A Common Criteria Authoring Environment Supporting Composition*

Rance DeLong[a], John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA USA

8th International
Common Criteria Conference
Rome, Italy
September 25, 2007

* Sponsored by AFRL via Raytheon
[a] LynuxWorks and Santa Clara University

Relationship of the CCAE to the MIPP

We describe two complementary activities:

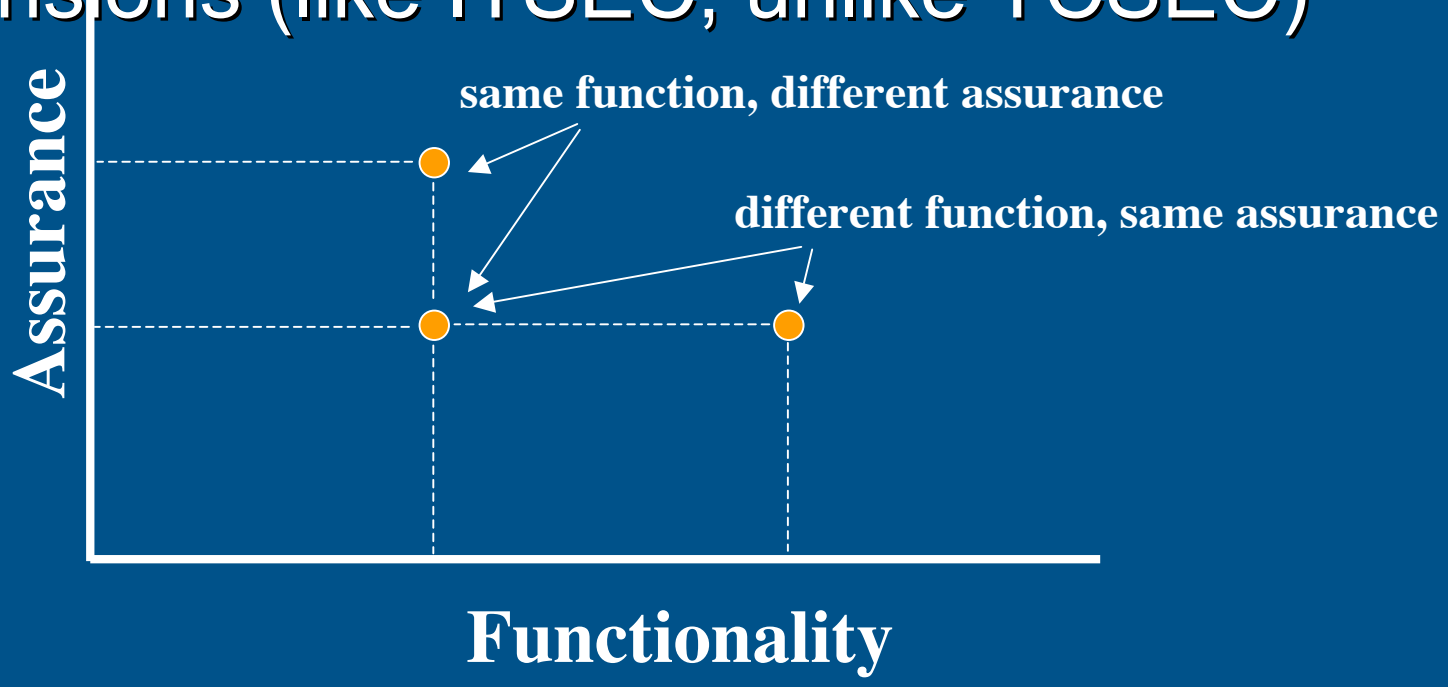
- a MILS Integration Protection Profile, and
- A Common Criteria Authoring Environment (CCAE) to support authors of MILS PPs and STs

Together these can provide strategic coordination to the MILS community.

The CCAE will enable authors to produce reviewed PPs and STs of higher quality in less time, and ones that will better serve the common interests of the MILS community

What CC protection profiles do: The CC provides us with

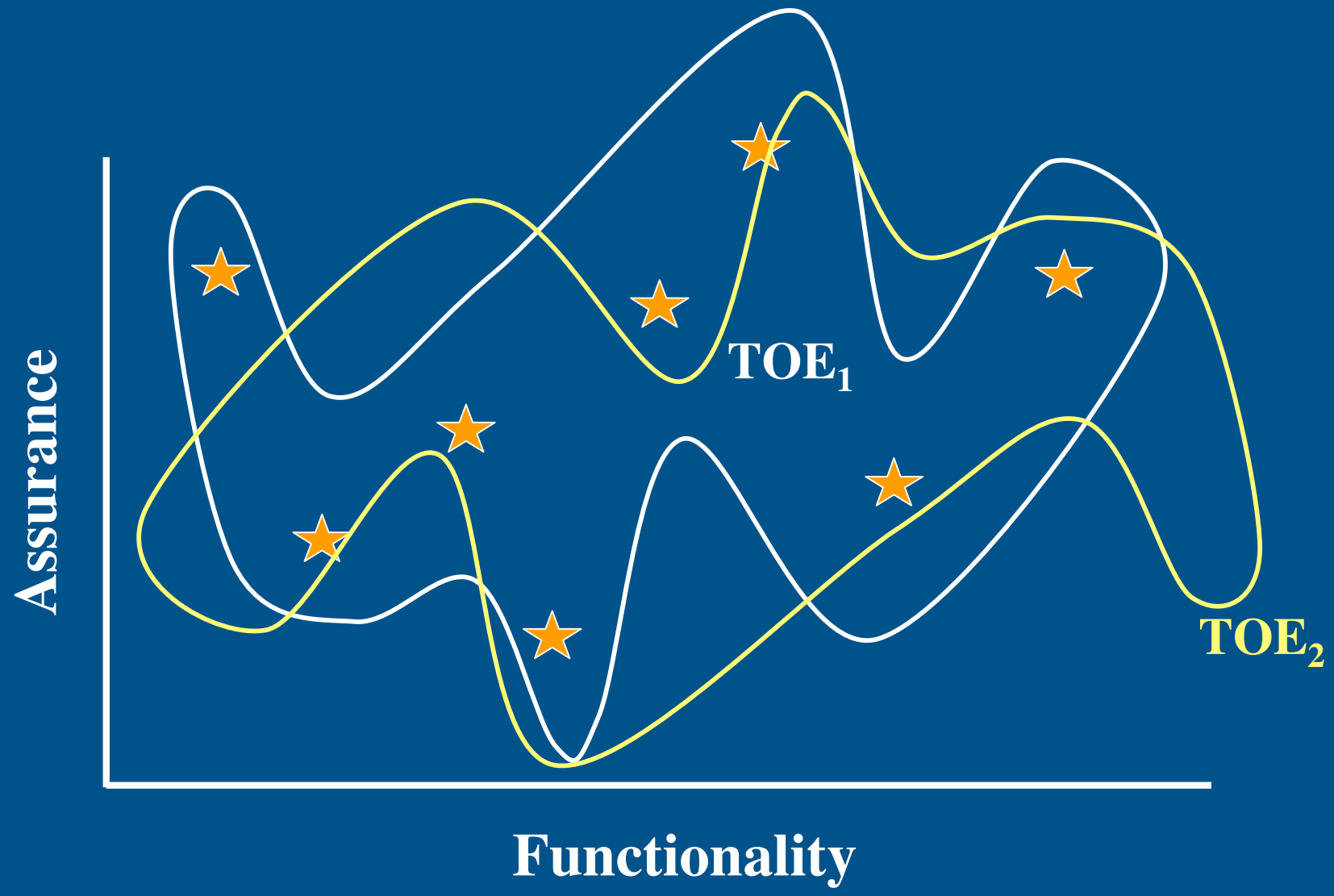
- A structure for the development of security requirements specifications
- Independent functional and assurance dimensions (like ITSEC, unlike TCSEC)



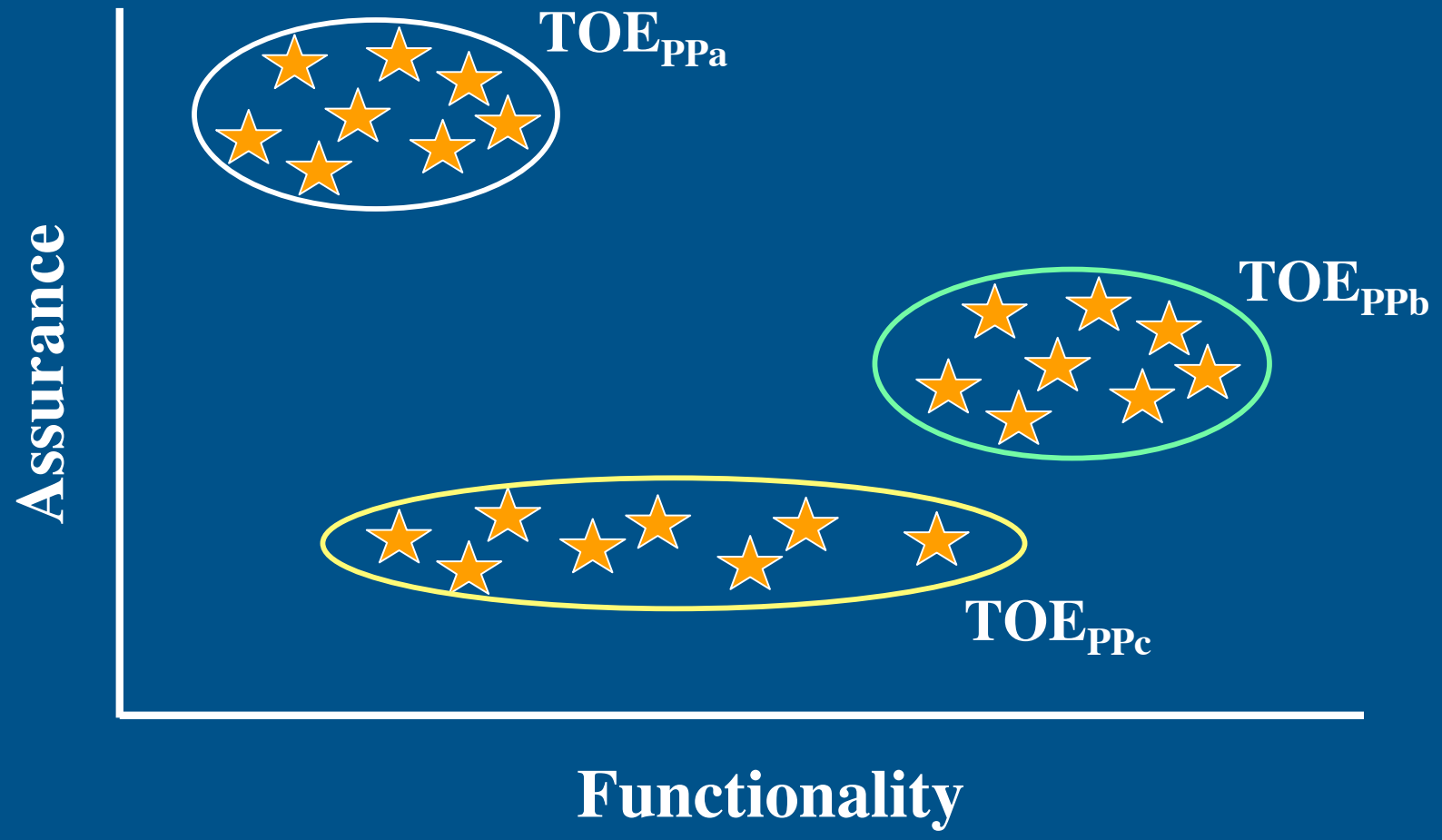
What CC protection profiles do: Constrain the space

- CC Protection Profile concept
  - Remedies some problems possible with ITSEC evaluations
    - Vendor could make claims for any point in the space of functionality × assurance and have those claims evaluated
    - Users were left comparing apples and oranges
  - PPs constrain the space of compliant products
  - PPs are written and evaluated by experts to present a “balanced” set of requirements to developers

What CC protection profiles do :
Unconstrained Function × Assurance space

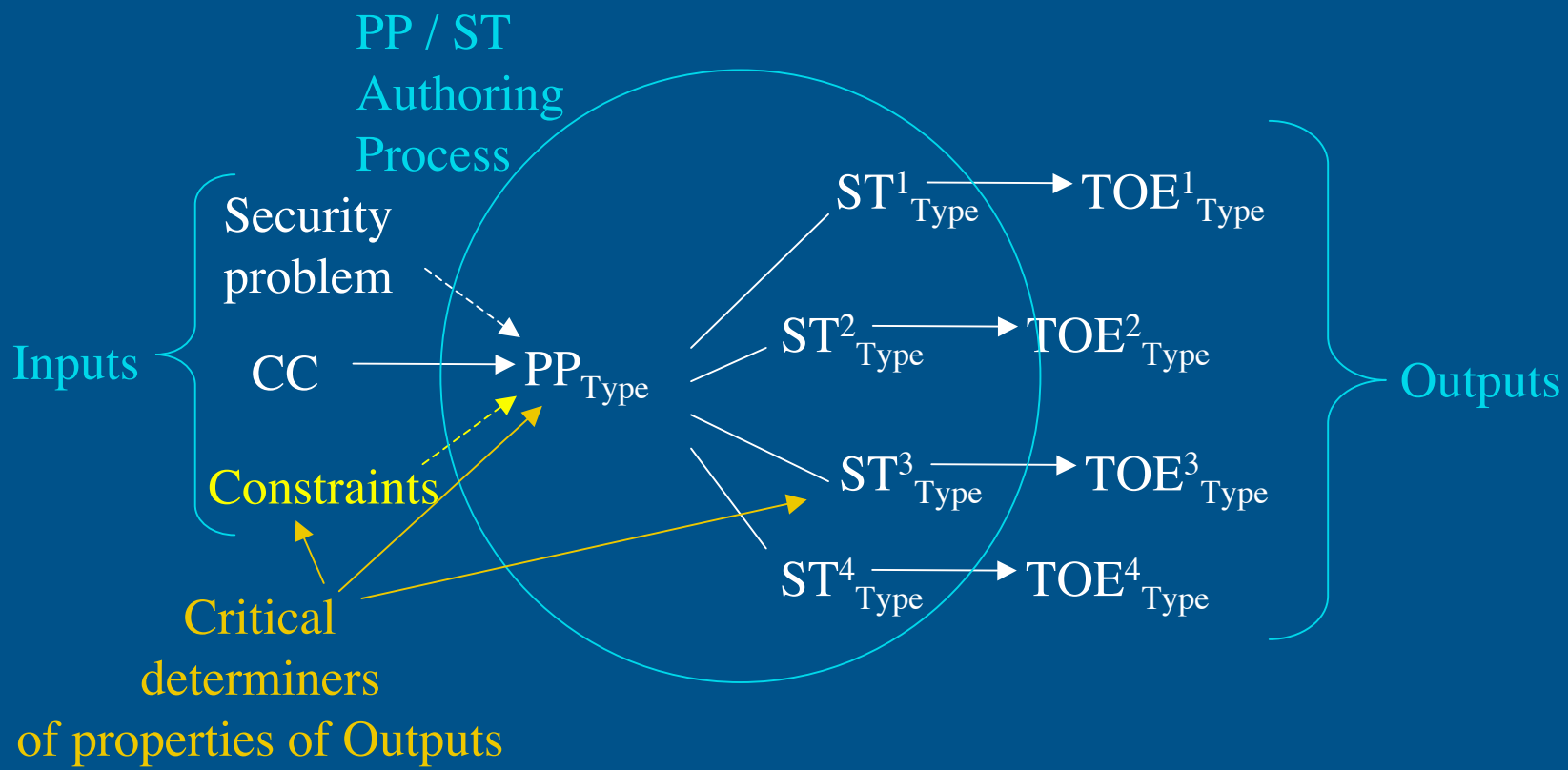


What CC protection profiles do : Function × Assurance space constrained by protection profiles



CC-based product (TOE) development

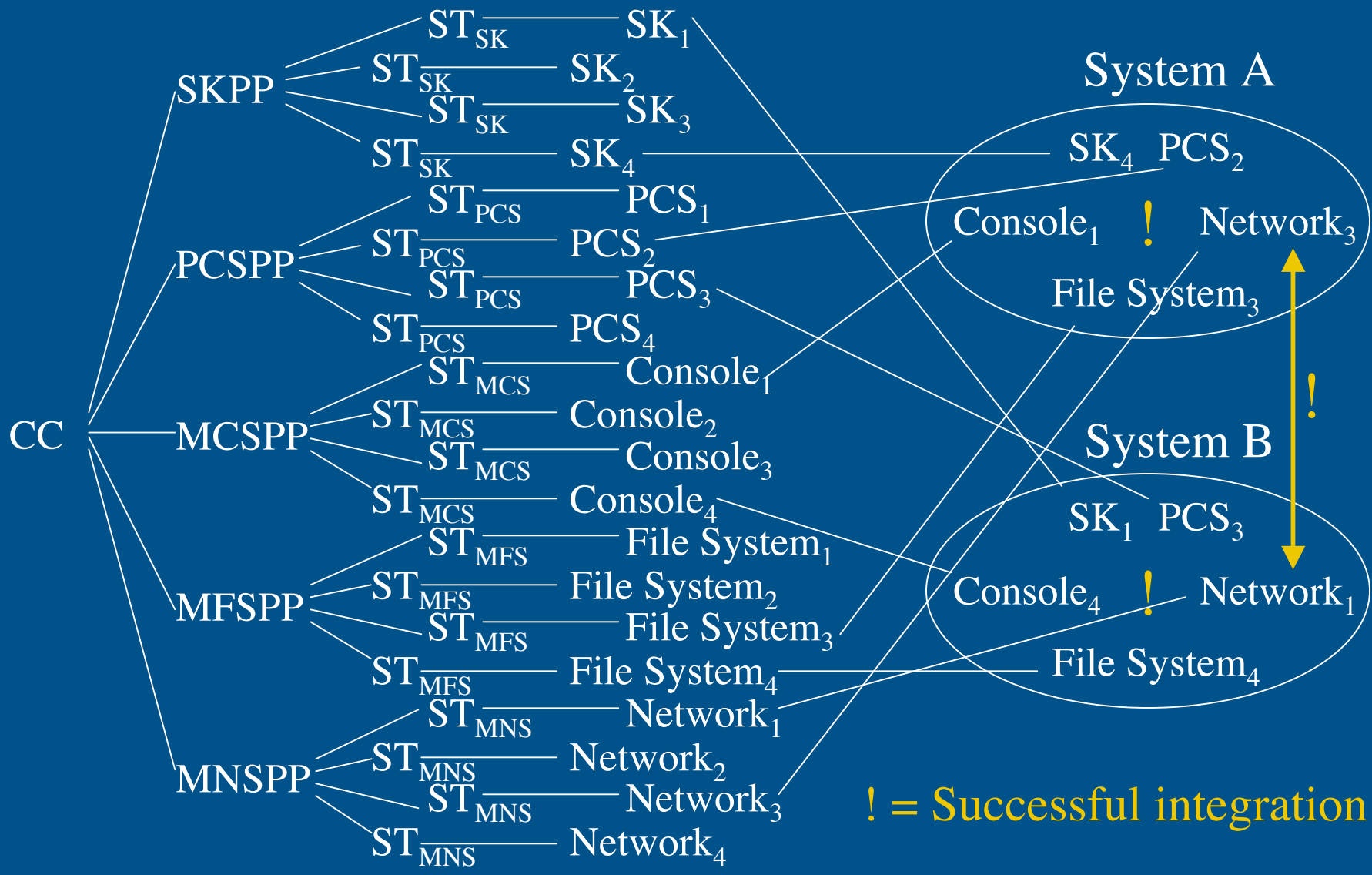
We expect multiple TOEs of each product type and have expectations of a relationship among instances of Type and with instances of other types



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

- MILS Integration Protection Profile (MIPP)
- Separation Kernel (SKPP)
- Partitioning Communication System (PCSPP)
- MILS Console System (MCSPP)
- MILS Network System (MNSPP)
- MILS File System (MFSPP)
- . . .

MILS PPs are expected to achieve:



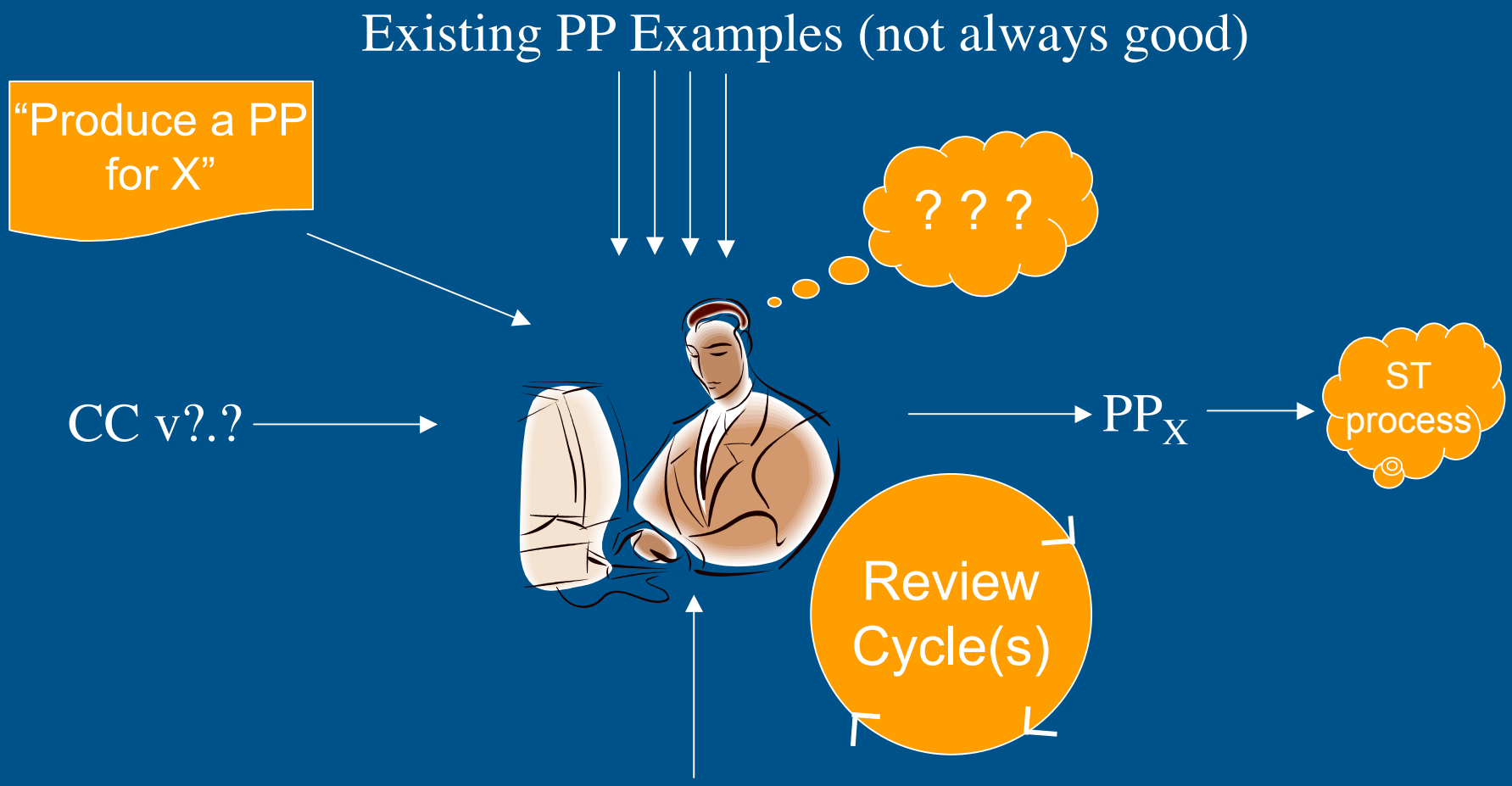
MILS architecture is *based on* ***composition***

- A dual challenge of high assurance and composition
- Components independently developed by different vendors
- Components are defined by Common Criteria-style protection profiles (PPs)
- The ***collection*** of PPs reflects an intended ***architecture***
- The PPs must be in agreement with the architecture
- ***CCAE is a vehicle to achieve this agreement***

Desirable composition support

- Successful composition requires
  - Policy composition (that enforced by each component's TSF)
  - Functional compositionality (foundational and operational)
  - Functional Interoperability (interfaces, interactions, behaviors)
  - Results in additional constraints on PP/ST/TOE development
- Apply CC CAP packages and ACO evaluation methodology
- Constrain PP/ST development beyond current CC guidance
  - Constraints flowed-down from the MIPP
  - Constraints from other community standards
  - Constraints on definitions of concepts and vocabulary for expressing the security problem and security environment
- Additional requirements in PPs
  - Ensure additional requirements are represented in new PPs
  - Apply uniformly across collection of composable products
- Provide a parallel framework for non-CC composition requirements

How many PPs have been written



Challenges of PP authorship

- It takes a long time (2+ years) and a lot of effort ($$$)
- Very tedious and error prone work
- Requires "legal" precision of language unfamiliar to some
- Bad examples are propagated like a virus
- Difficult to track differences in CC versions
- Difficult to assess impact of global change to MILS PP family
- Difficult to generate and maintain mappings in a PP
- Difficult to check consistency and completeness
- Difficult for PP to feed into further development
- Authors may have limited expertise in CC or security
- PP and ST authors have little guidance or ability to enforce / achieve shared standards
- Little support to structure the author's PP development effort
- Nothing to assure that the MILS PPs will "hang together"

The CC Authoring Environment for MILS will provide (1/2)

- Common Criteria in a structured, "machinable" form
  - Capturing the semantic content
  - A "Plugged-in CC" , instead of "CC Unplugged"
- Library of documentation generation objects
  - Foundation document object classes
  - Formatting and typography rules
- Catalog of (re)usable community standards:
  - Definitions of basic CC and MILS terms
  - MILS evaluator guidance and robustness level guidance
  - Threats and countermeasures
  - Bibliography of MILS-related references

The CC Authoring Environment for MILS will provide (2/2)

- Mechanical checks
  - Consistency
  - Constraints needed for composability and compositionality
  - Requirements traceability
  - Analysis and Statistics
- Guidance based on expert knowledge base that can evolve and be adapted.
  - Security ontology
  - Workflow rules
  - Expert usage / instantiation patterns
  - Decision support
  - MILS Integration PP relationships and constraints
  - CC documentation conventions
  - Guidance for desired robustness level
  - Evaluator guidance
- Output that can be (re)consumed by CCAE and/or other tools

The CC Authoring Environment for MILS Benefits (1/2)

- Achieve uniformity and sufficiency of PPs and STs
- Relieve much of the tedium, to better apply author's effort
- Reduce/eliminate many types of errors and inconsistencies
- Reduce the document maintenance problem
- Shorten PP and ST development time and raise quality
- Can be used by authors and reviewers of PPs and STs to explore/query the information represented in the document
- Explore / create "what if" variants
- More easily adapt to later versions of the Common Criteria
- More easily incorporate evolving community standards
- More easily revisit existing PPs and STs when security environment or external requirements change

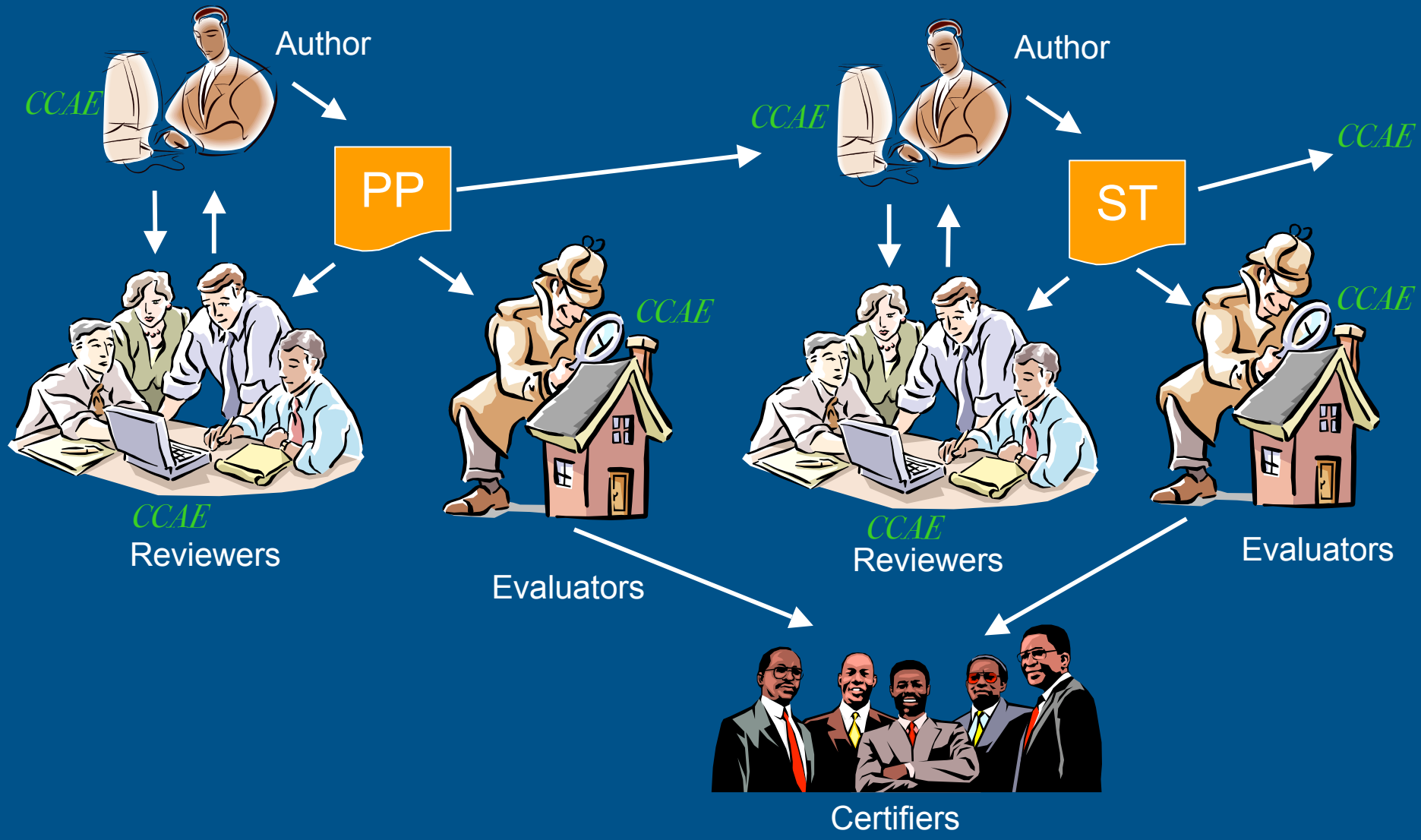
The CC Authoring Environment for MILS Benefits (2/2)

- MILS PPs harmonized to achieve "additivity" property for foundational PPs
- Expert knowledge base can grow, adapt, come from new sources, and be refined and effectively be passed on to others
- Automated repeatable checking encourages continuous QA
- Produce a database representing the current stage of product definition that can be input to the next stage
  (e.g., PP --> ST --> …)
- Produce output that can be consumed by other tools during product development
- Provide a vehicle for applying / propagating the MILS Integration PP constraints to all MILS component PPs and guaranteeing coherence
- Help ensure that the PP or ST remains a living part of the definition and development of a product

TheCC Authoring Environment for MILS
What it is *Not*

- Not a pushbutton protection profile
  - Not a "Protection Profiles for Dummies"
  - Not a substitute for a knowledgeable author
  - It IS a power tool for subject matter experts
- Not a simple "template" for a protection profile
  - It IS more like a class library, with inheritance, that must be instantiated and specialized for a particular PP

Users of the CCAE



Future Vision for the CCAE

- MILS Collaborative Portal - web services-based
  - Centralized support for authors, reviewers, evaluators, and developers
  - Online repository
- MILS Coordination Services Framework
- MILS Component Interoperability - avoid “semantic dissonance”
  - Support for evaluation documentation development
- MILS Component Interoperability
  - Synergistic with another SRI project (ONISTT) that has developed a workable approach to improvisational interoperability of complex DoD systems
  - ONISTT concepts / implementation techniques similar to CCAE: expert knowledge, ontologies, reasoning engine, Prolog/OWL/XML
- Evaluation Documentation (ADV) Support
  - A natural and direct extension of CCAE support for PP/ST development

Collaboration

- Collaboration without meetings
- Partial automation of informal social process*
- Keep central repository of expert knowledge
- No distribution or update headaches
- Seamless way to provide feedback in a semantically rich way
- Medium for formal “buyer-seller” contracts
- Community of authors, reviewers, developers, evaluators, integrators, certifiers

*** Bunch Of People Sitting Around a Table**

CCAE Collaborative Environment

CC Authoring Environment illustrated

PP/ST Author

Rule Base
CC Component Operation Rules, Semantic Rules, Relational Model, Workflow Rules

Env Library
Components, CC SFRs/SARs, Interps, CIM, Security Ontology, Resource Registry MILS Integ FW

CCAE Document Repository

UI Agent

Parent PP, MILS TOE Concept, or TOE Flow-down Requirements

Document Creation/Revision
Doc Assembly, Catalog Selection, Checking, Rewriting, Inference, Rule Execution, Queries, XML gen

Current Document Factbase

Doc Creation Library
Conventions, Doc comp classes Doc generators: PP, ST, FSP

XML

Project Team Exchange or Export

Document Publishing
Rendering & Conversion

PDF, DOCX XLSX, …

Documents & Reports

PP, ST, stats

Negotiation model of interaction

- Objective: Achieve a PP that is *acceptable* to both CCAE and the author
  - There is considerable latitude in this outcome -- we do not want to force too specific an embodiment or restrict the author's creativity
- 2-party negotiation
  - The author and CCAE share the Objective
  - Both the author and CCAE acknowledge they don't have perfect knowledge of an "evaluatable" PP -- that will be externally decided in evaluation
  - Author brings initiative, understanding, creativity, and common sense
  - CCAE brings process framework and an array of techniques serving as a proxy for a true oracle
  - The CCAE works with the author from the start
  - The parties rest when both are satisfied with the PP to the extent of their ability -- then it goes to review or evaluation
- Staged development
  - CCAE can work in stages with an incomplete PP
  - Each stage concentrates on a particular aspect of the PP development
  - Allows interim review versions
  - Can apply gradually increasing threshold of acceptability as PP completed

Libraries - e.g. environment library

- "Plugged-In" Common Criteria, by versions
  - Lifetime of last official version, 13 months (proves the point!)
  - CC versions 2.3 and 3.1 available in XML
    - CC parses into Prolog terms with existing SGML / XML parser
    - Build relations within the CC, e.g., dependencies, EALs, custom EALs
    - Index back to text in XML for display and export
    - Relations to MILS ontology and expert knowledge
  - Support for older versions would require some labor
- MILS technology and security ontology
  - Create with Protégé/OWL
  - OWL (Ontology Web Language) library for Prolog
  - Create a consistent and semantically rich representation of security threats, policies, assumptions, objectives, functional countermeasures, and assurance measures
  - MILS conventions and standards
  - Flow-down constraints from MILS Integration PP

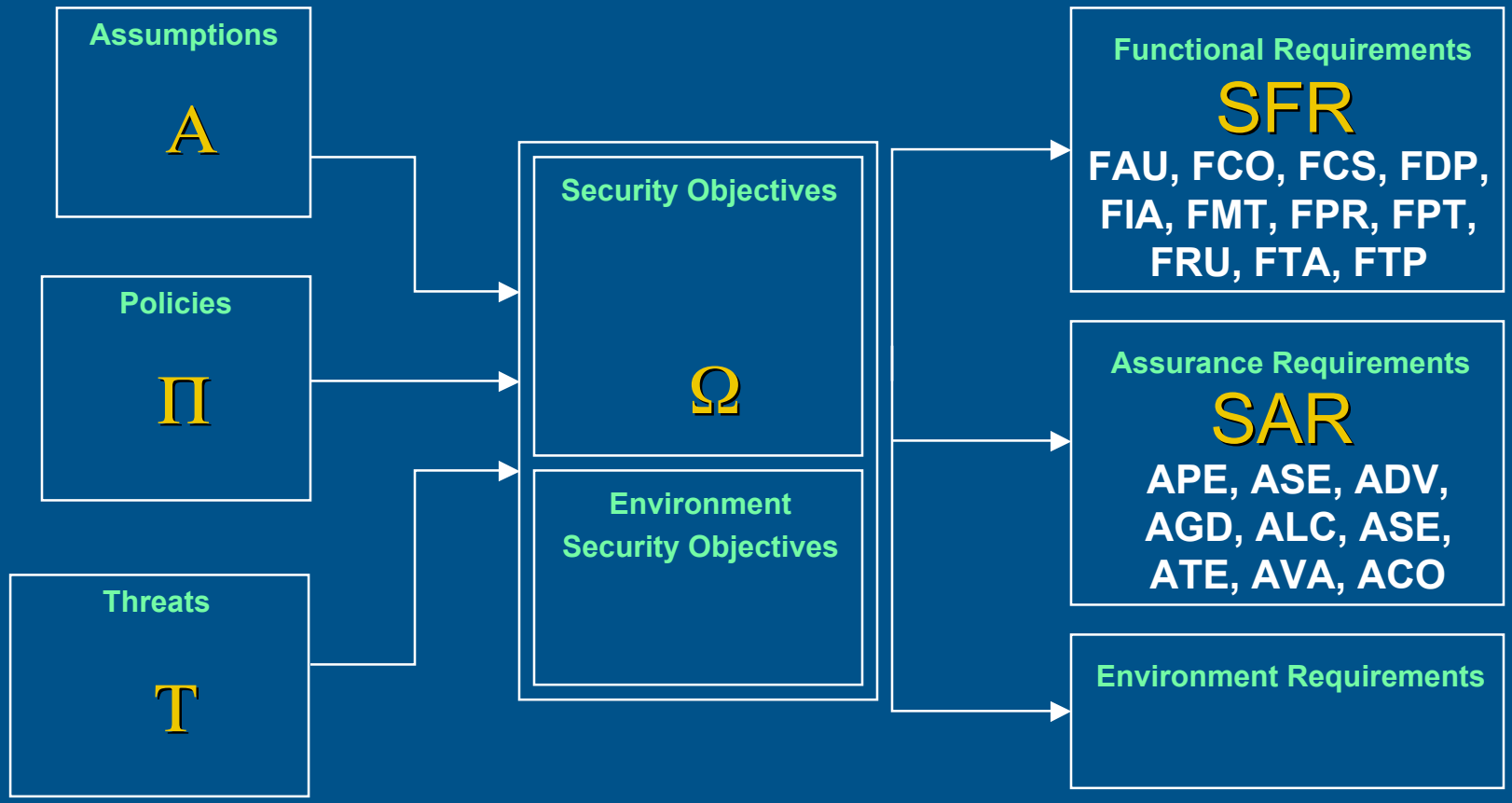
Expert Knowledge

- PP authors may not be security experts and/or may not have written a PP before
- We would like to effectively bring to the author the knowledge of experts:
  - Security engineering
  - Evaluation requirements and methodology
  - Academia and security research
  - Common Criteria model, methodology, and documentation
  - MILS architecture
- Evolving and improving on an on-going basis
- Distributed and applied by authors as quickly as possible

Simplified relational model of a PP

Let

- T universe of threats
- Π u. of organizational policies
- A u. of assumptions
- Ω u. of security objectives
- SFR u. of CC security functional rqmts
- SAR u. of CC security assurance rqmts



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

Simplified Relational Model of a PP

- The Ω-anchored space PP of tuples

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

  represents all possible PP relations

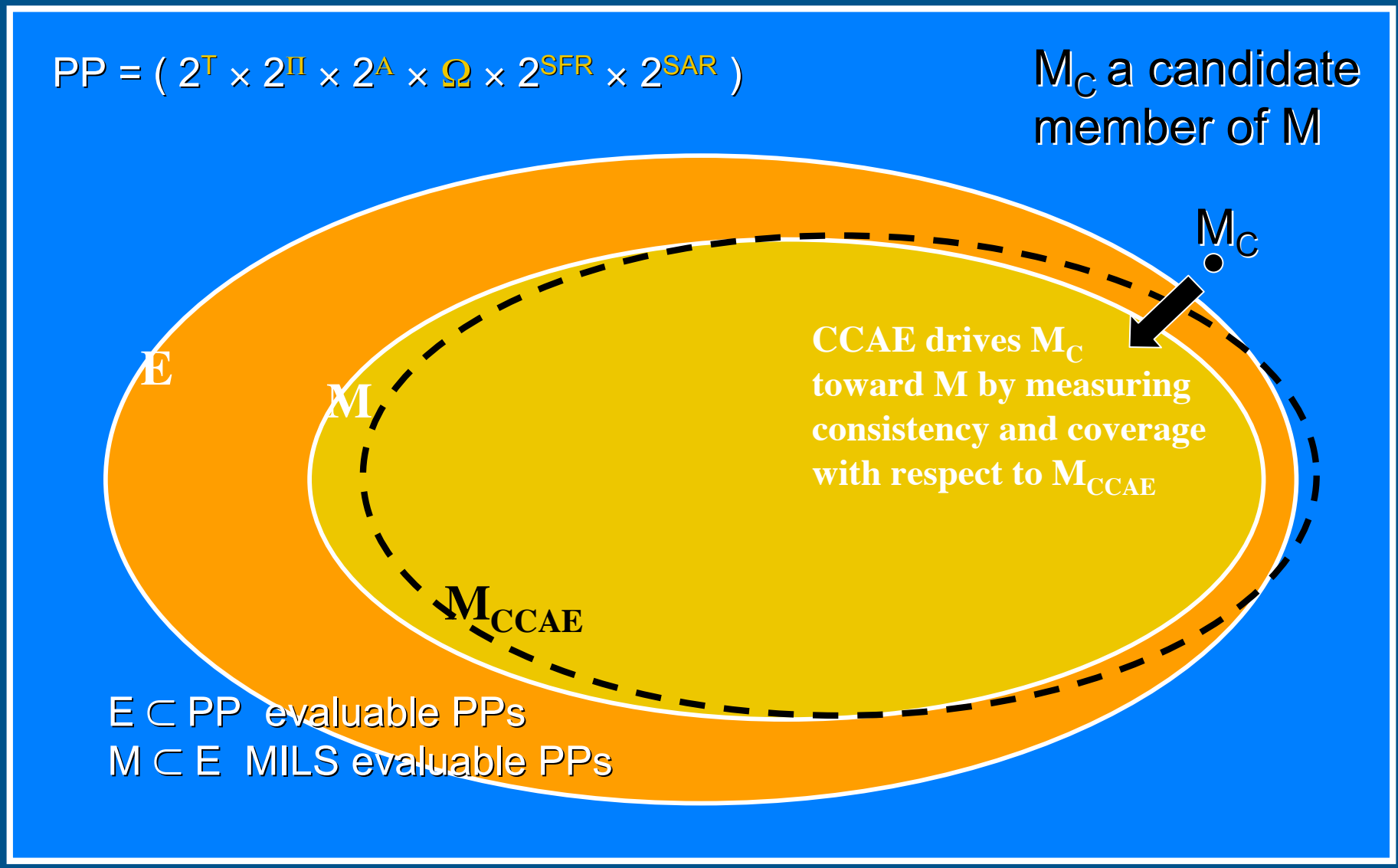
- The relation E:

$$E \subset (2^{T} \times 2^{\Pi} \times 2^{A} \times \Omega \times 2^{SFR} \times 2^{SAR})$$

  is an oracle accepting "evaluable" PPs

- The relation $M \subset E$ is an oracle accepting evaluable MILS PPs
- E and M are *unknowable a priori*

M_{CCAE} Approximation of M



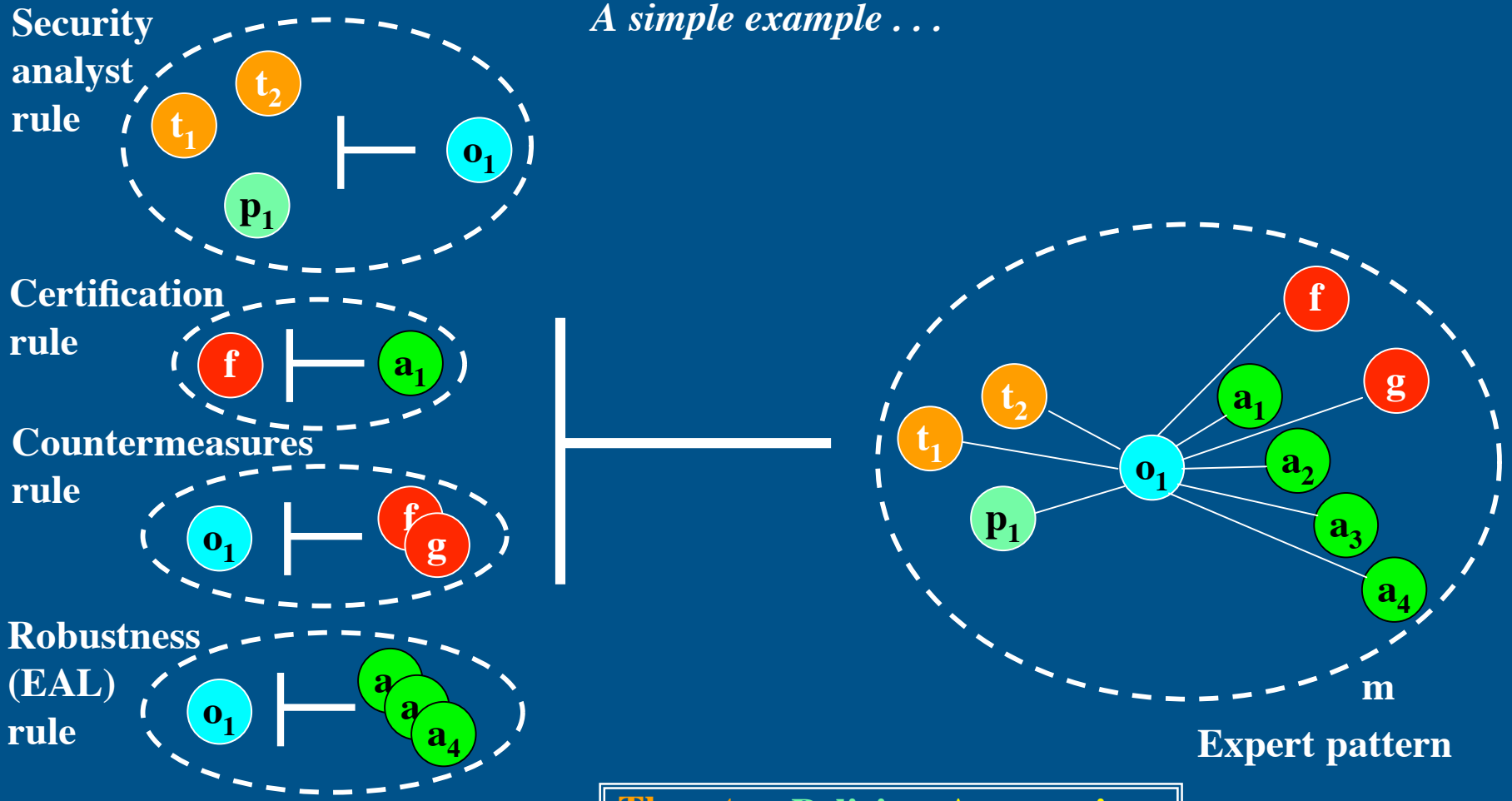
Expert Guidance and Advice (1/3)

- The concept: bring a dynamic body of expert knowledge to bear from the start of every authoring activity
- Knowledge acquisition
  - Explicit rule encoding
  - Generalization from expert interaction on specific authoring projects
  - Harmonization of knowledge from different experts
- Knowledge application
  - Expert patterns constructed from expert knowledge base
  - Author patterns are constructed from the draft PP
  - Author patterns are “compared”* to expert patterns
  - Advice is generated for the author’s consideration
- Negotiation model of interaction
  - author and system negotiate an acceptable PP

*** fuzzy unification**

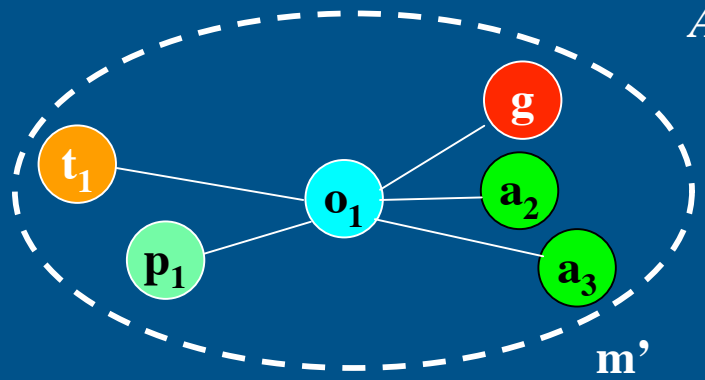
Expert Guidance and Advice (2/3)

A simple example . . .



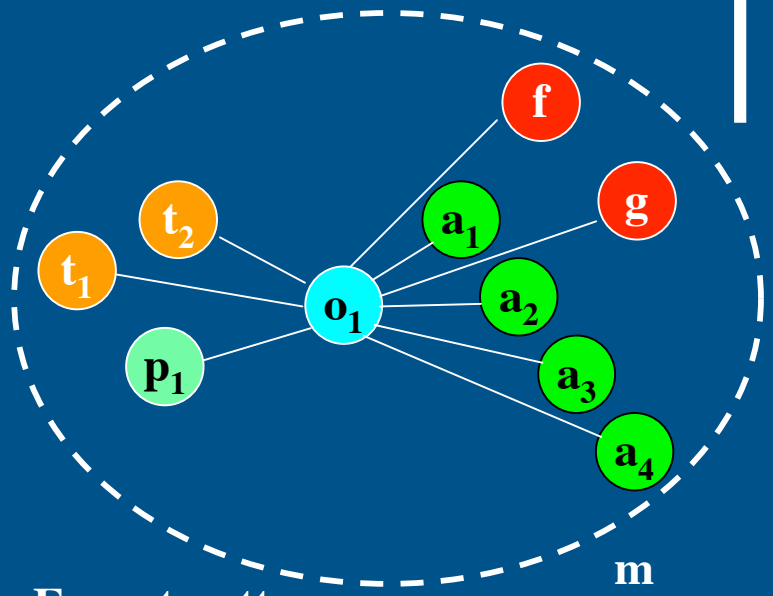
Expert Guidance and Advice (3/3)

A simple example . . .



Draft PP pattern

$m' \approx_F m$



Expert pattern

Advice

Threat t_2 may be an unidentified threat

Objective o_1 is customarily realized by countermeasure f in addition to g

Assurance measures a_1 and a_4 may be needed due to the EAL sought and a certification requirement associated with countermeasure f

$m' \approx_F m$ inference + fuzzy unification

Threats **Policies** **Assumptions**

Objectives

SFRs **SARs**

•Summary and Recommendations

- MIPP establishes architectural relationships and constraints on components, CCAE provides a vehicle to support composition by managing constraints among component PPs
- CCAE can facilitate CC-based PP/ST process and also provide framework for extra-CC coordination
- Future versions of CC could consider some of the issues that have motivated our work
  - Product lines, product families, “polymorphic PPs”
  - Changes to systems, integration for systems-of-systems
  - Explicit assurance cases to focus efforts
  - Elevated component element levels, for higher EALs
  - Elevated PP/ST scope/depth/rigor at higher EALs

Grazie

Fine

CCAE-supported author, reviewer, evaluator tasks

Choose security environ threats, policies, assump.	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

CCAE-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 CCAE
Assure dependencies and consistency	Apply known dependencies in CC and knowledge base