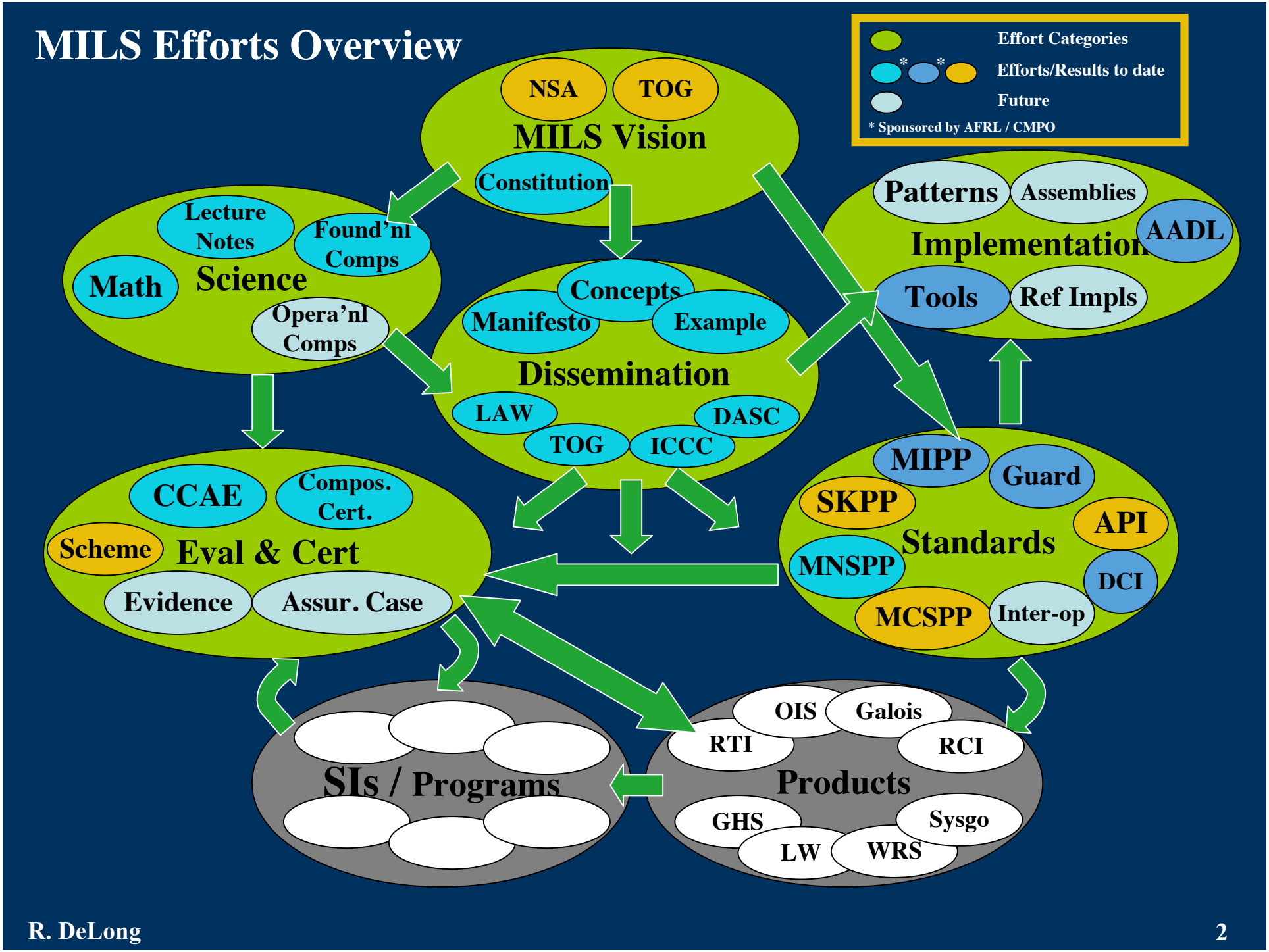
MILS Research Montage

LAW
Work-In-Progress Session
December 6, 2011

Rance DeLong
Consulting Researcher

MILS Efforts Overview



Research Enabling MILS Development and Deployment (REMDaD)*

- Objective:
  Move to next stage of MILS deployment and development
- 4 Themes
  - Components – development and assurance of individual components
  - Integration – integration of MILS components and systems
  - Deployment – facilitate MILS deployment
  - Certification – enable MILS evaluation and certification
- Initial tasks (2010)
  - Evidence and toolchains for MILS certification study
  - MILS Cross Domain Solution (CDS) operational component Study
  - MILS Delivery, Configuration, and Initialization (DCI) Study

* Performed at SRI, sponsored by AF Research Laboratory and AF Cryptographic Modernization Program Office.

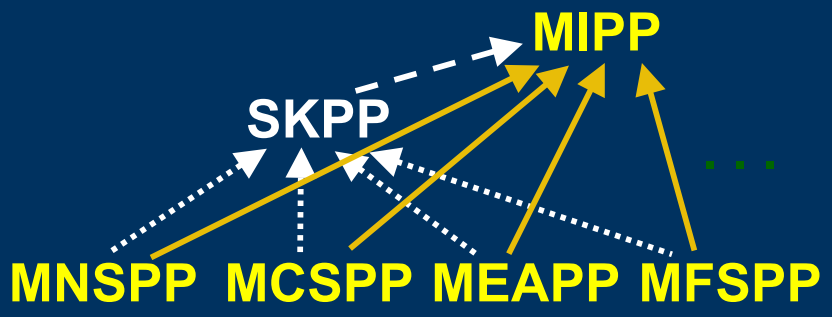
Research Enabling MILS Development and Deployment (REMDaD)*

- Current tasks (2011-2012) -
  (John Rushby, Dave Hanz, Rance DeLong)
  - AADL and MILS
  - MIPP completion (MIPP as a document)
  - “Programming the MIPP” (MIPP encoded in the CCAE)
  - MILS Delivery, Configuration, Initialization model
  - MILS Cross Domain Solution investigation
  - MILS Network Subsystem Protection Profile

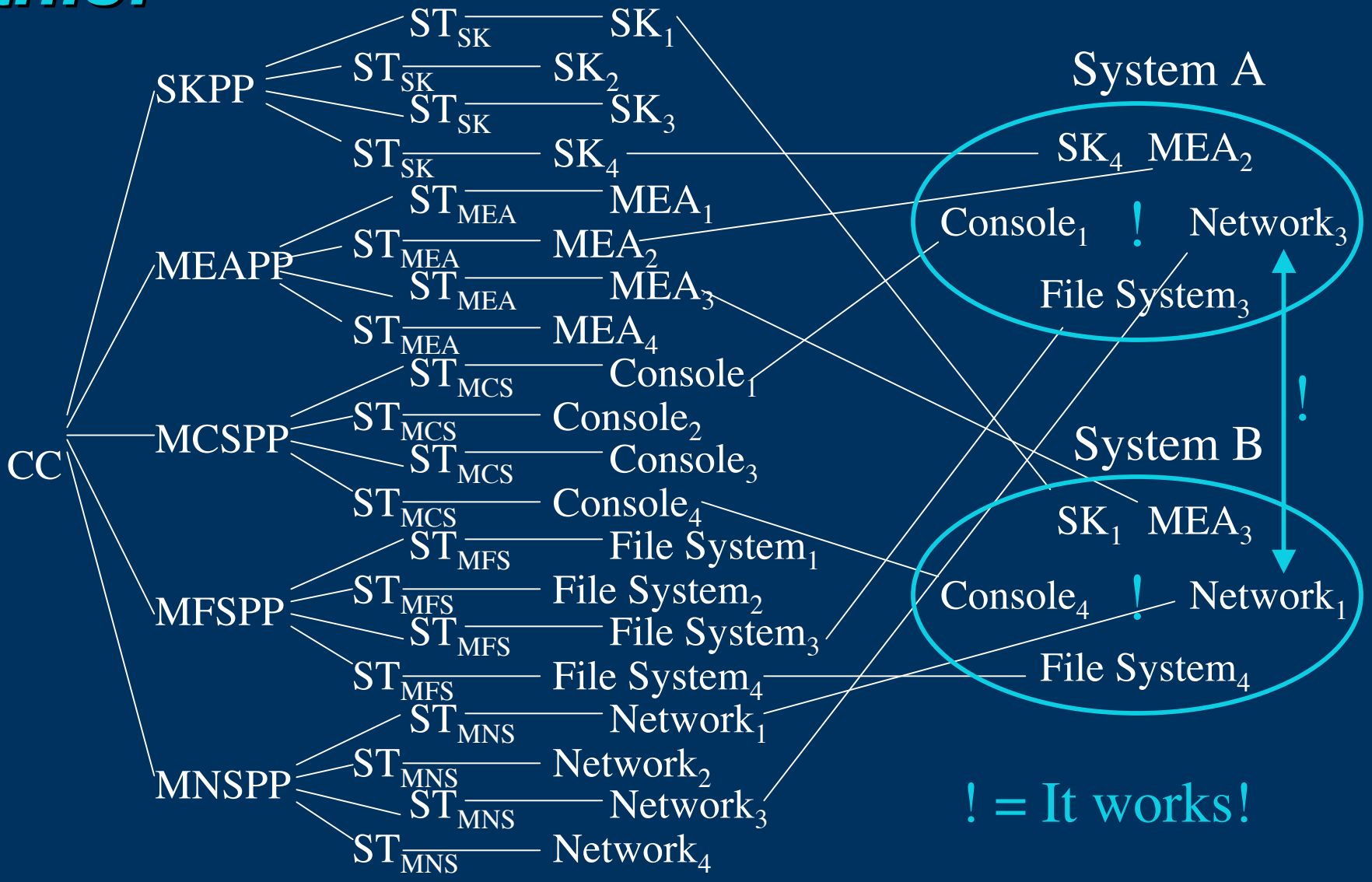
*** Performed at SRI, sponsored by AF Research Laboratory and AF Cryptographic Modernization Program Office.**

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

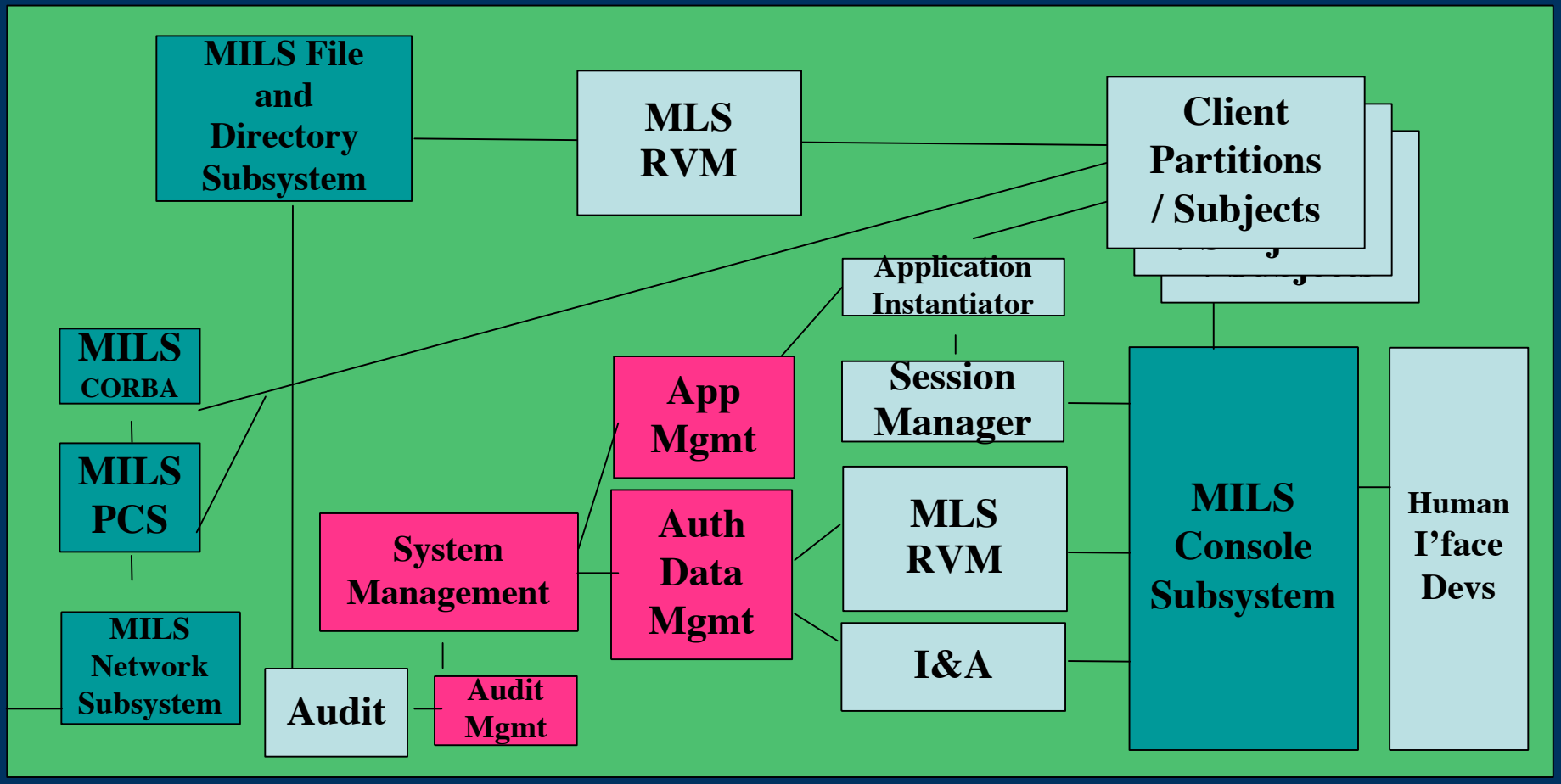
- Separation Kernel (SKPP)
- MILS Network System (MNSPP)
- MILS Console System (MCSPP)
- MILS Extended Attributes PP (MEAPP)
- MILS File System (MFSPP)
- . . .
- MILS Integration Protection Profile (MIPP)



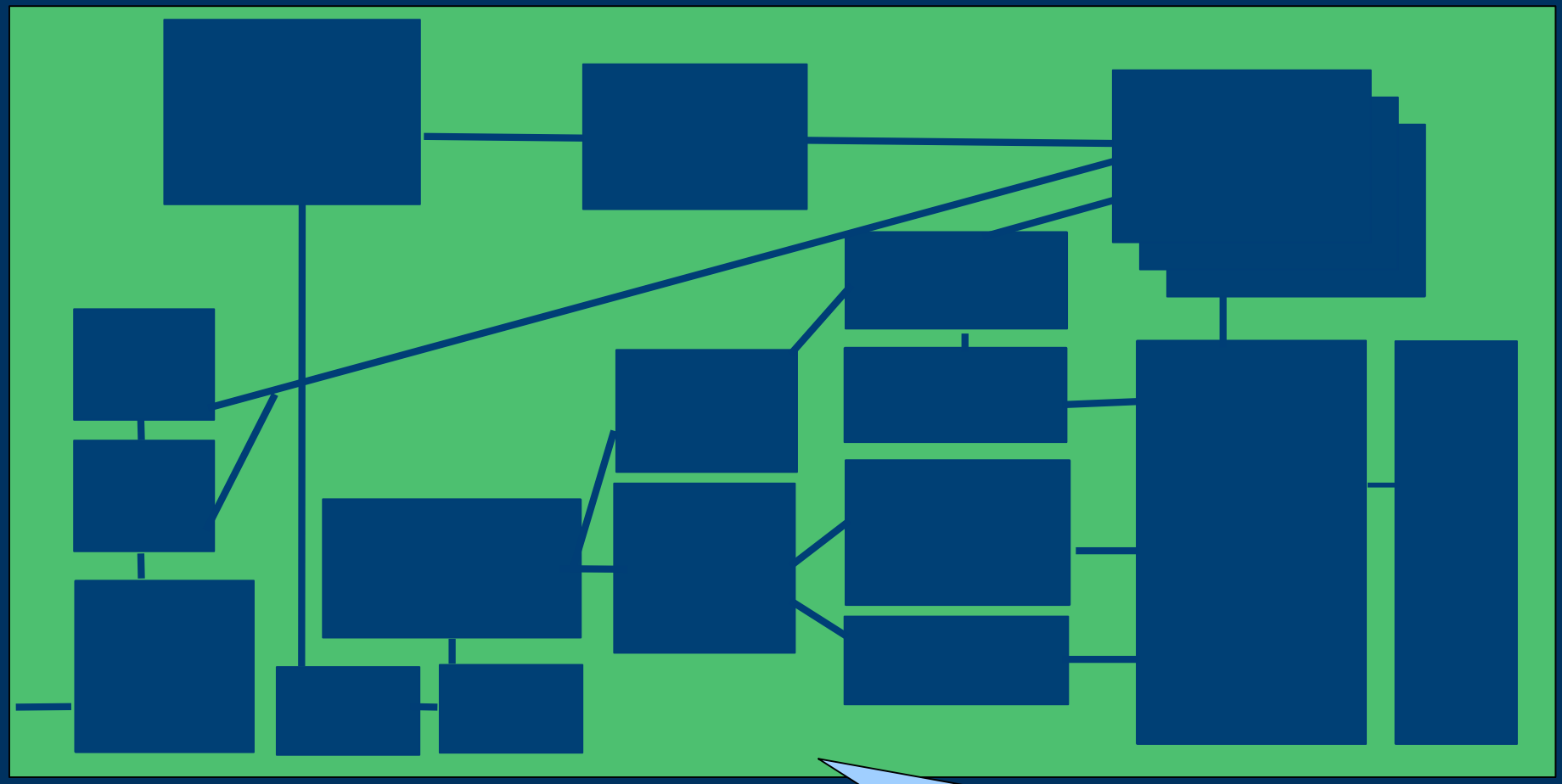
Mils PPs are expected to achieve *this:*



Illustrative Architecture of a MILS-based MLS workstation - a collection of connected "things"



Architecture of a MILS based workstation - itself is *Something*



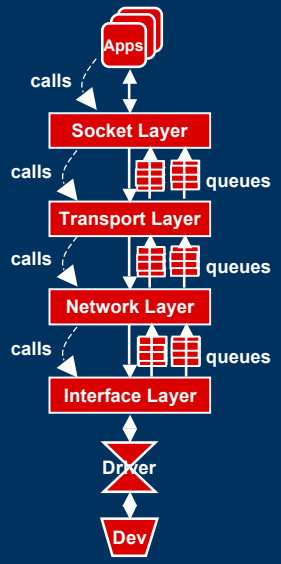
Something that must be designed.
Something that has properties.

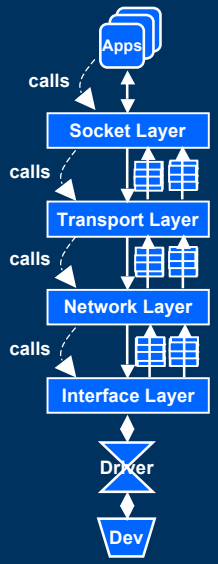
Architecture as an
Integration Framework

This *Something* is what the MIPP describes

- The system level security problem (T/P/A)
- The system level security objectives
- The system level SFRs and SARs
- A system concept and reference architecture
- Identification of, and connections among, the components
- A basis for formal composition of component properties
- Constraints on the MILS components that fit in the “holes”
  - Security objectives, or modified ones, that pass to the component
  - Relationships and obligations (rely-guarantee) among the components
  - Interaction schemas for interacting components

Some architecture alternatives for MILS network system





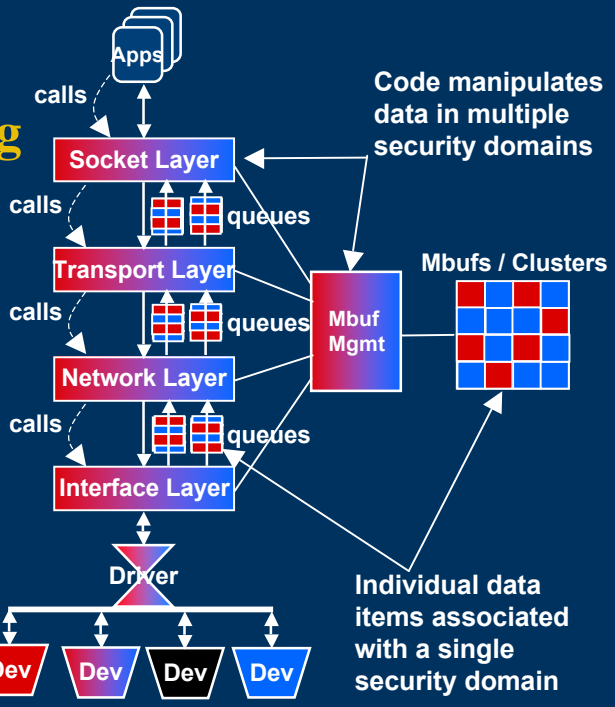
Nothing Trusted

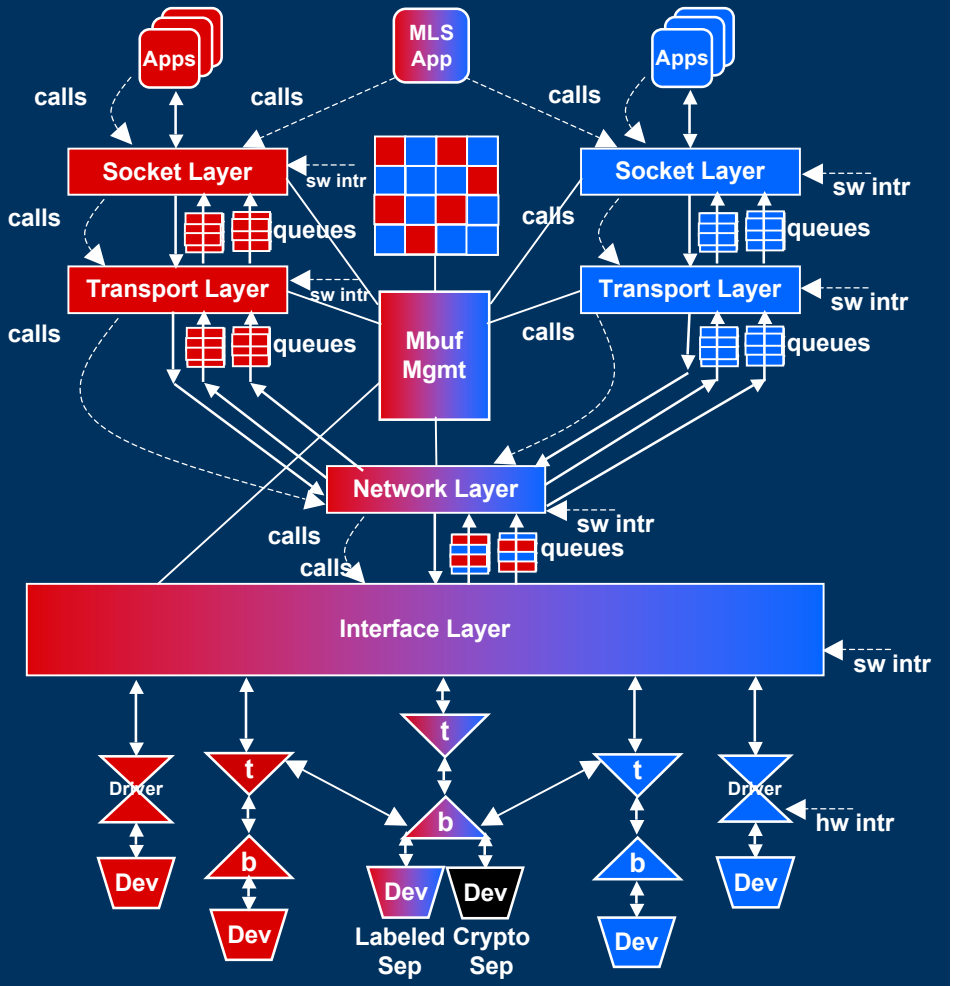
queues

queues

queues

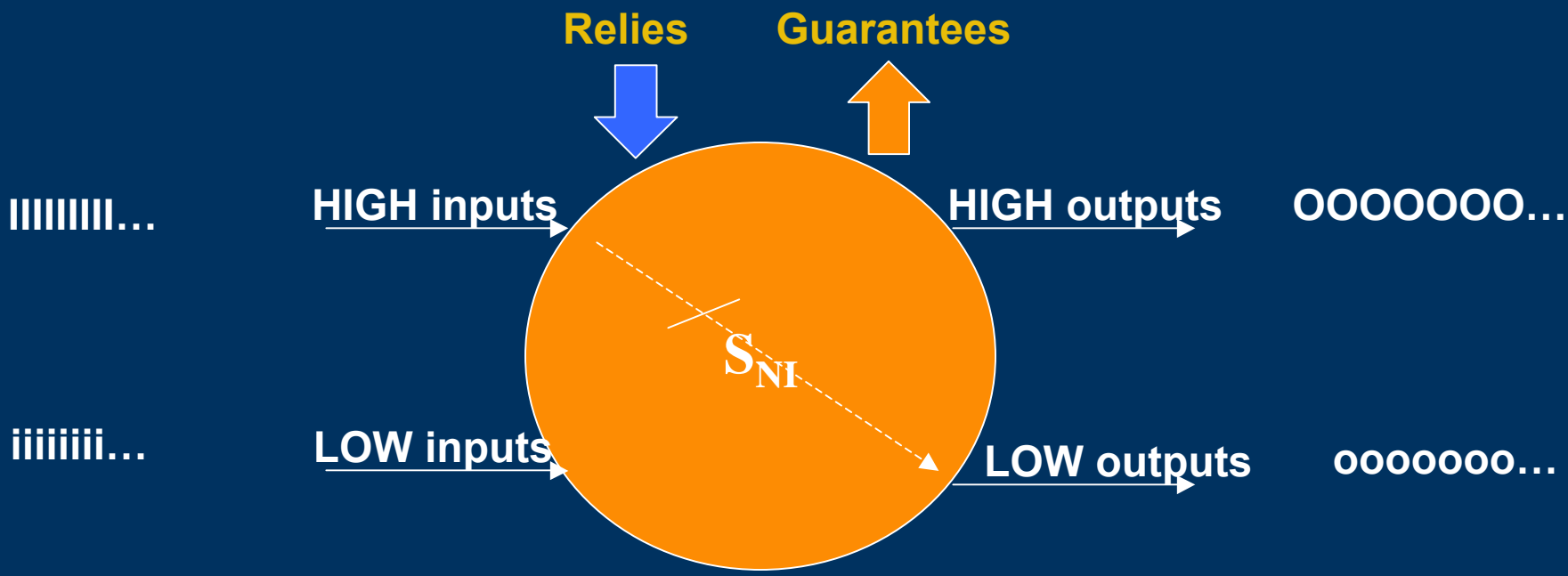
Everything Trusted



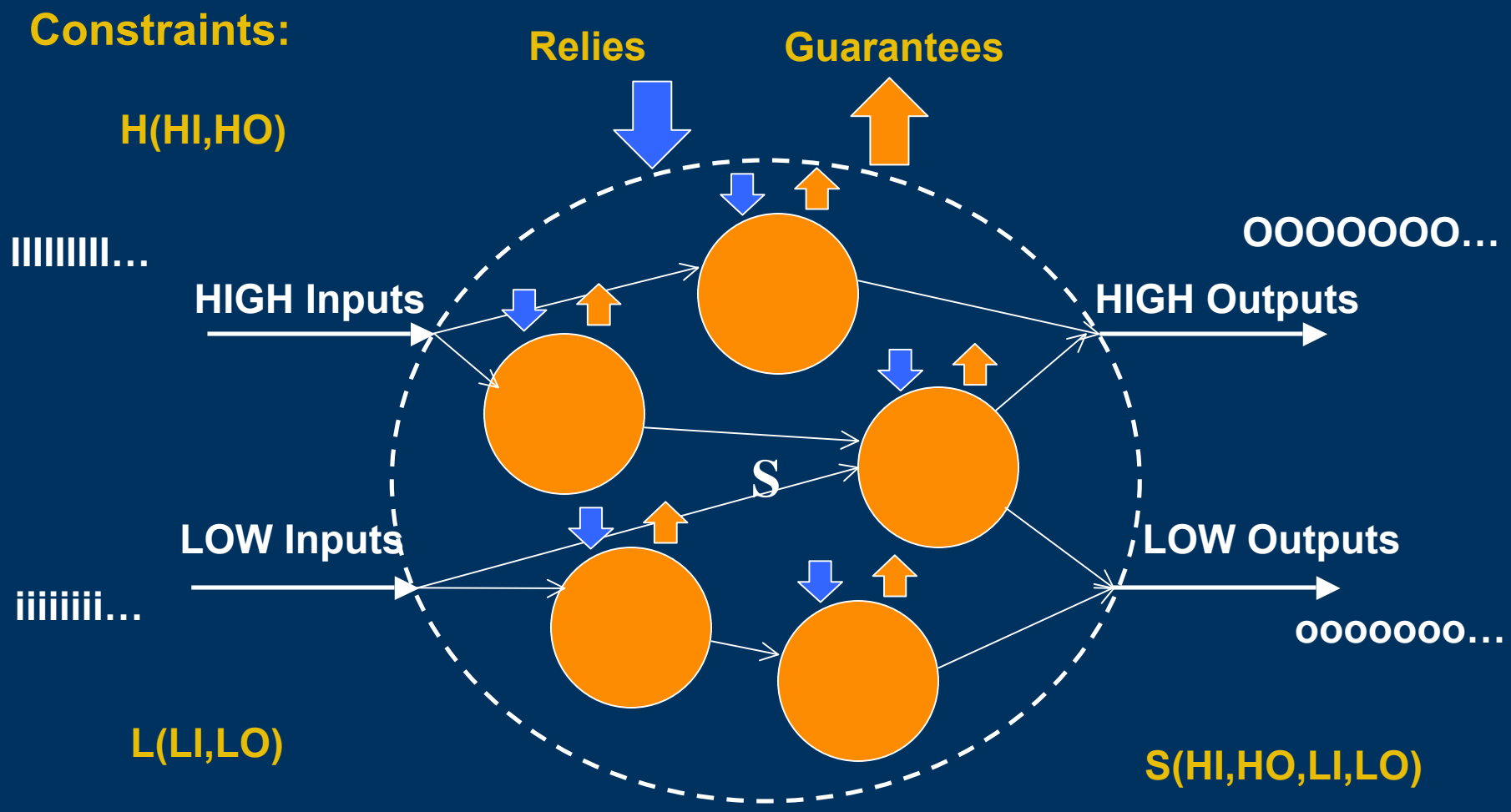


Combination of Trusted and Untrusted

System Inputs, Outputs, Relies and Guarantees

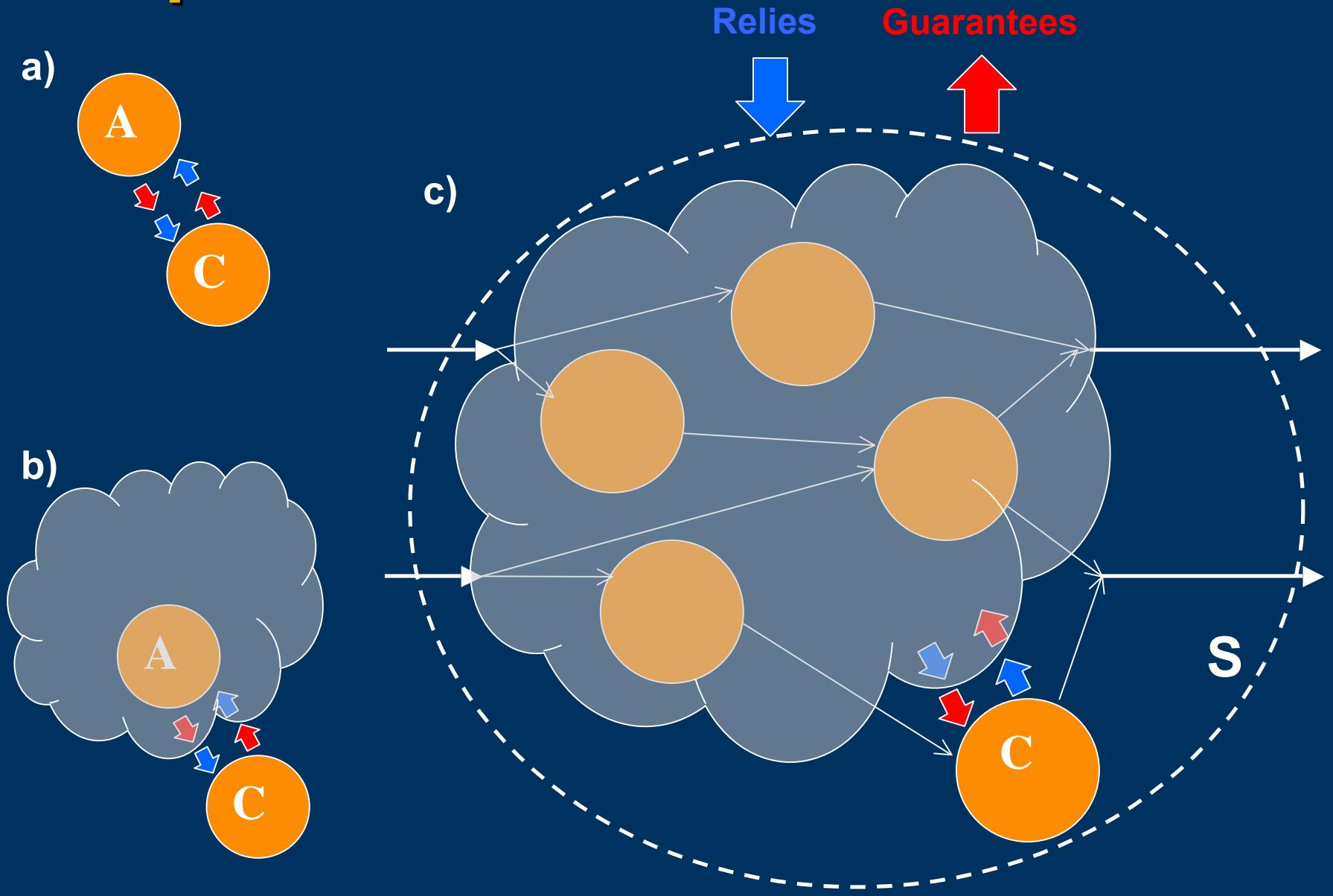


MILS System from Components/Subsystems



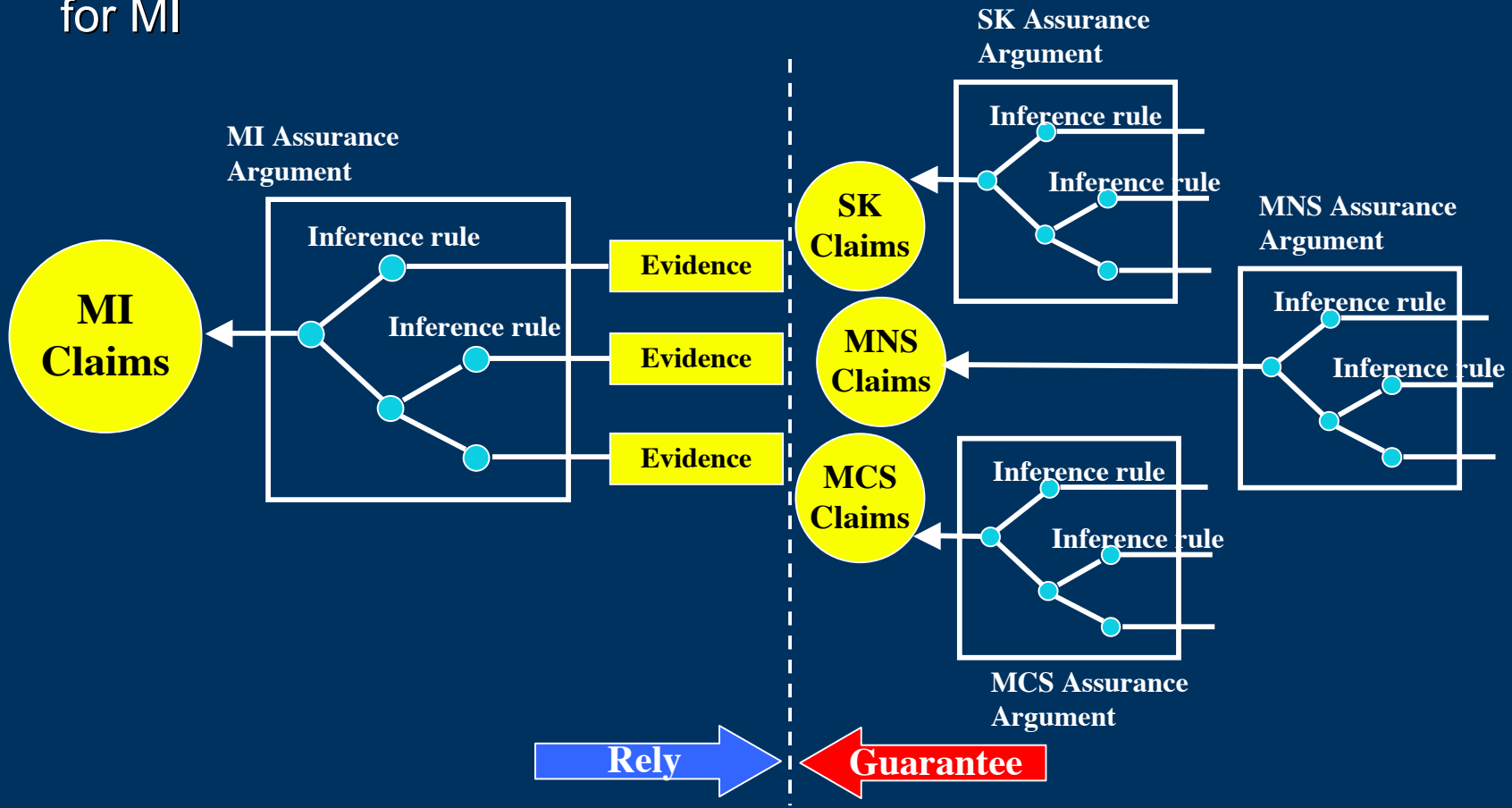
Properties: P(HI,HO,LI,LO) st S ≤ P

Compositional Relies / Guarantees

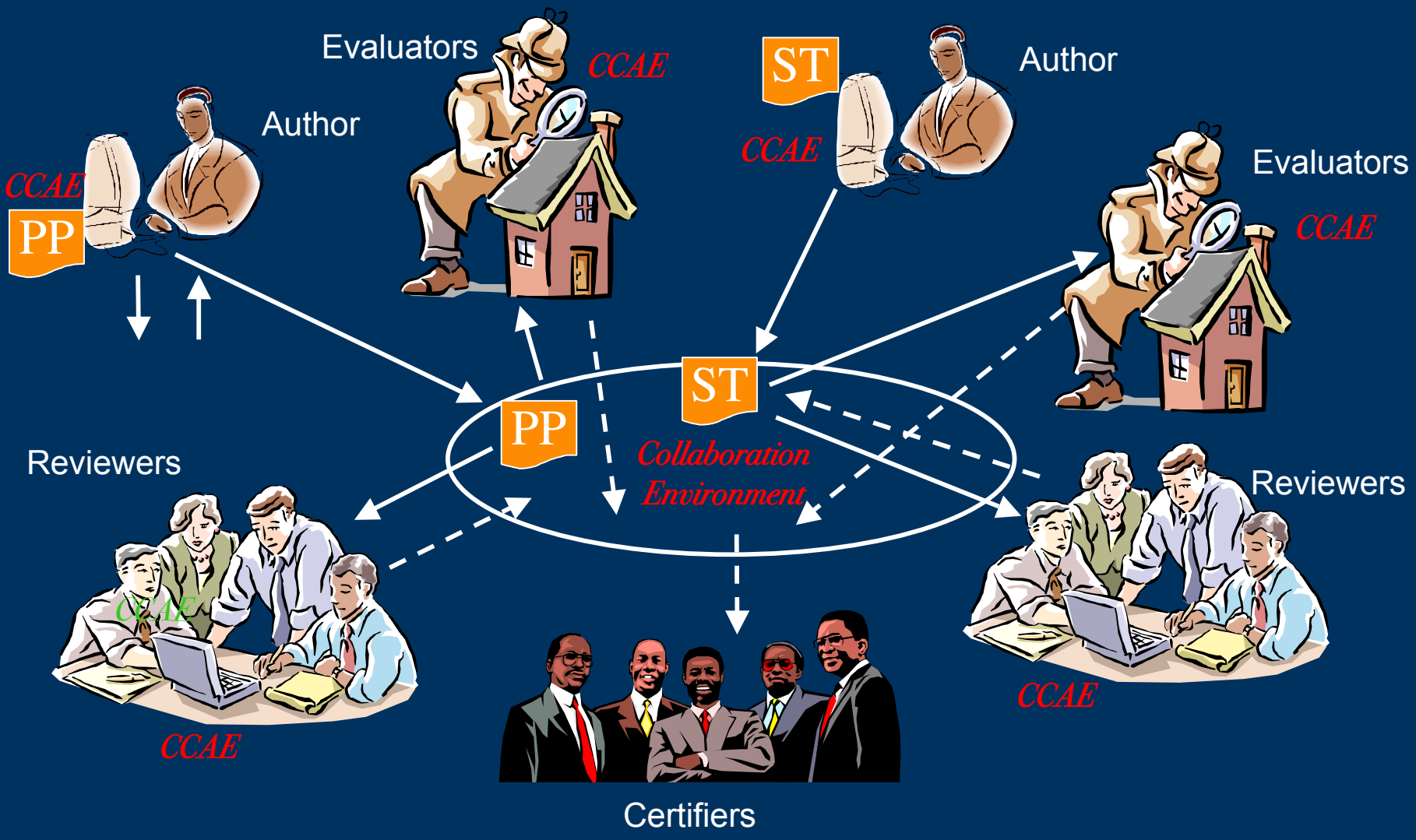


MILS Composite Assurance Case

- Compose assurance cases using Assume-Guarantee Reasoning
- Assumptions from MI assurance case become requirements on the components
- Assured Claims from component assurance cases become evidence for MI



Common Criteria Authoring Environment as a distributed collaboration environment



CCAE User and Components

Author/Reviewer

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, Reviewing, 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

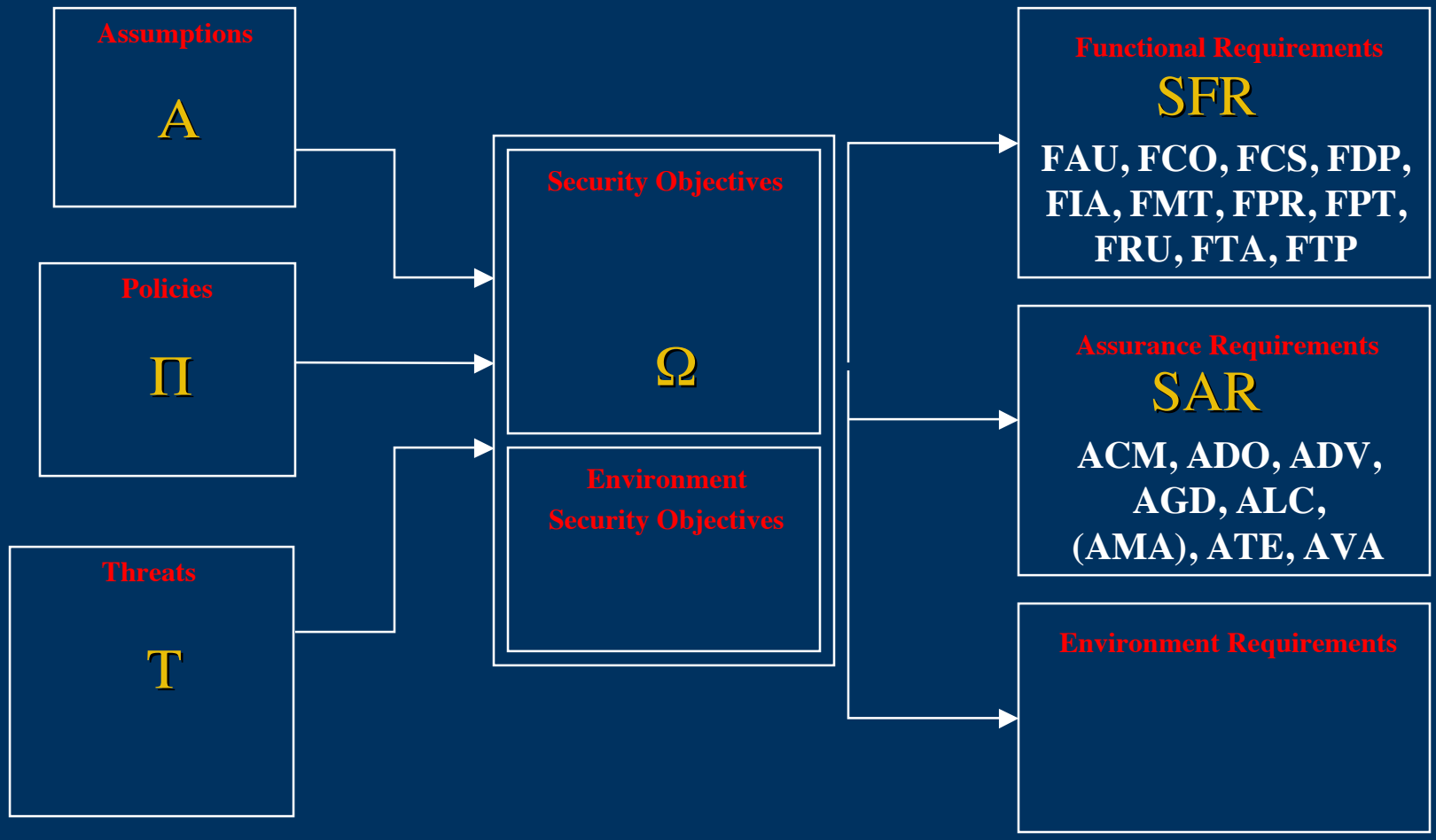
Document Publishing
Rendering & Conversion

PDF, DOCX XLSX, …

Documents & Reports

PP, ST, stats

Relational Structure of a Protection Profile

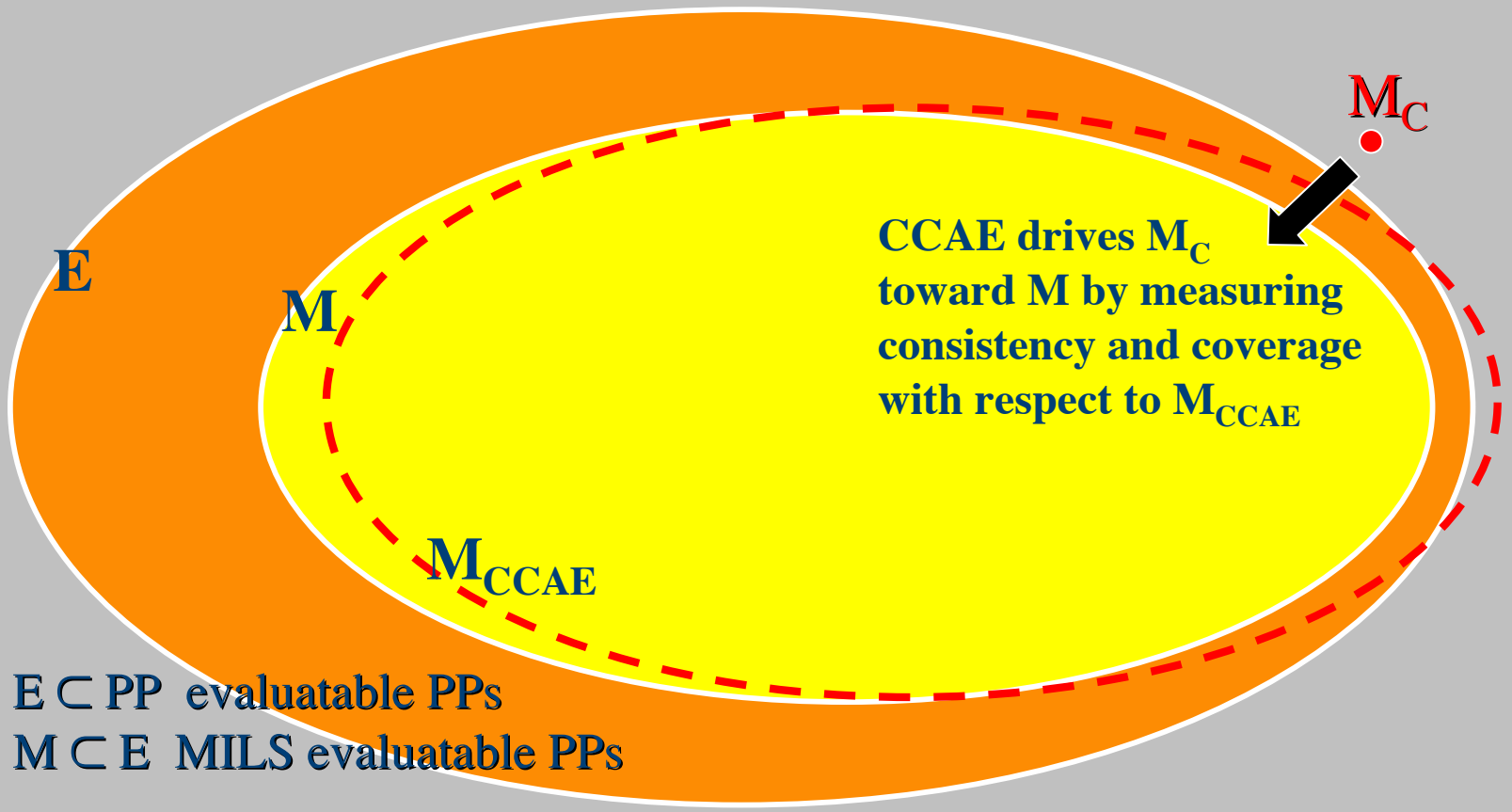


"Space" of PPs = ($2^{T} \times 2^{\Pi} \times 2^{A} \times \Omega \times 2^{SFR} \times 2^{SAR}$)

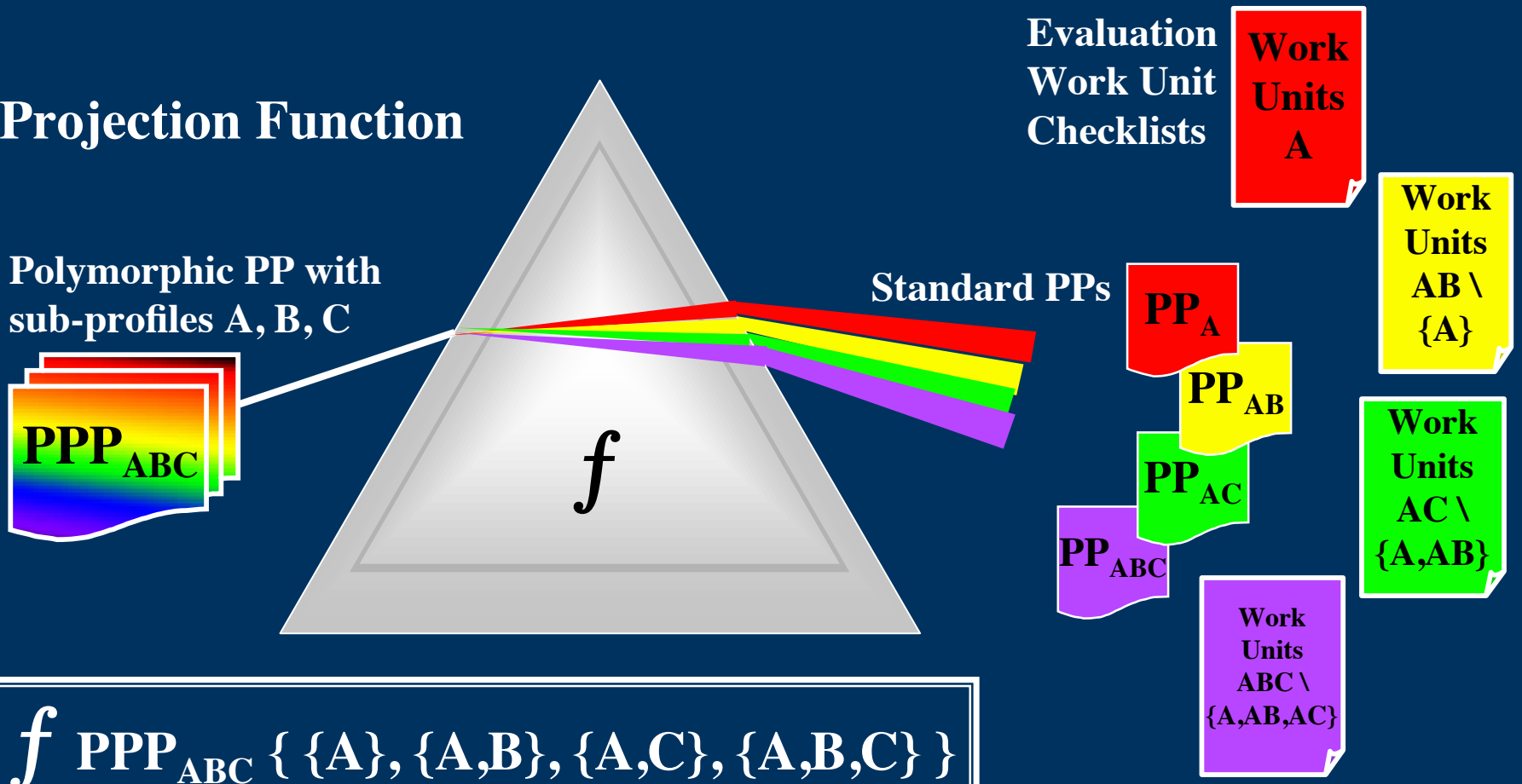
Approximation of a MILS PP Oracle (M_{CCAE})

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

M_C a candidate member of M



Projecting the MILS PPP to standard PPs



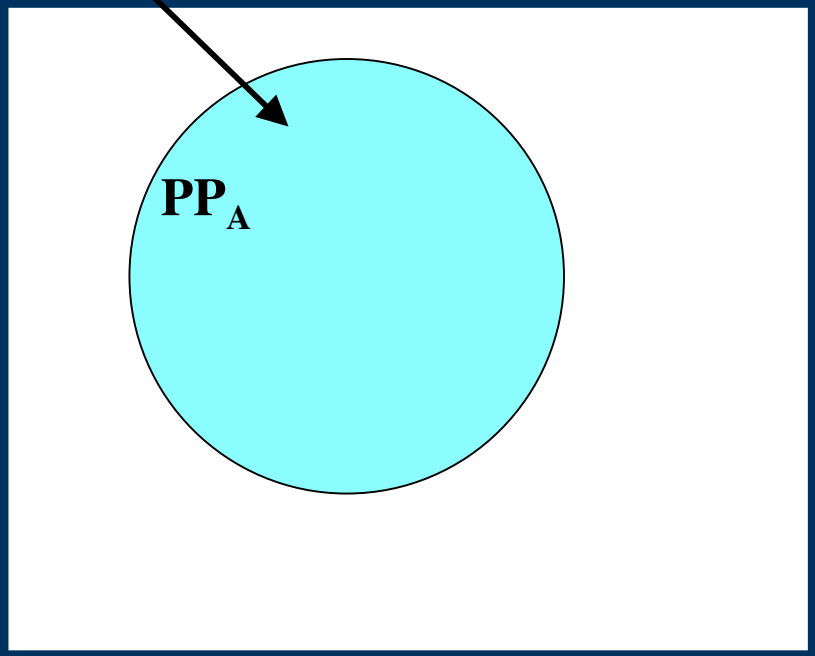
$$f\ PPP_{ABC}\ \{\{A\},\{A,B\},\{A,C\},\{A,B,C\}\} = \{PP_A,\ PP_{AB},\ PP_{AC},\ PP_{ABC}\} + \text{Evaluation Work Unit Checklists}$$

Difference operator " \ " applies comp'nt dependency, hierarchy, and other PP property closures. Differential work units assume ordered evaluation of PPs.

Evaluation differential work units (1)

Entailed work units to be performed to

evaluate f $PPP_{ABC}\{A\} = PP_A$

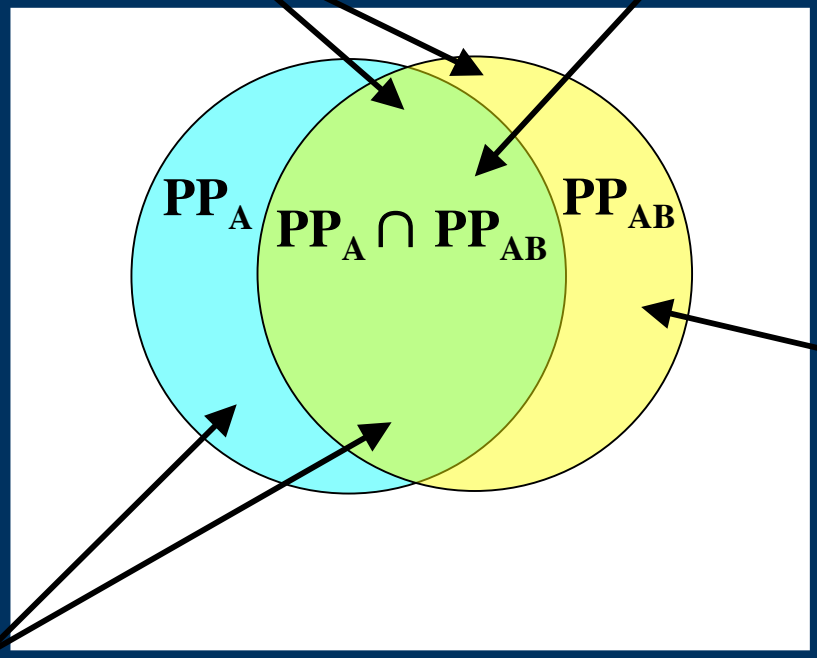


Note, the following Venn diagrams represent contents of projected PPs, not PPP sub-profiles. Projected PPs may have substantial intersection, while sub-profiles may be disjoint.

Evaluation differential work units (2)

Work units entailed to evaluate $f\ PPP_{ABC}\{A,B\} = PP_{AB}$

PP_{AB} common work units completed for evaluation of PP_A

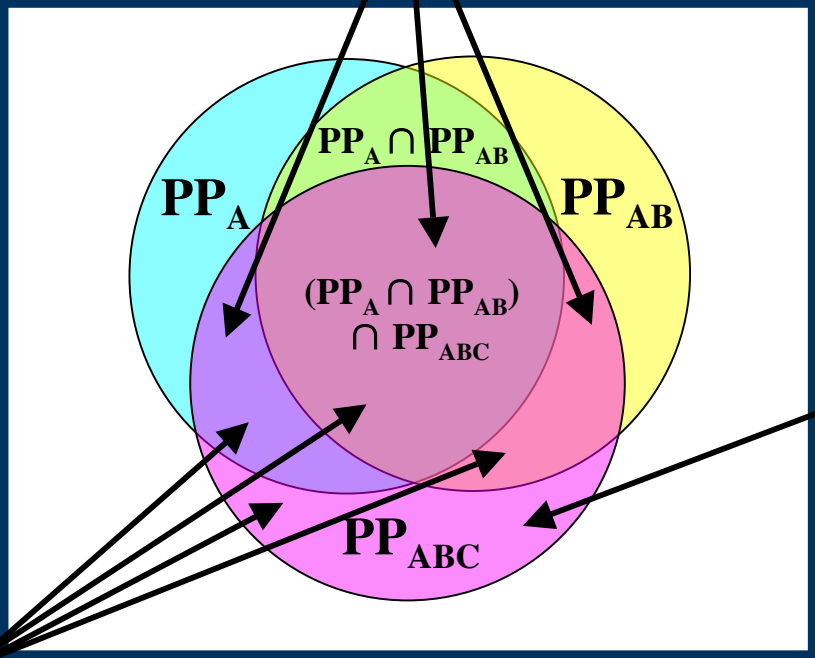


Differential work units $AB \setminus \{A\}$ to be performed to complete evaluation of PP_{AB}

Work units already completed during evaluation of PP_A

Evaluation differential work units (2)

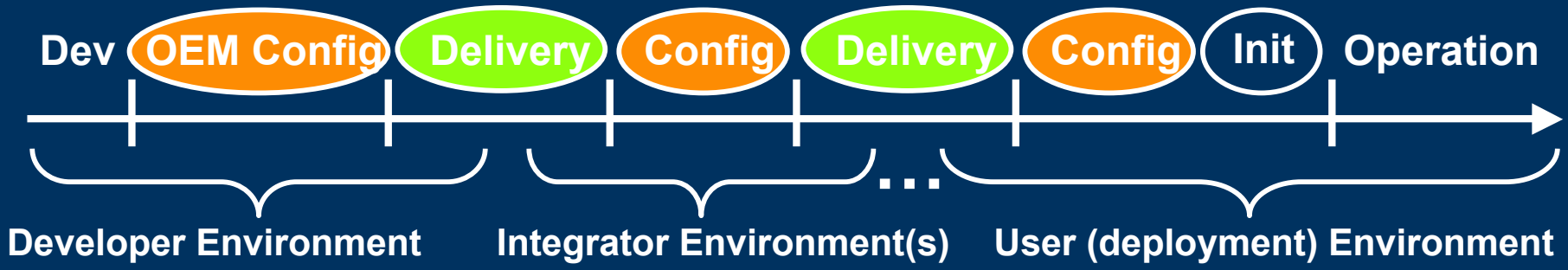
PP_{ABC} common work units completed
for evaluation of PP_A and PP_{AB}



Differential work units $ABC \setminus \{A,AB\}$ to be performed to complete evaluation of PP_{ABC}

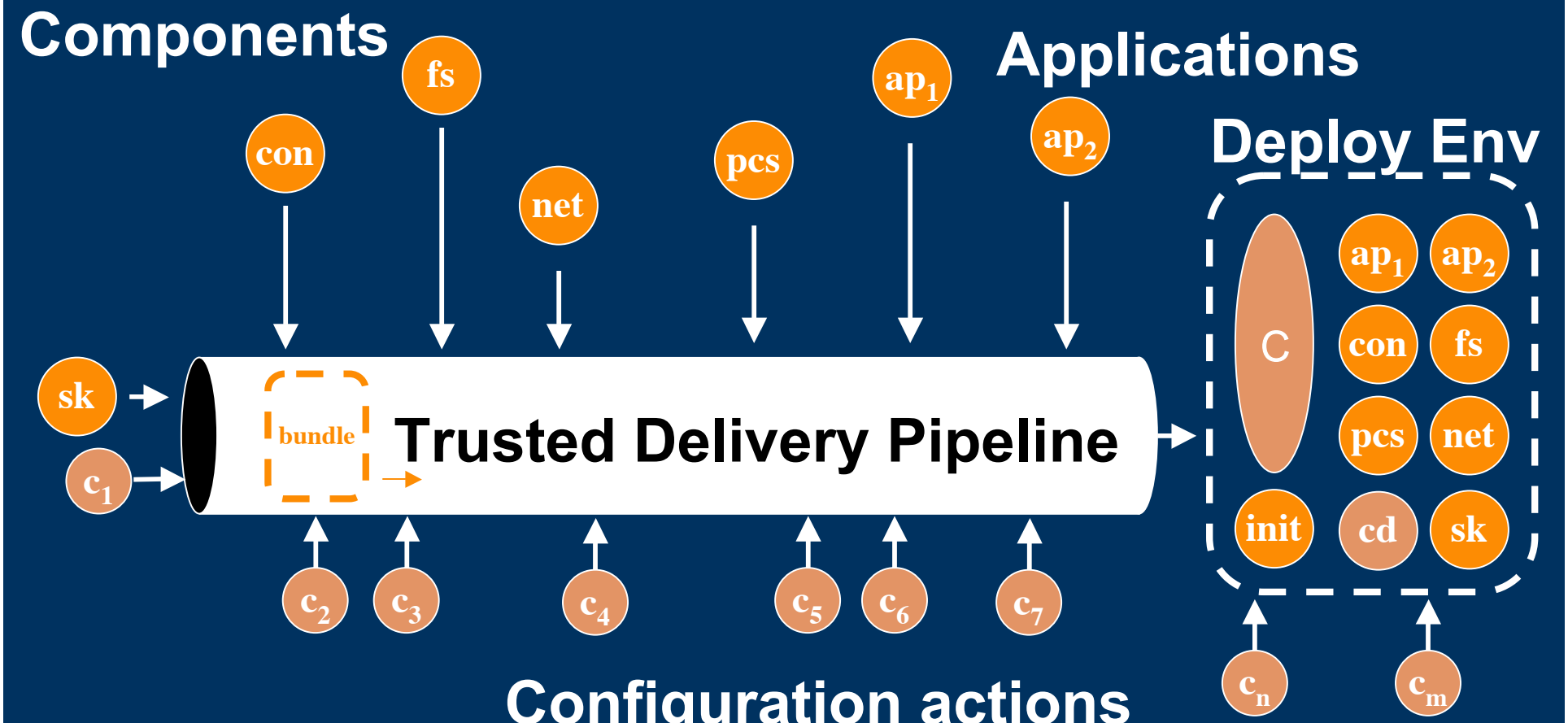
Work units entailed to evaluate f $PPP_{ABC}\{A,B,C\} = PP_{ABC}$

Generalized Delivery, Configuration, and Initialization interpretation



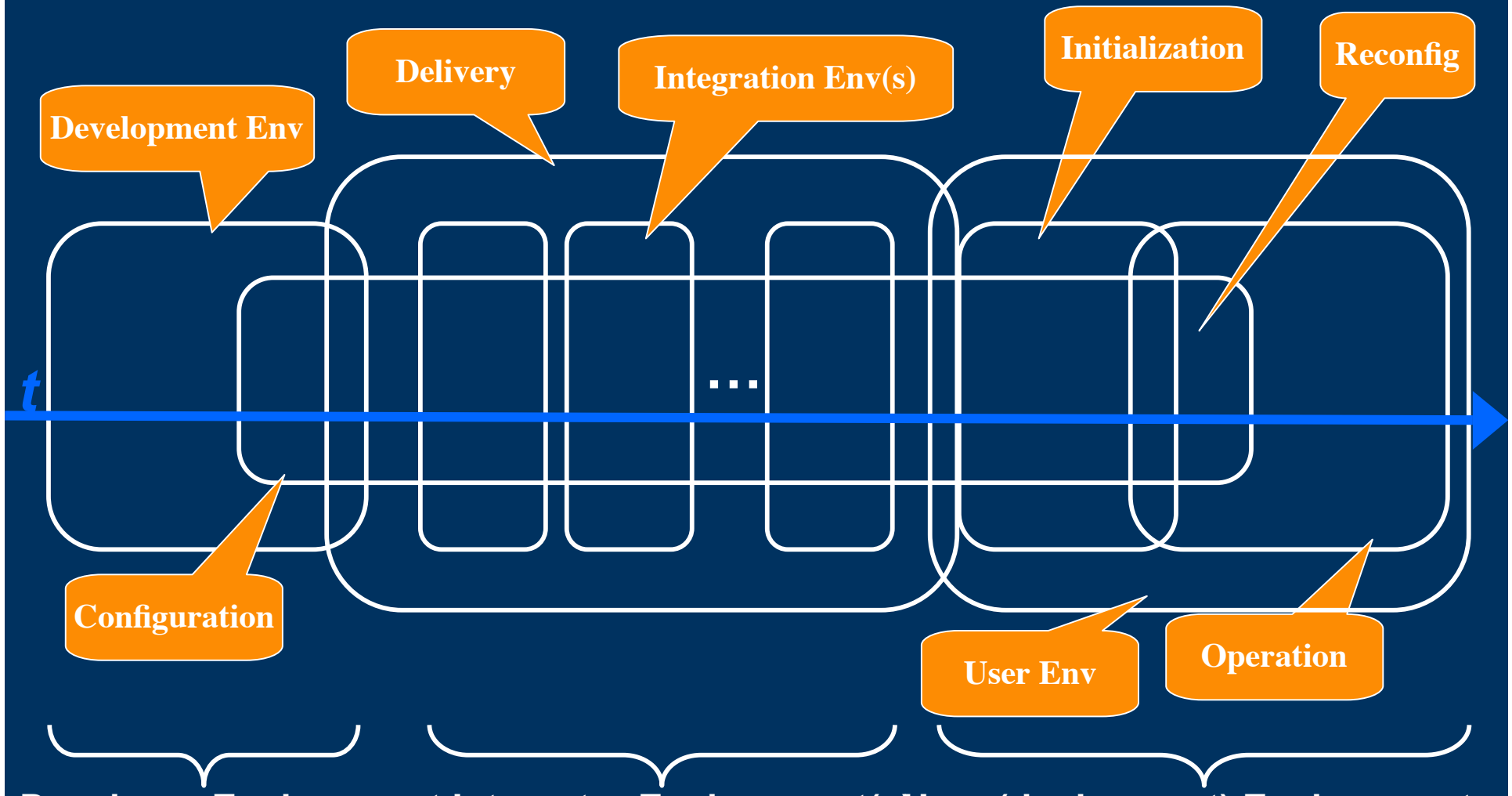
- Interleaved configuration and delivery
- Configuration and integration is ***incremental*** due to separation of concerns and separation of duty
- OEM TOE developer is responsible for providing trusted delivery and for trusted initialization
- Trusted delivery should protect TOE to the deployment environment, providing basis for establishment of secure initial state
- There can be multiple intermediate integrator environments!

Incremental accumulation of component / configuration data bundle protected by, and updated within, Trusted DCI pipeline

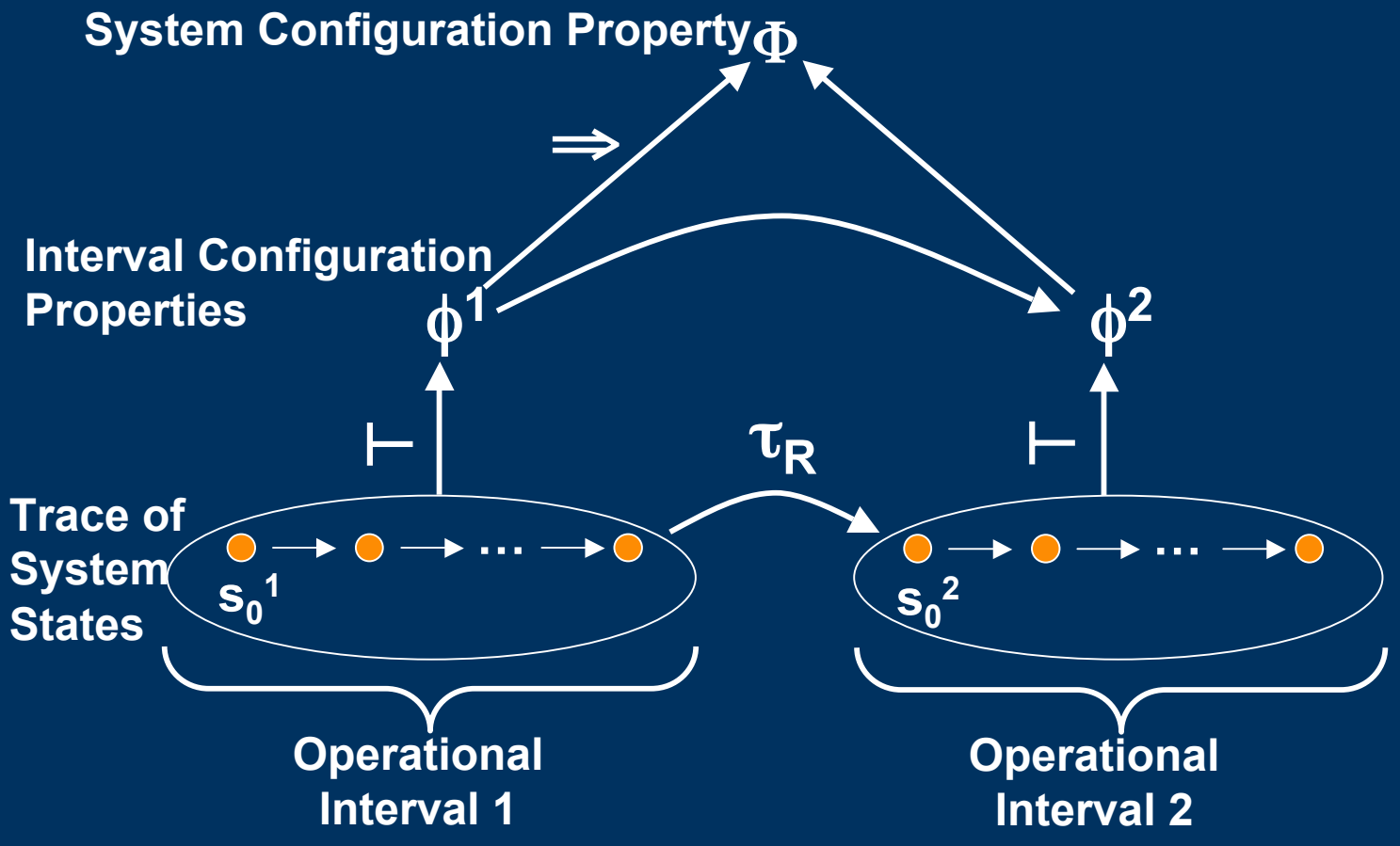


The big picture, scope of phases

Temporal overlap and location spanning



Generalized Reconfiguration



Φ - system configuration property
ϕ^i - interval configuration property
τ_R - reconfiguration transition