knowledge guidance
Select SFR/SARs from CC catalog	Check correspondence to security objectives
Complete SFR/SAR component operations	Tracked in work flow
Define new component operations for ST	Tracked in work flow
Supply mappings and rationale	Tracked in work flow and relational model



© 2008 SRI International

27

CCAIE-supported author, reviewer, evaluator tasks

Fashion explicit SFR/SARs	Help avoid gratuitous departure from CC
Select EAL and guarantee it is met	Ensure minimums for EAL met despite explicit rqmts
Assess conformance to abstract PP model	Quantitative measurement against model and scoring
Assure proper use of CC conventions	Conventions applied to form, semantics, typography
Assure accuracy of CC text and versions	“Automated” version of CC built into CCAIE
Assure dependencies and consistency	Apply known dependencies in CC and knowledge base



© 2008 SRI International

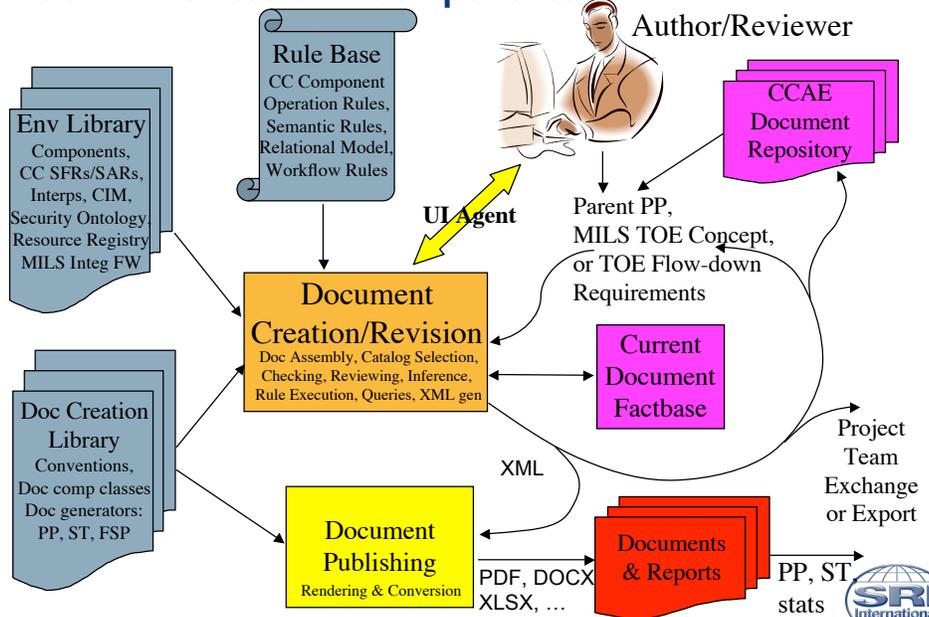
28

CCAE Architecture Review . . .



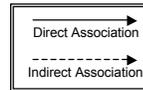
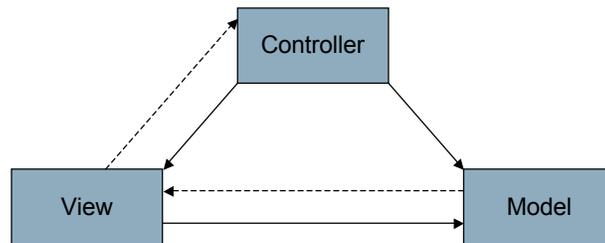
© 2008 SRI International

CCAE Architectural Components



© 2008 SRI International

Model-View-Controller Architectural Pattern



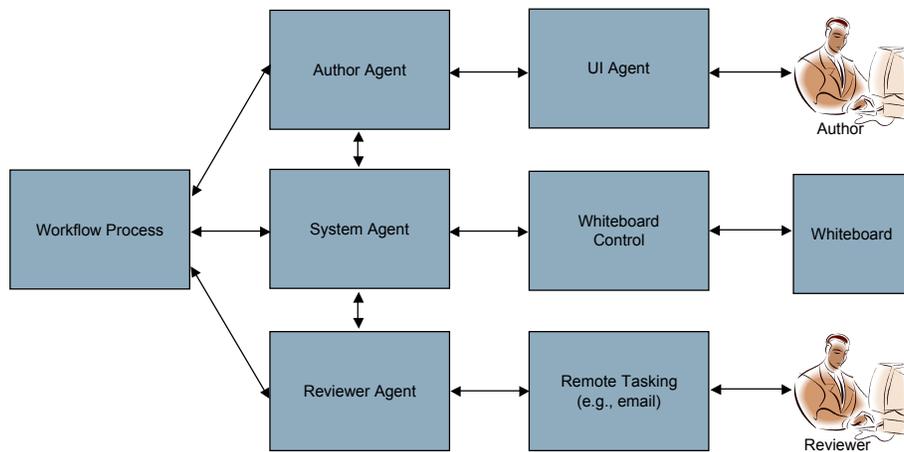
Adapted from Wikipedia

© 2008 SRI International



31

Workflow Process and Agents



© 2008 SRI International



32

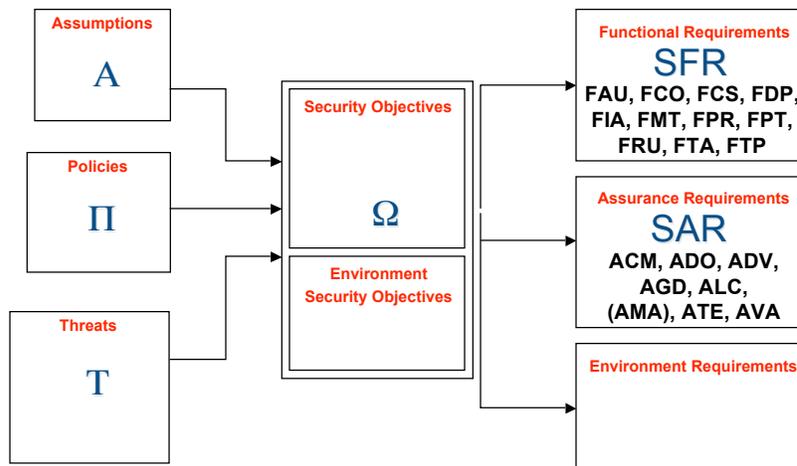
CCAE Principles of Operation Overview . . .



© 2008 SRI International

33

Relational Structure of a Protection Profile



$$PP = (2^T \times 2^\Pi \times 2^A \times \Omega \times 2^{SFR} \times 2^{SAR})$$



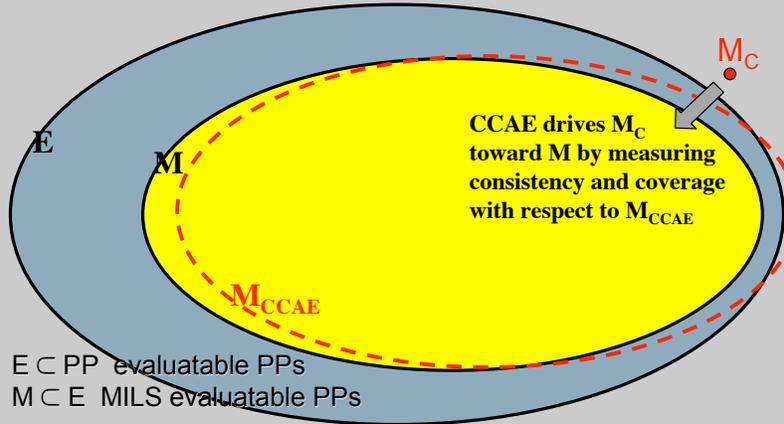
© 2008 SRI International

34

Approximation of a MILS PP Oracle

$$PP = (2^T \times 2^{\Pi} \times 2^A \times \Omega \times 2^{SFR} \times 2^{SAR})$$

M_C a candidate member of M

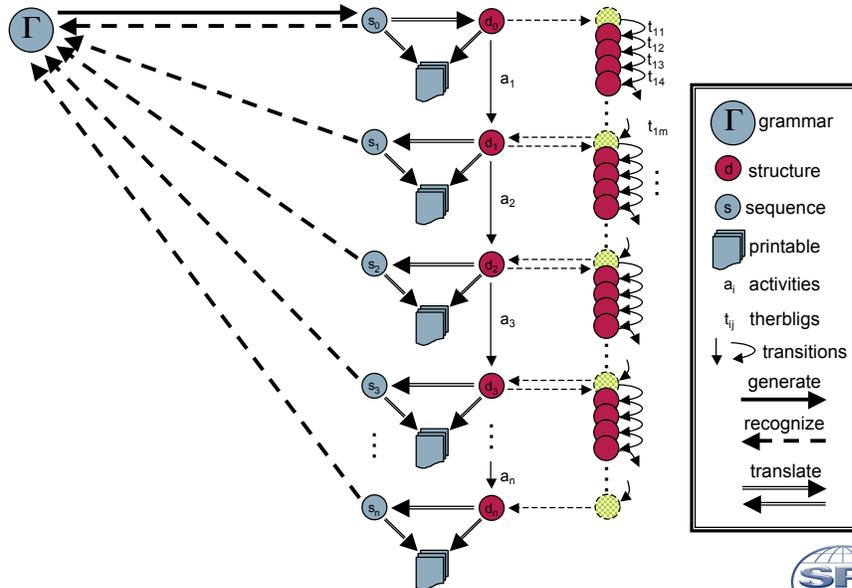


E C PP evaluable PPs
M C E MILS evaluable PPs



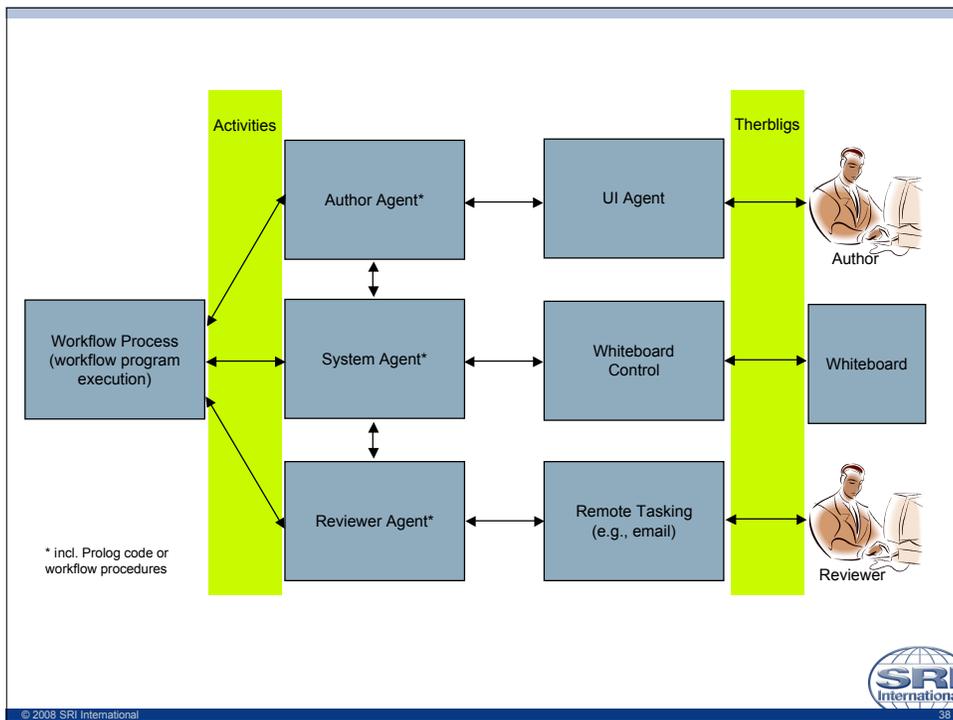
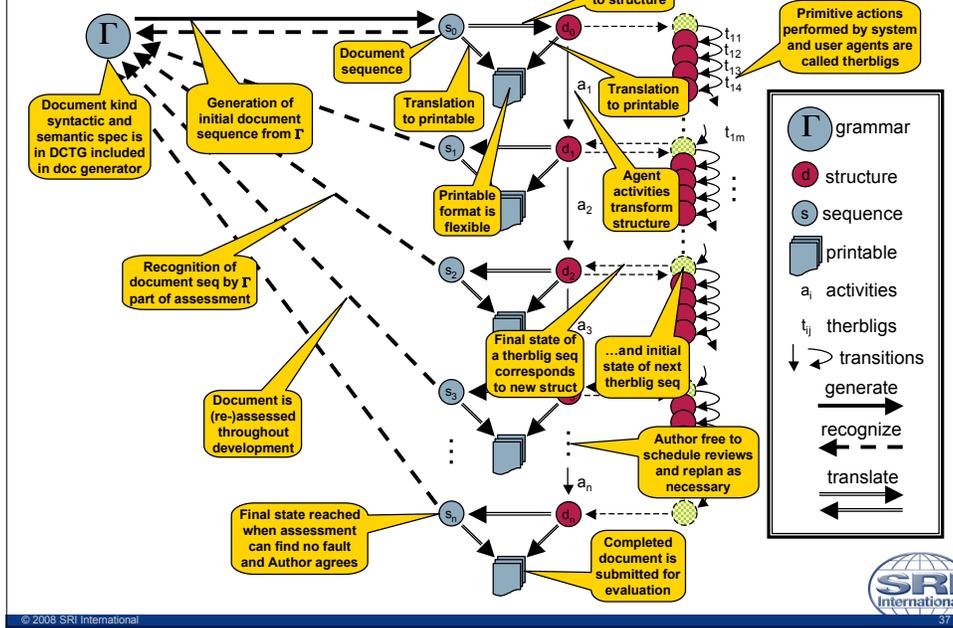
© 2008 SRI International

Document Development Strategy and Tactics

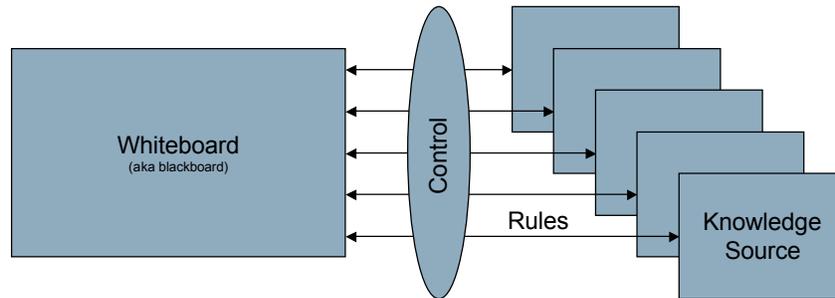


© 2008 SRI International

Document Development Strategy and Tactics



Whiteboard Architectural Pattern



© 2008 SRI International

39

Knowledge Source Production Rules for Whiteboard Interface

Condition \longrightarrow Action

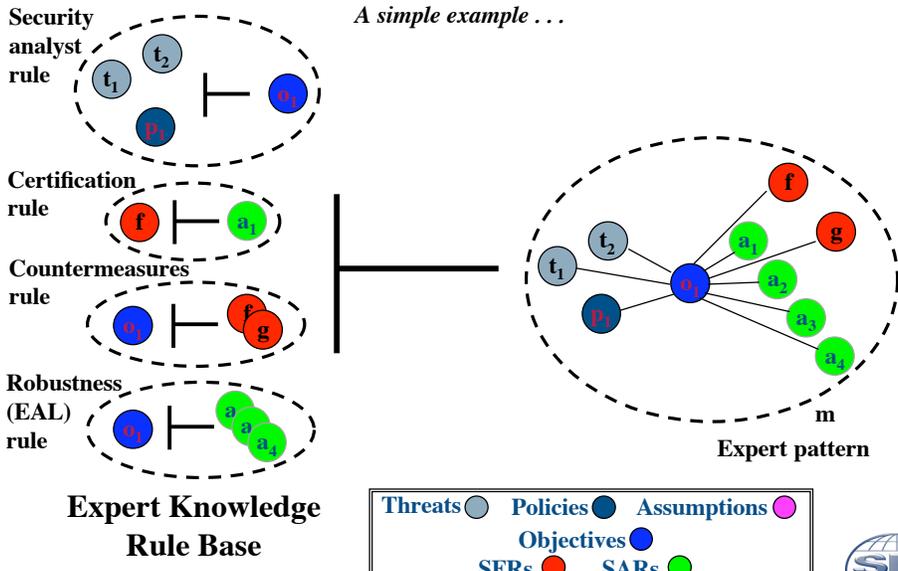
$[C_1, C_2, \dots, C_n] \longrightarrow [A_1, A_2, \dots, A_m]$



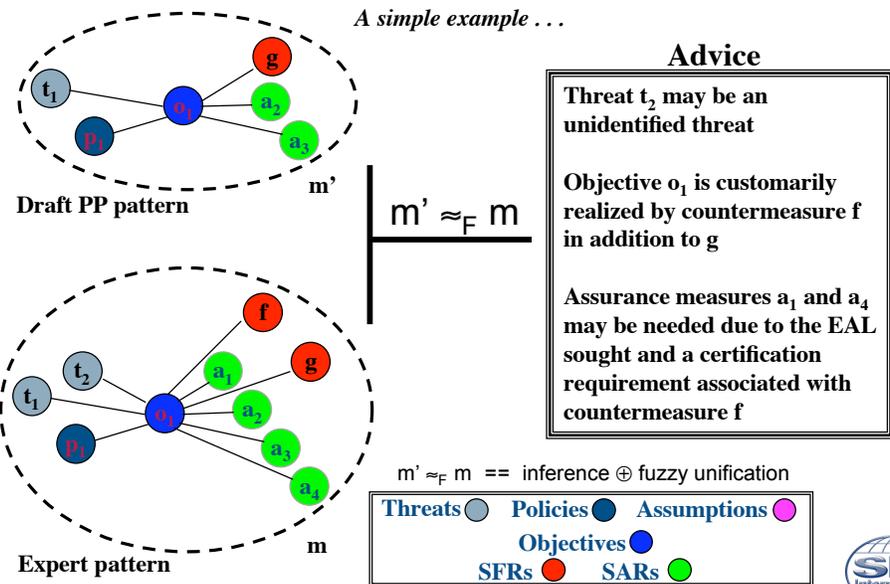
© 2008 SRI International

40

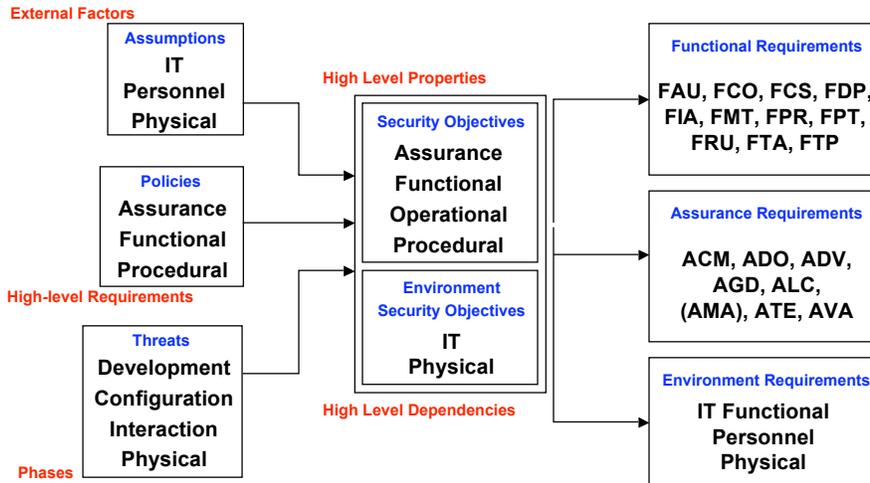
Constructing a Usage Pattern from Expert Knowledge



Expert Advice Generation



Relational structure of a protection profile superimposed with a security taxonomy



Taxonomy yields better conceptual coverage:
 External Factors x High-level Rqmts x Phases => Properties x Deps => Rqmts



© 2008 SRI International

43

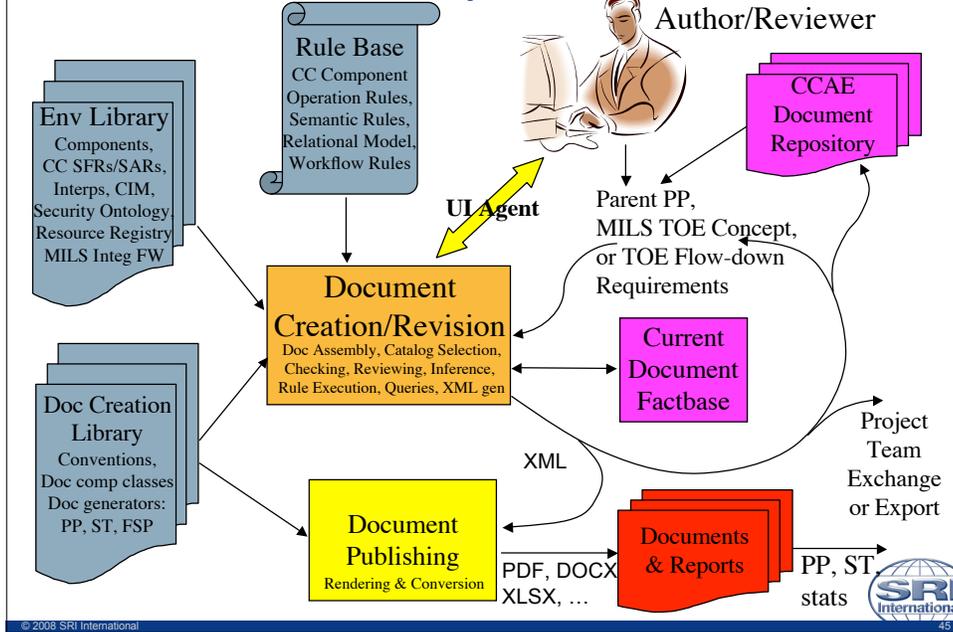
CCAE Prototype Demonstration Overview . . .



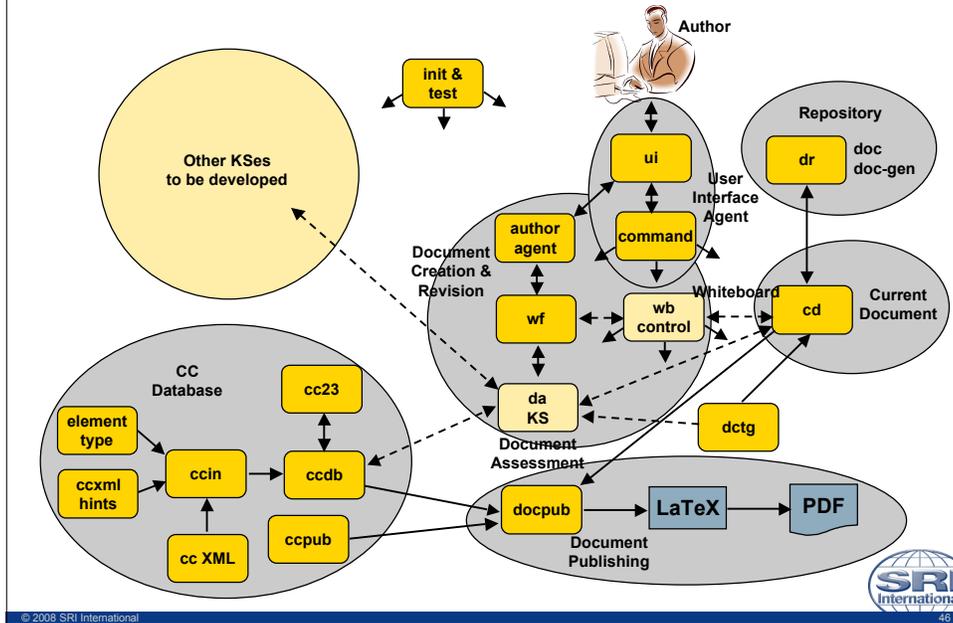
© 2008 SRI International

44

CCAIE Architectural Components



Current CCAIE Modules and Environment



CCAE Prototype Demonstration

- What you will see
 - Demo of mostly low-level functionality through recently developed command interface
- The Demo script
 - Initialize a project to develop a new PP using a simple document generator “spp”
 - Show the initial state and publish skeletal document using LaTeX
 - Add some SFRs and SARs
 - Publish modified document using LaTeX
 - Show repository document representation of SKPP
 - Load the SKPP and publish



Simplified Document Generator for a PP

```
document_generator([
doc_kind(simplified_pp),
doc_gen_ver('1'),
doc_grammar([
  spp :=
    pp_frontmatter,
    pp_chapters,
  (pp_frontmatter :=
  pp_title_page
  <->
  title_info('Simplified Protection Profile','0.00','Author','Date') ,
  (pp_title_page :=
  [doc_title(spp,'Simplified Protection Profile'),
  doc_version('0.00'),
  doc_date(today),
  doc_author('Author'),
  doc_kind(simplified_pp),
  doc_cc_version(cc23)],
  (pp_chapters :=
  pp_intro,
  pp_toe_desc,
  pp_sec_env,
  pp_sec_obj,
  pp_sfrs,
  pp_sars,
  pp_rationale),
  (pp_intro :=
  [chapter(introduction),
  author_supplied(paragraph),
  section(identification),
  section(overview),
  section(mutual_recognition),
  section(conventions),
  section(glossary),
  section(organization)]),
  (pp_toe_desc :=
  [chapter(toe_description),
  section(product_type),
  section(toe_functionality),
  section(toe_environment)],
  (pp_sec_env :=
  [chapter(sec_environment),
  section(threats),
  section(policies),
  section(assumptions)],
  (pp_sec_obj :=
  [chapter(sec_objectives),
  section(toe_security_objectives),
  section(env_security_objectives)],
  (pp_sfrs :=
  [chapter(toe_sfrs),
  author_supplied(sfr_selection),
  author_supplied(sfr_end_notes)],
  (pp_sars :=
  [chapter(toe_sars),
  author_supplied(sar_selection),
  author_supplied(sar_end_notes)],
  (pp_rationale :=
  [chapter(rationale),
  author_supplied(obj_from_threats),
  author_supplied(obj_from_policies),
  author_supplied(obj_from_assump),
  author_supplied(reqs_from_obs),
  author_supplied(env_reqs_from_obs)]
  ]),
  doc_workflow([
  SEE NEXT SLIDE
  ]),
  doc_resources([ conforms_to([common_criteria('2.3')) ] )
  ]),
  ])
```



Workflow Program in 'spp' Document Generator

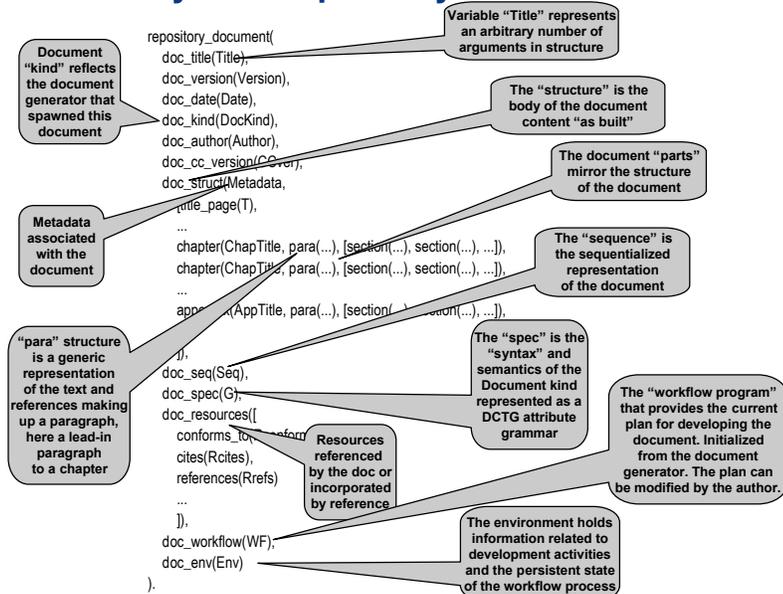
```

doc_workflow([
  activity(author, 'Review and set preferences', []),
  activity(author, 'Review and modify workflow plan', []),
  activity(author, 'Schedule reviews', []),
  activity(author, 'Security environment analysis', []),
  activity(author, 'Provide explanation for security environment', []),
  activity(author, 'Derive security objectives from security environment analysis', []),
  activity(author, 'Select SFRs from CC catalog', []),
  activity(author, 'Select SARs from CC catalog', []),
  activity(author, 'Complete or defer CC component operations in chosen SFRs/SARs', []),
  activity(author, 'Specify (new) component operations to be performed in the ST', []),
  activity(author, 'Map security objectives to SFRs/SARs, and provide rationale', []),
  activity(author, 'Define refinements to SFRs/SARs to better address objectives', []),
  activity(author, 'Define explicit SFRs/SARs as necessary to address objectives', []),
  activity(author, 'Ensure that explicit SFRs/SARs have objective evaluation basis', []),
  activity(author, 'Provide rationale that SARs are adequate to support explicit SFRs', []),
  activity(author, 'Assess leveling and balance of SFRs/SARs', []),
  activity(author, 'Select appropriate evaluation assurance level package', []),
  activity(author, 'Identify augmentations to EAL package to address objectives', []),
  activity(author, 'Assess all aspects of draft PP from an evaluation perspective', []),
  activity(author, 'Confirm that chosen SARs are compatible with EAL claim', []),
  activity(author, 'Provide rationale for security objectives wrt security environment', []),
  activity(author, 'Provide rationale for each SFR/SAR wrt security objectives', []),
  activity(author, 'Provide rationale for completion of component operations in the PP', []),
  activity(author, 'Provide justification for component operation not completed in PP', []),
  activity(author, 'Provide justification for each explicit requirement wrt objectives', []),
  activity(author, 'Assure proper use of CC conventions', []),
  activity(author, 'Assure all CC-originated dependencies are satisfied', []),
  activity(author, 'Compose TOE description to explain product type and features', []),
  activity(author, 'Confirm PP is complete, coherent, and internally consistent', []),
  activity(author, 'Measure quality of conformance by PP', []),
  repeat([
    concurrent([
      activity(reviewers, 'External review', []),
      activity(author, 'Incorporate changes due to review comments', []),
    ]),
    activity(author, 'Assess document', []),
    activity(author, 'Review and modify workflow plan', [NewTasks]),
    perform(NewTasks),
    activity(author, 'Assess document', [A])
  ], author_and_CCAE_rest(A)),
  activity(author, 'Submit PP for evaluation', []),
]);

```



Anatomy of a Repository Document

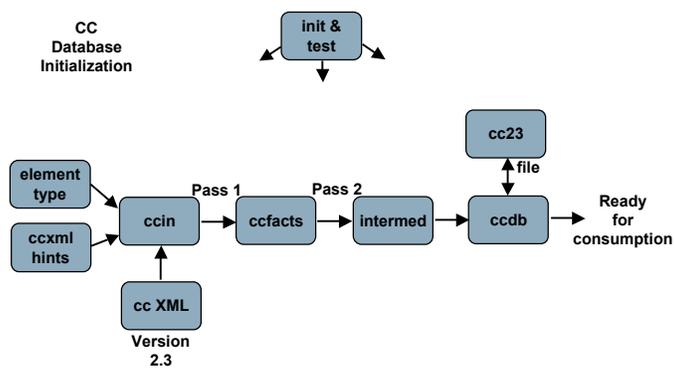


SKPP Repository Document

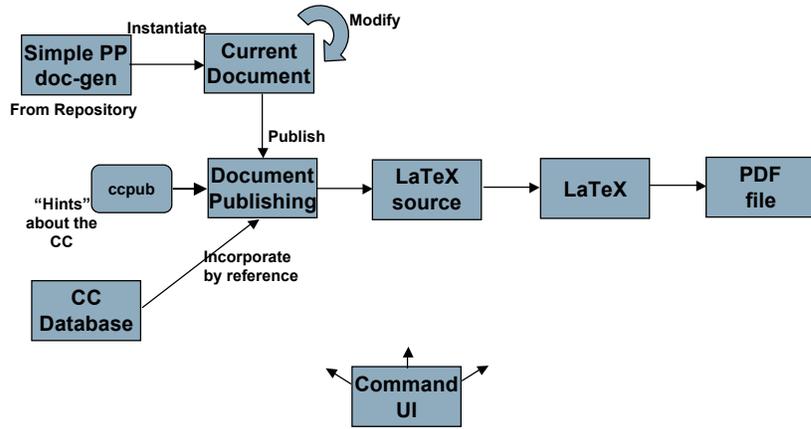
- Shown in demo



Artifact Flow in the Demo



Artifact Flow in the Demo

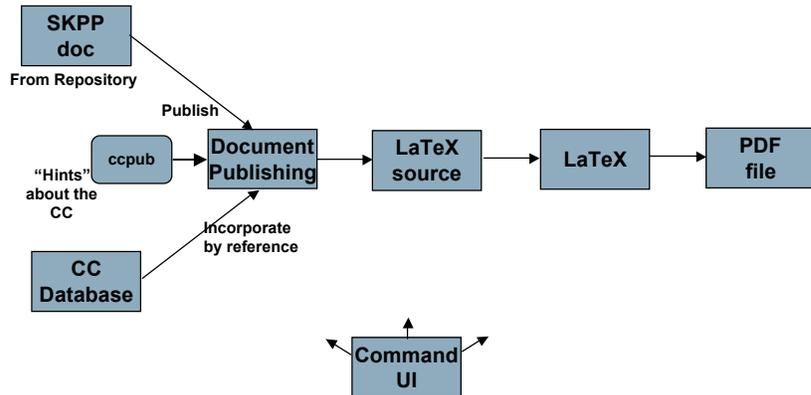


© 2008 SRI International



53

Artifact Flow in the Demo



© 2008 SRI International



54