MILS Initiatives Within The Open Group

MILS Workshop

Amsterdam

20 January 2015

Rance J. DeLong

THE Open GROUP

Making standards work®

Topics

- ❑ MILS, MILS Initiative, and Mils™
- ❑ Abbreviated Overview of MILS concepts
- ❑ Mils™ Corpus
- ❑ Mils™ Evaluation and Certification Support Scheme
- ❑ Mils™ API for Assured Subjects
- ❑ Mils™ Development Environment

MILS, MILS Initiative, and Mils™*

- "MILS" – initially an acronym for "Multiple Independent Levels of Security". Its usage has referred primarily to the concept of strong partitioning on a single platform, such as that provided by a separation kernel.
- "MILS Initiative" – a community of vendors, system integrators, research sponsors, researchers, educators and customers pursuing the "MILS idea" for over a decade. This Initiative, having its nexus within The Open Group, has yielded a collection of concepts, notions, beliefs, products, research results, and documentation that comprise the ***Reservoir of MILS.***
- To facilitate achievement of the long-standing MILS objectives The Open Group RTES Forum seeks to establish a coherent and unifying set of standards under the name "Mils".
- **"Mils™"** – Now used as a proper noun, rather than an acronym, Mils™ refers to a refined** set of standards for the concepts, terminology, architecture, doctrine, practices and support for the development, evaluation, certification and deployment of Mils™ components and systems, that will achieve the objectives long held for "MILS".

*** Mils™ is a trademark of The Open Group** **** and continuing to be refined**

Abbreviated Overview of MILS and “Modern MILS” Concepts

1981 - 2012

What is MILS?

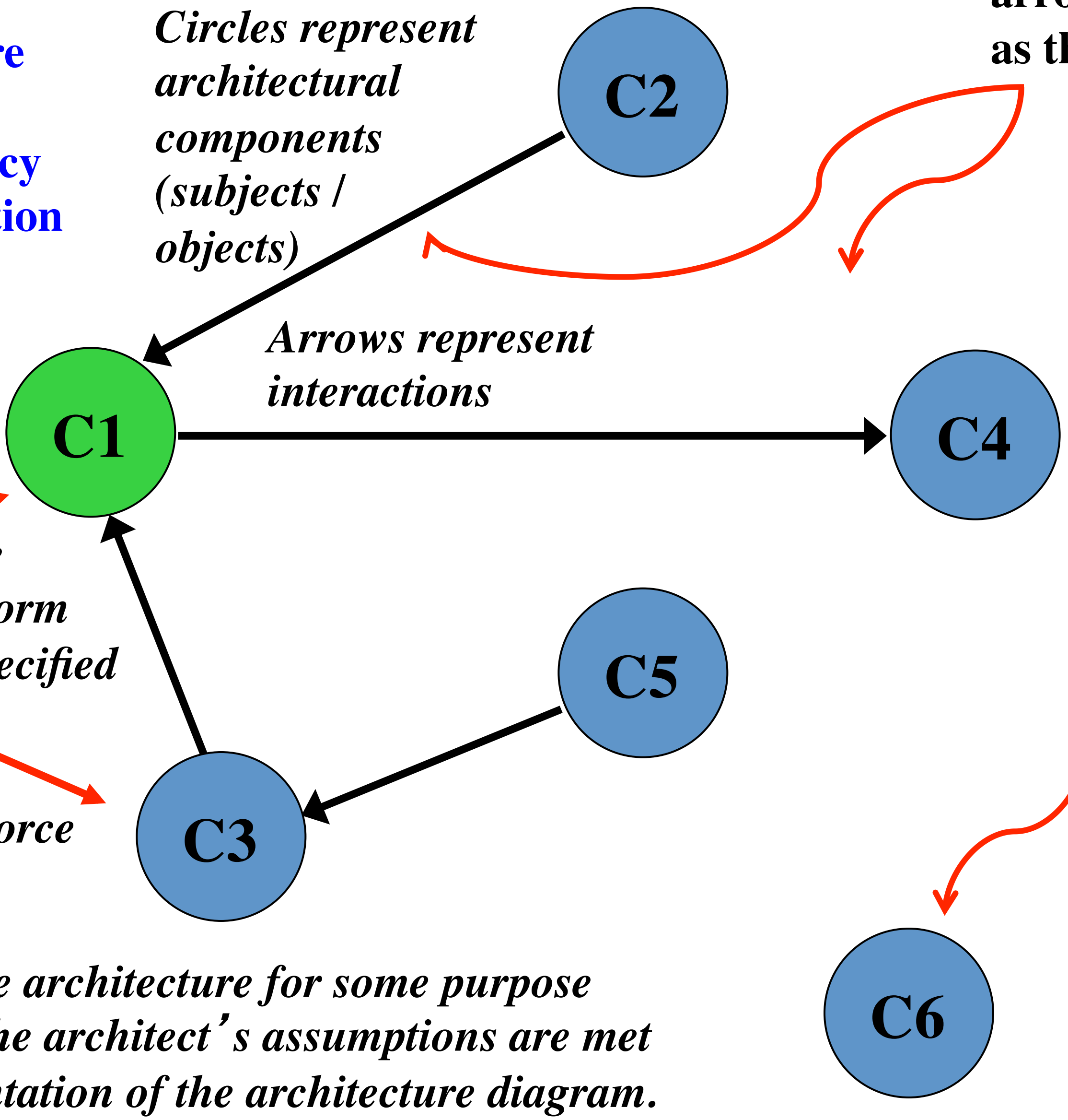
- MILS is a component-based approach to secure systems design and implementation that encourages a marketplace of general-purpose COTS components
- MILS can be understood as a two phase approach:
  - Design a Policy Architecture
    - Abstract architecture diagram represented by "boxes and arrows"
    - Operational components and architecture achieve system purpose
    - Assumes architecture (components and connectors) strictly enforced
  - Implement on a robust resource-sharing platform
    - MILS foundational components share physical resources, creating strongly separated "exported resources"
    - Individually developed and assured according to standardized specifications
    - Compose "additively" to form a distributed trusted sharing substrate, the MILS Platform
- Provides compositional approach to construction, assurance, and system certification

MILS Policy Architecture

The architecture expresses an interaction policy among a collection of components

Circles represent architectural components (subjects / objects)

The *absence* of an arrow *is as significant* as the *presence* of one



Arrows represent interactions

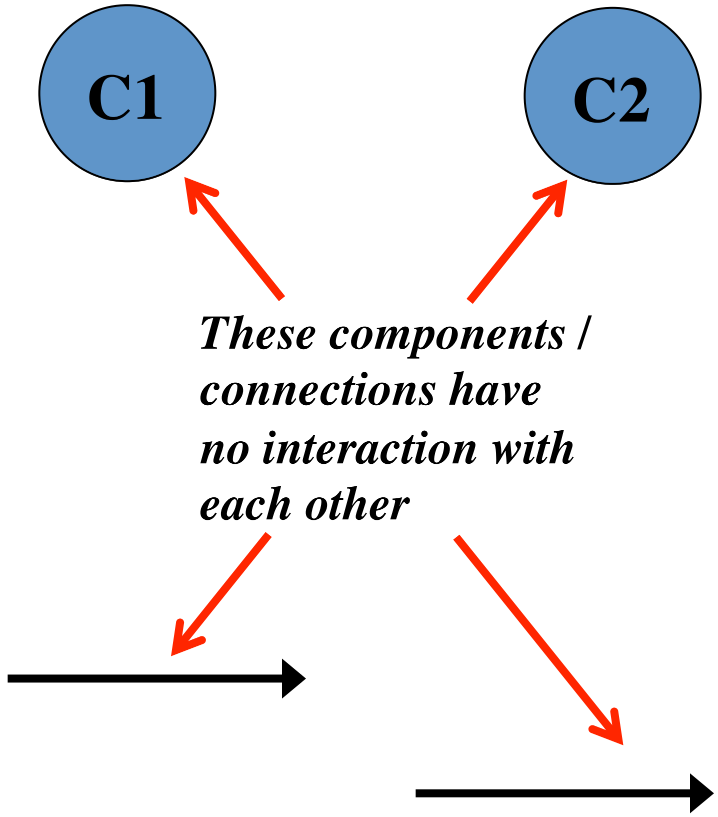
Components are assumed to perform the functions specified by the architect (trusted components enforce a local policy)

This component has *no interaction* with any other

Suitability of the architecture for some purpose presumes that the architect's assumptions are met in the implementation of the architecture diagram.

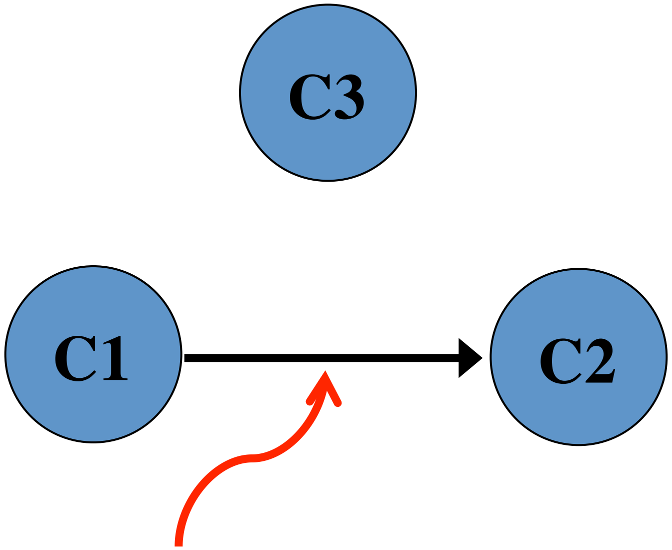
Assumptions Implicit in the Architecture Represent Two Primitive Policies

1. Isolation



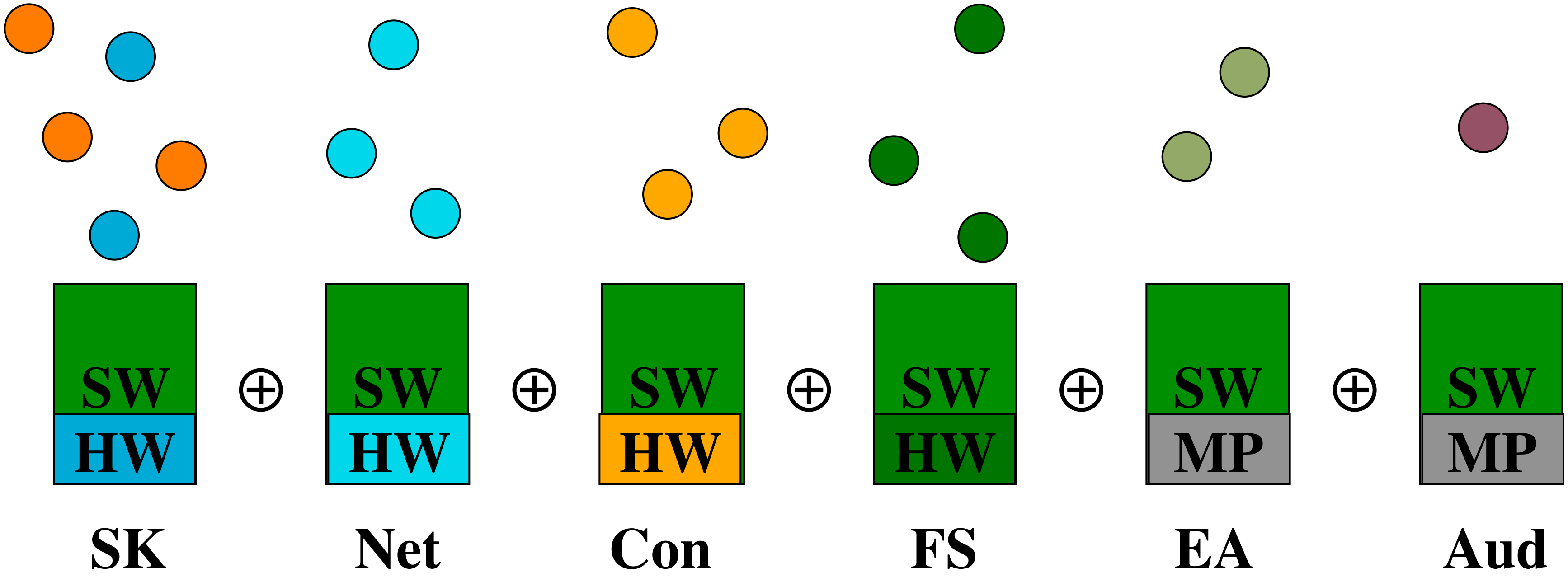
These components / connections have no interaction with each other

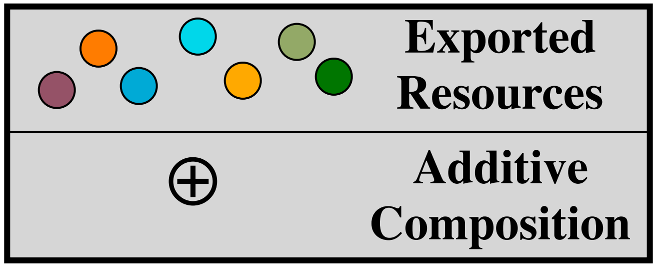
2. Information Flow Control



Only *explicitly permitted* causality, or *interference*, is permitted. The architecture *permits* this flow. Only C1 or C2 can *cause* the flow, not C3. The flow is directional and intransitive.

The MILS Platform: a Composition of Foundational (resource-sharing) Components

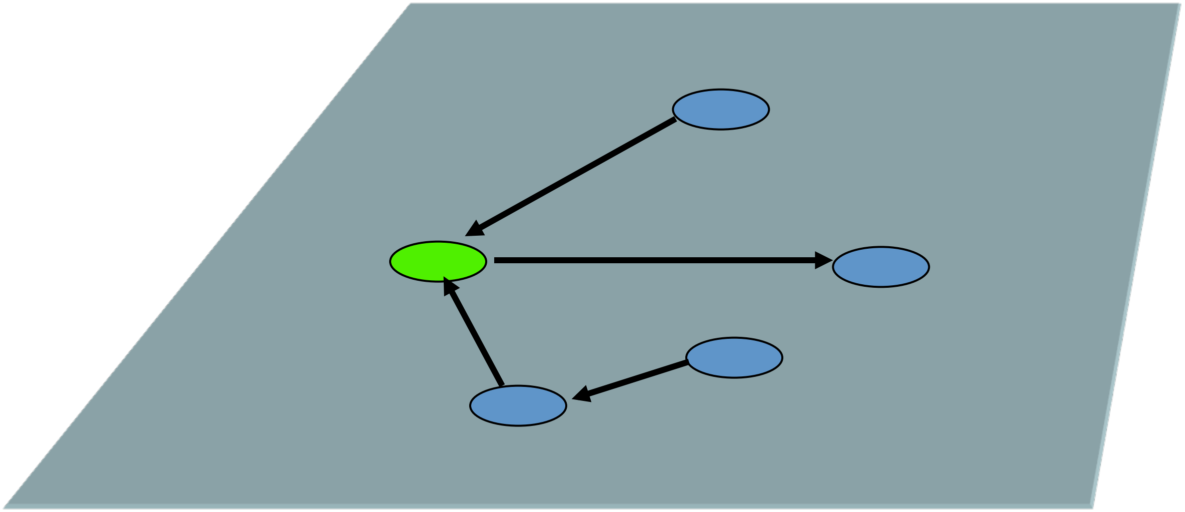




additive compositionality – e.g., a Partitioning Kernel ⊕ Partitioning Net
= Partitioning (Kernel + Net)
MP = MILS Platform

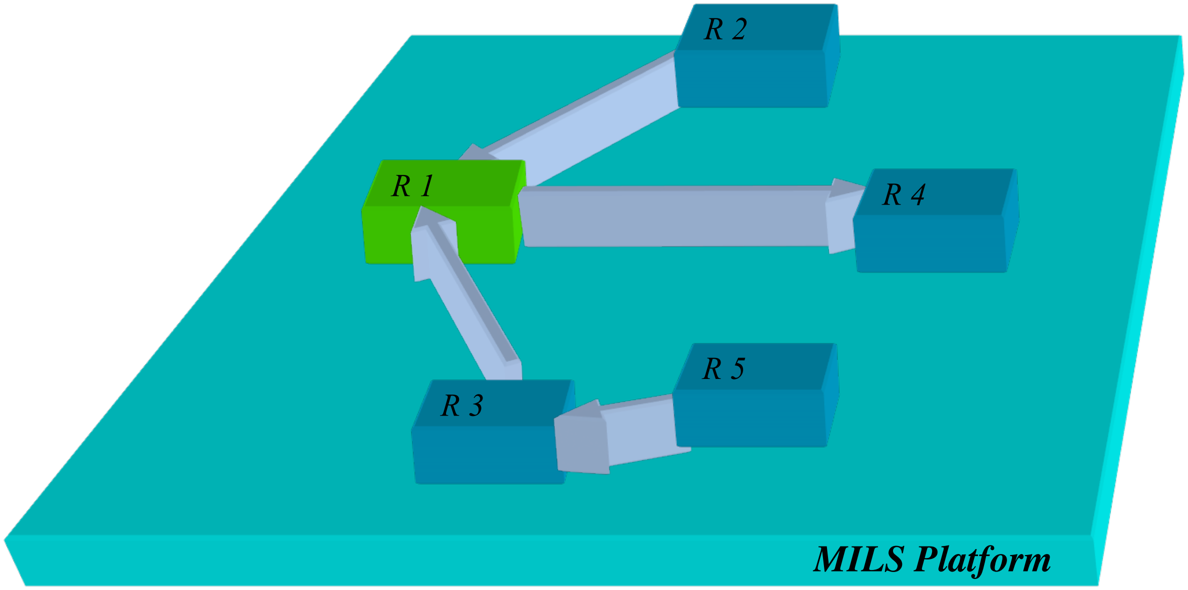
MP – MILS Platform

MILS Platform – Provides Straightforward Realization of Policy Architecture



Architecture

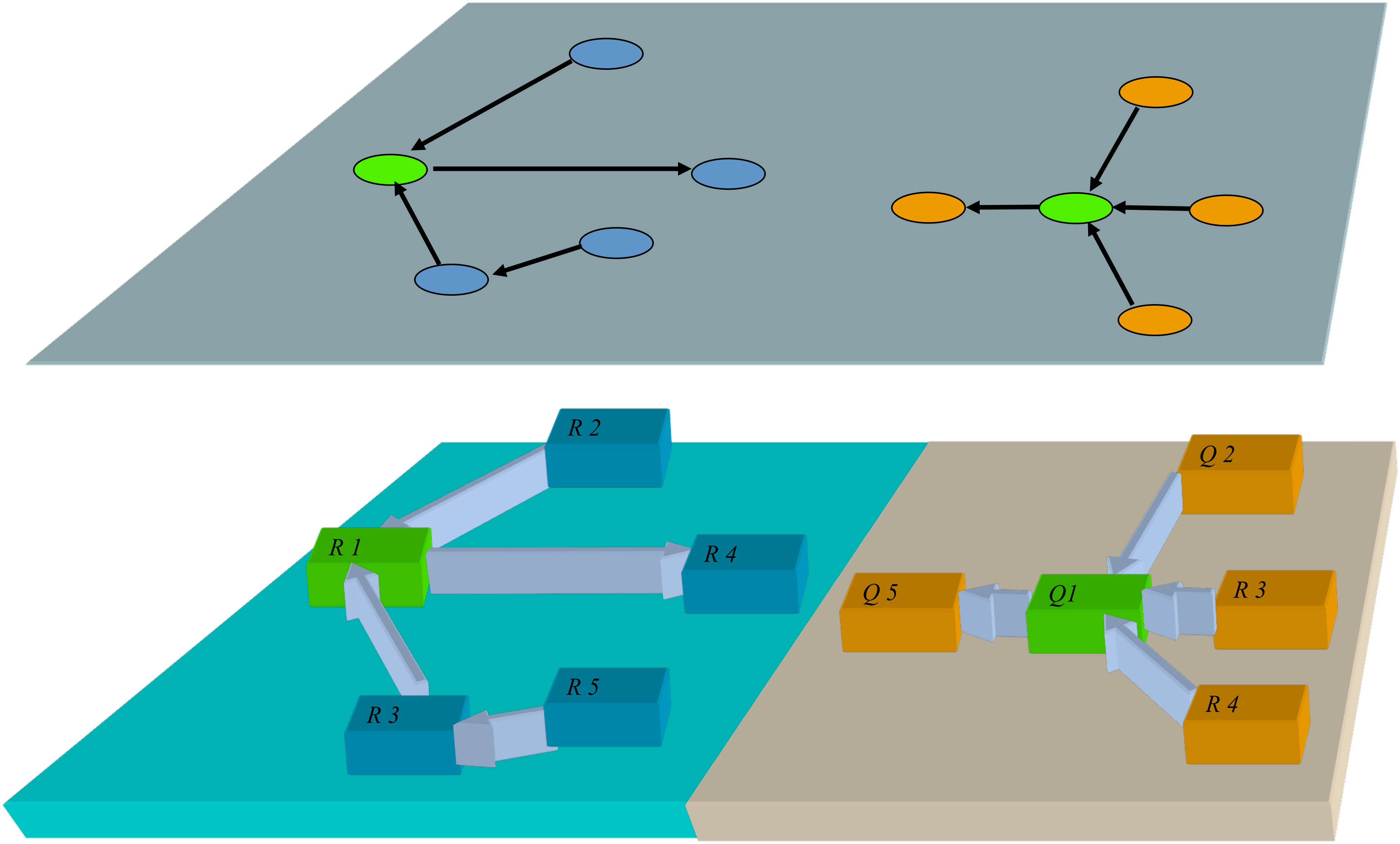
Validity of the architecture assumes that the *only* interactions of the circles (operational components) is through the arrows depicted in the diagram



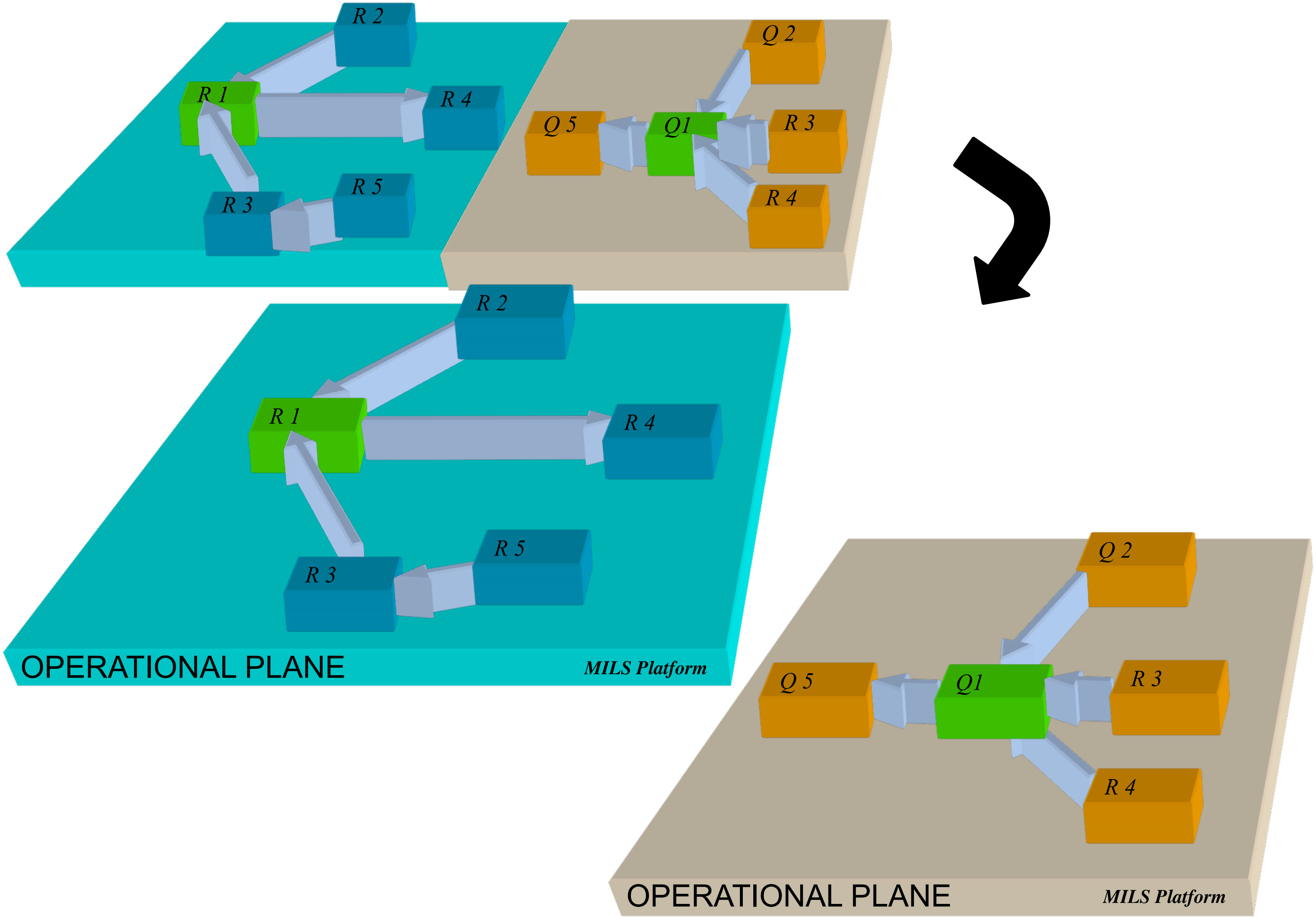
Realization

SK, with other MILS foundational components, form the *MILS Platform* allowing operational components to share physical resources while enforcing Isolation and Information Flow Control

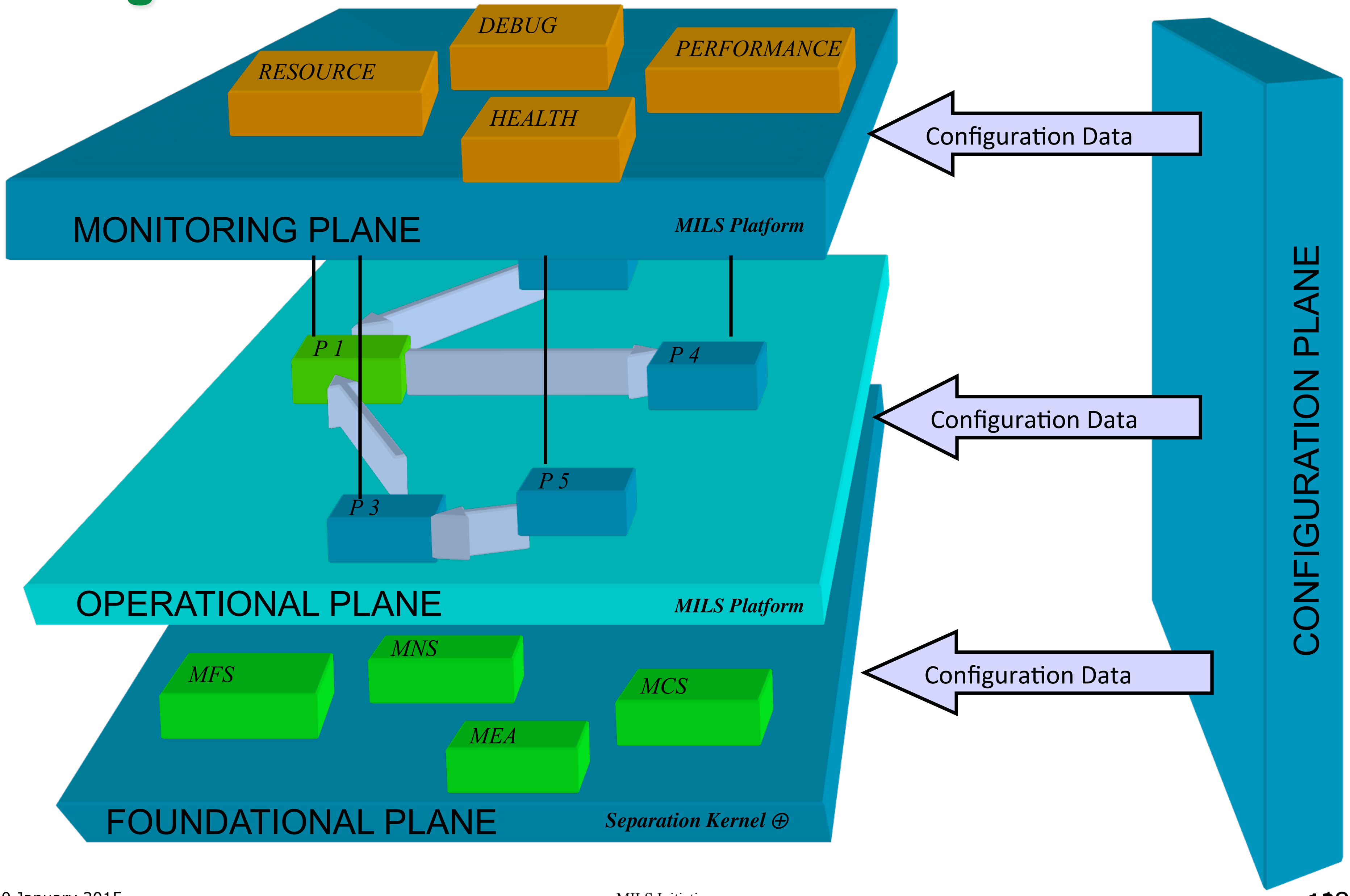
Policy Architecture with Isolated Subsystems



Isolated Subsystems in Distinct "Operational" Planes



MILS Foundational, Operational, Monitoring, and Configuration Planes



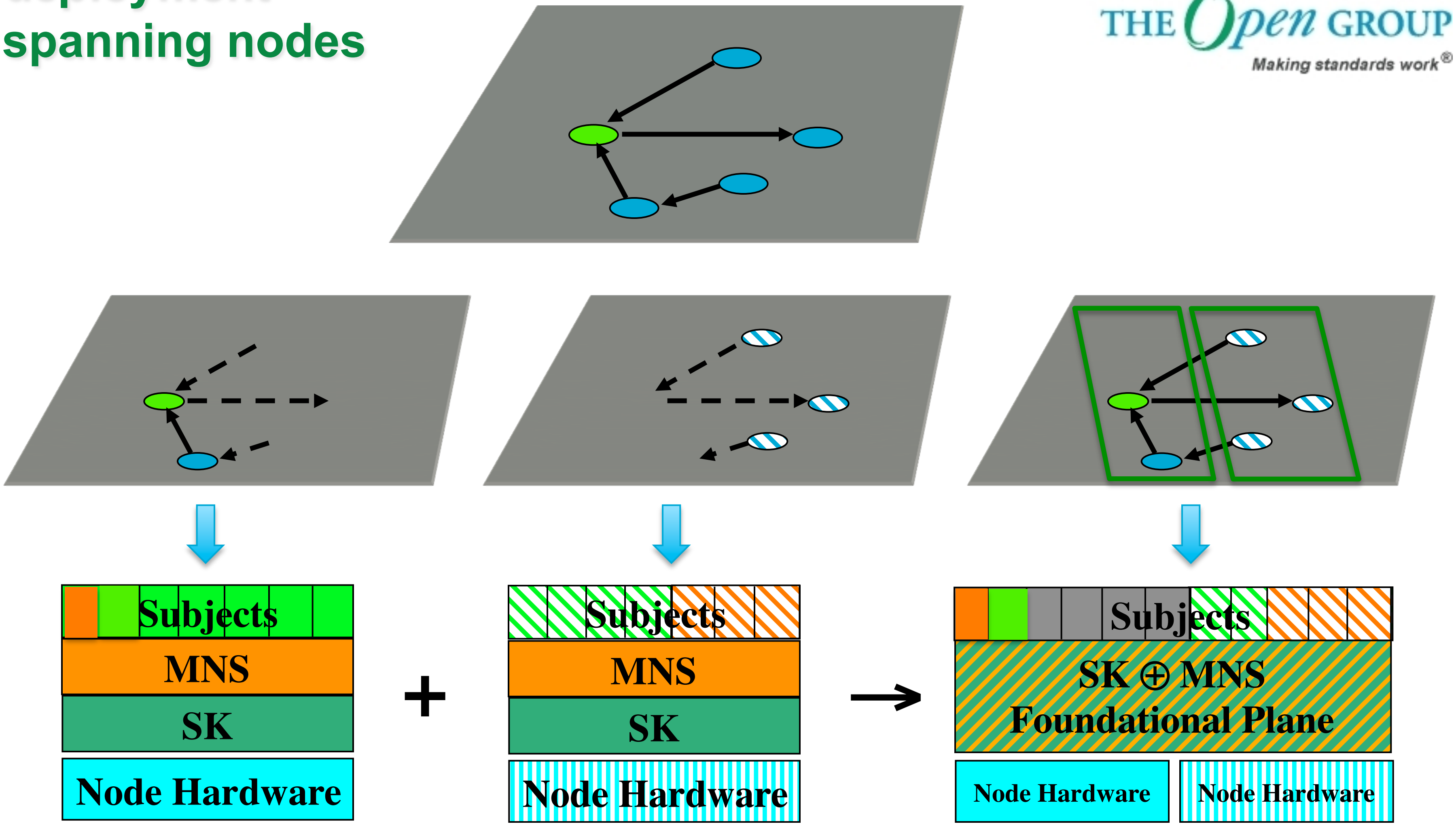
Distributed MILS: Policy architecture deployment spanning nodes

European Commission FP7
ICT-2011.1.4 Trustworthy ICT
Project #318772
2012 – 2015

SEVENTH FRAMEWORK PROGRAMME

D-MILS

THE Open GROUP
Making standards work®



Subjects
MNS
SK
Node Hardware

+

Subjects
MNS
SK
Node Hardware

→

Subjects
SK ⊕ MNS
Foundational Plane
Node Hardware
Node Hardware

MILS Platform Objectives

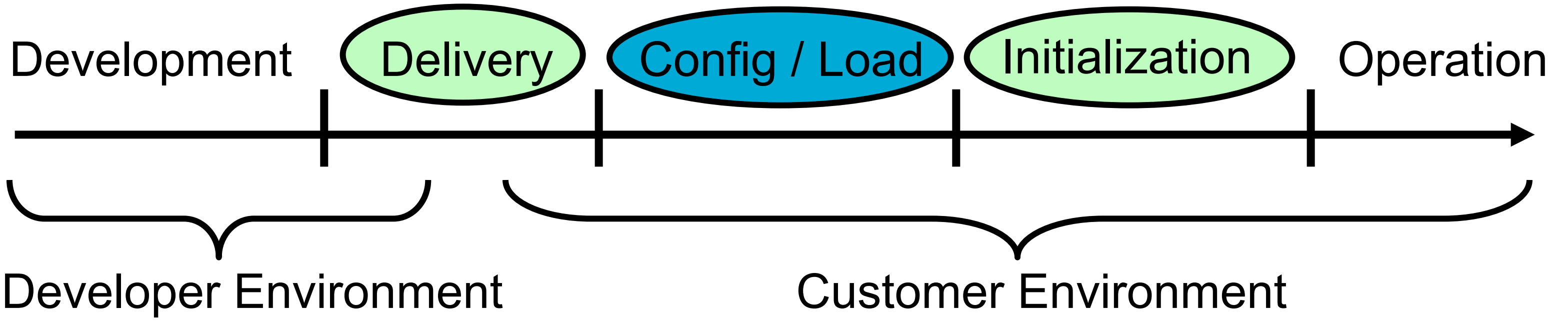
- MILS Platform – a standardized, component-based high-assurance platform
- Predictable behavior, security, safety and performance
- Improved dependability at reduced cost
- Maintainable assurance at reduced cost
- Firm guarantees provided to the application-level policy architecture
- Compositional assurance of systems based on component assurance and composition analysis
- Framework for construction and certification of critical systems built on the MILS platform supported by automated tools and processes
- Distributed and Dynamic MILS
- Interoperable foundational components
- Supported by trusted Delivery, Configuration, and Initialization

Security functions and security-relevant functions

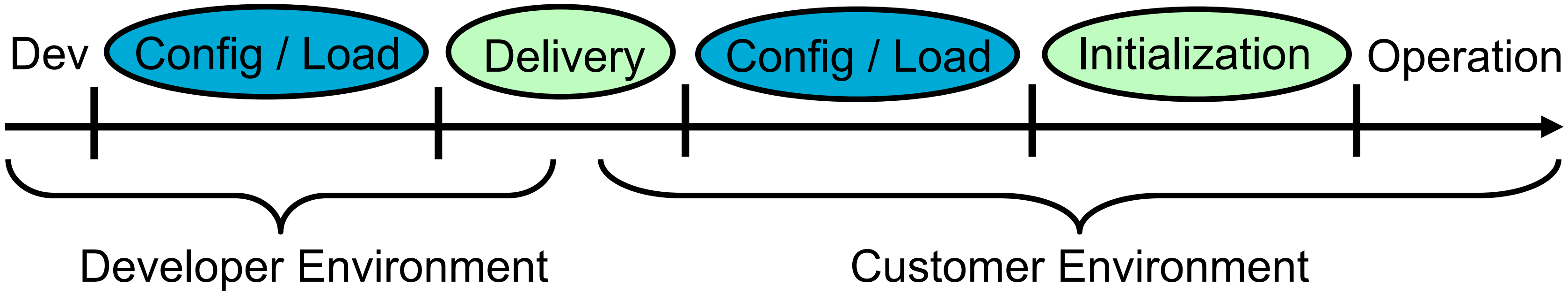
- MILS foundational component security functions at execution time
  - Resource sharing
  - Isolation and information flow control
- Pre-execution time security-relevant functions
  - Delivery
  - Configuration
  - (Load)
  - Initialization
- May be pre-execution *and* execution-time
  - Configuration (dynamic reconfiguration)
  - (Load)
  - Initialization (dynamic reconfiguration)
- Trusted Delivery, Configuration, and Initialization - “DCI”

Simple DCI

- The TOE developer employs *trusted delivery* to get the product from the developer (vendor) to the customer
- The developer and/or the customer performs the *configuration/load* in their respective environments
- *Initialization* occurs in the customer environment
- E.g., sequential delivery, config/load, initialization



Shortcomings of simple DCI



Dev

Config / Load

Delivery

Config / Load

Initialization

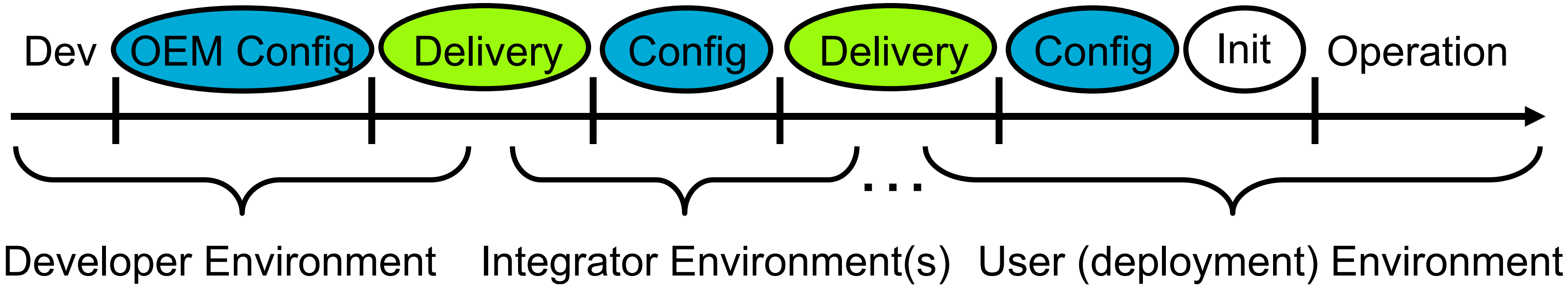
Operation

Developer Environment

Customer Environment

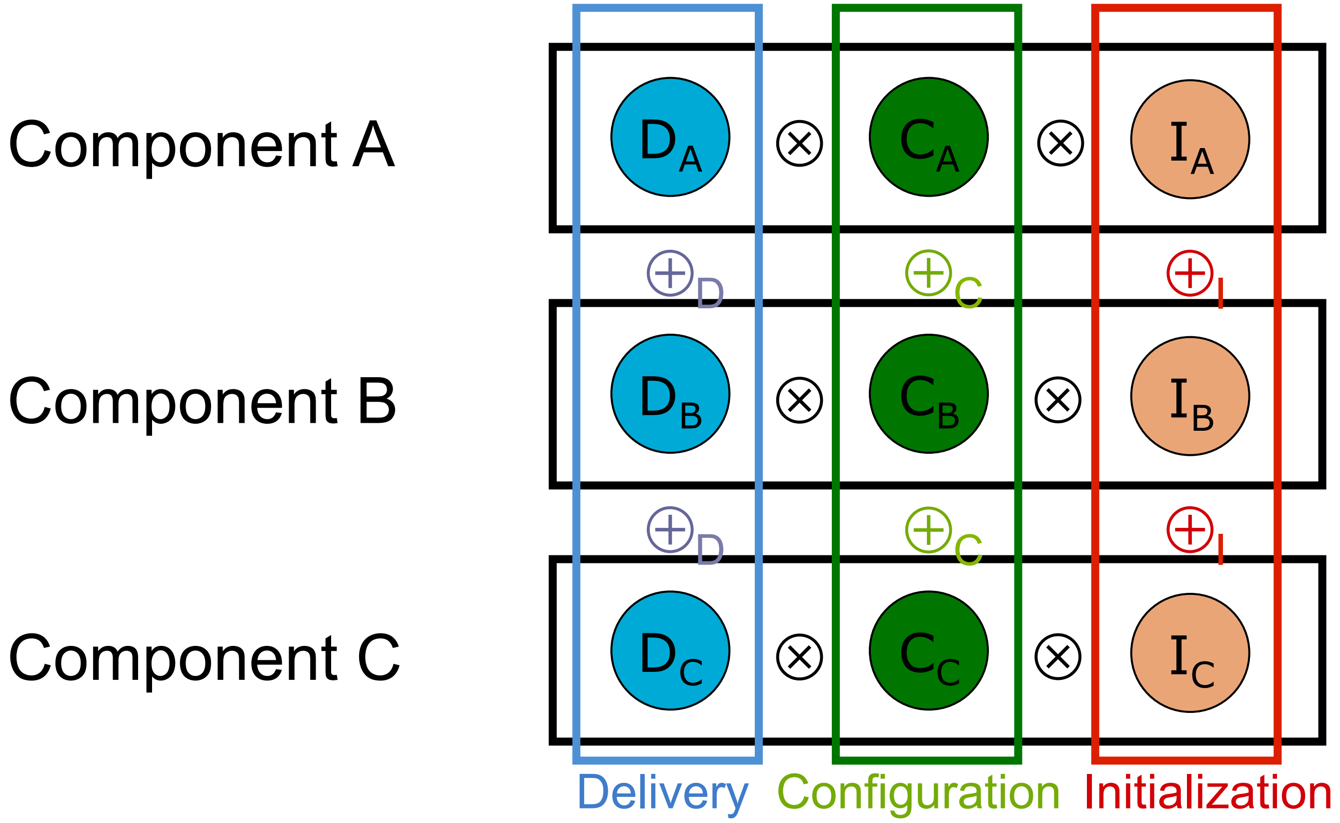
- Developer may need to do some configuration
  - Configuration in developer environment and is protected by delivery
  - Other configuration occurs in customer environment
  - Therefore, configuration is incremental
- "Customer" may not be the "end user"
  - System integrator combines components and provides applications
  - Performs configuration of integrated components and applications
- End user environment different from integrator environment
  - Requires trusted delivery (again, or ***still***)
  - Final configuration, initialization, and operation
- Does not account for component configuration composition

Generalized DCI



- Appears to be 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!

Composition of DCI Functions



Component A $D_A \otimes C_A \otimes I_A$

$\oplus_D$ $\oplus_C$ $\oplus_I$

Component B $D_B \otimes C_B \otimes I_B$

$\oplus_D$ $\oplus_C$ $\oplus_I$

Component C $D_C \otimes C_C \otimes I_C$

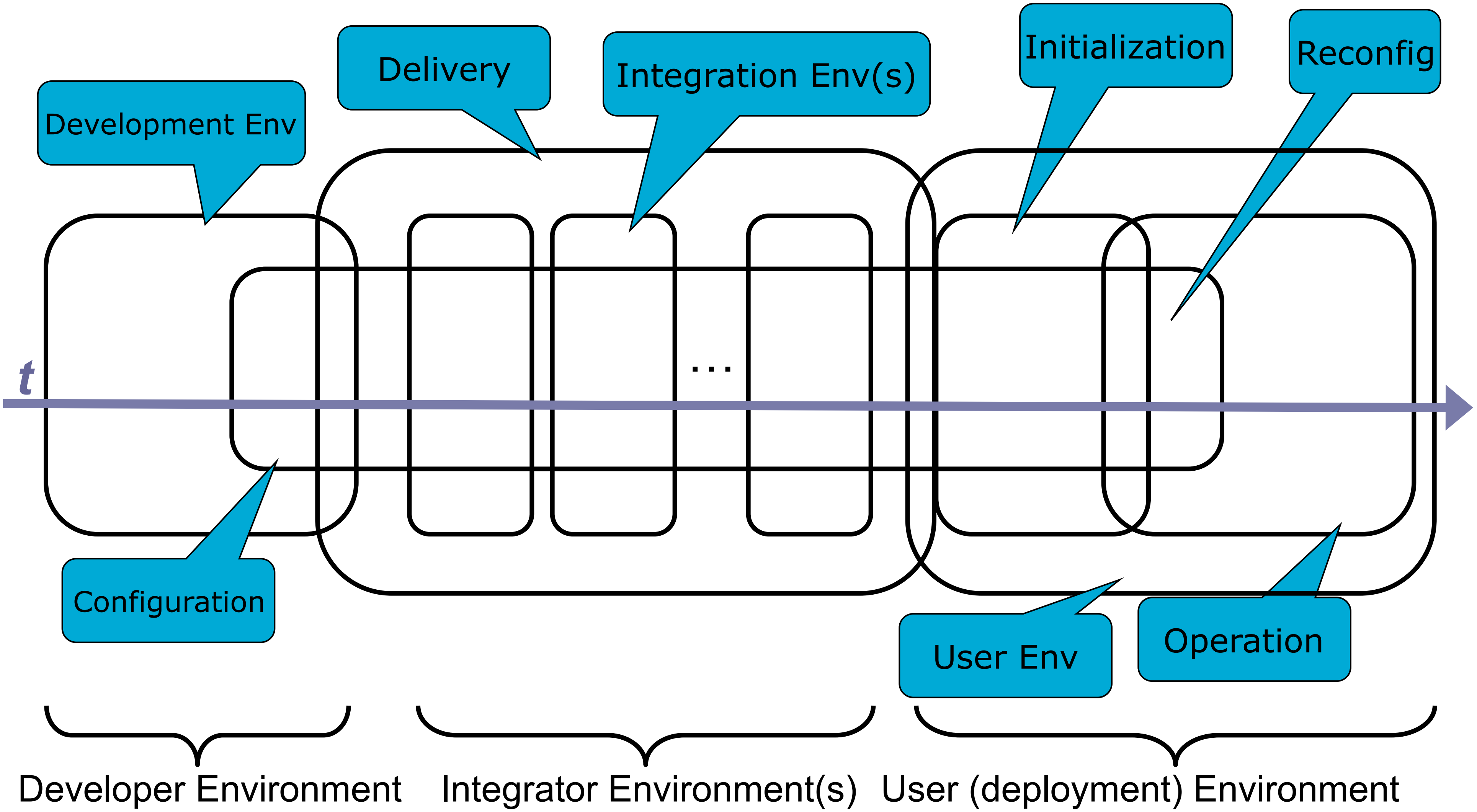
Delivery Configuration Initialization

$\oplus_f$ Composition of like functions

$\otimes$ Composition of diverse functions

The big picture, scope of phases

Temporal overlap and location spanning



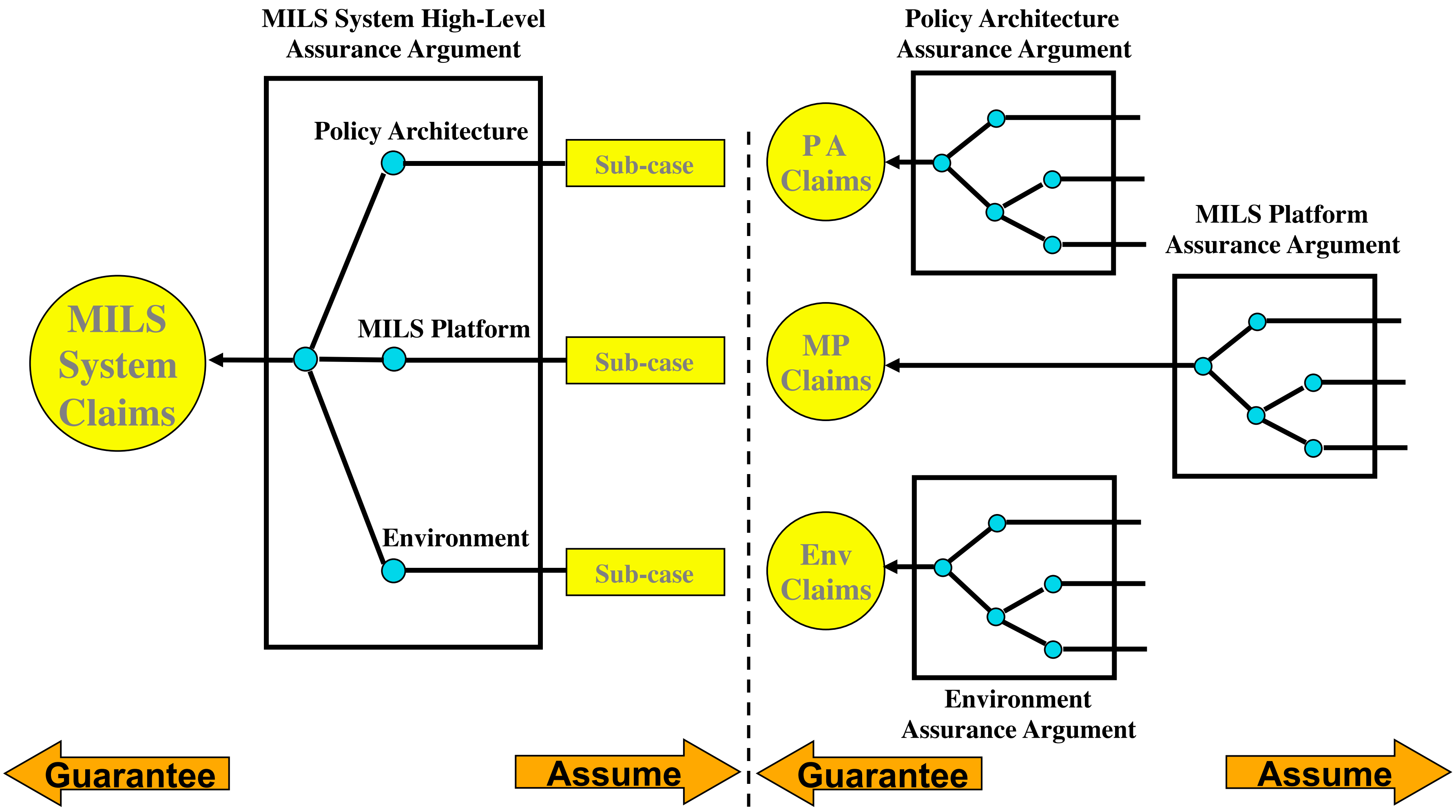
Dynamic Reconfiguration

- Changes to system configuration after transition from initialization to operational state
- May leave a portion of the system configuration unaffected by the configuration change
- Can be a natural development from one-time static configuration
- Requires some of the state construction to be moved from offline to online
- Requires application of constraints to changes

➔ ***Dynamic* MILS** !

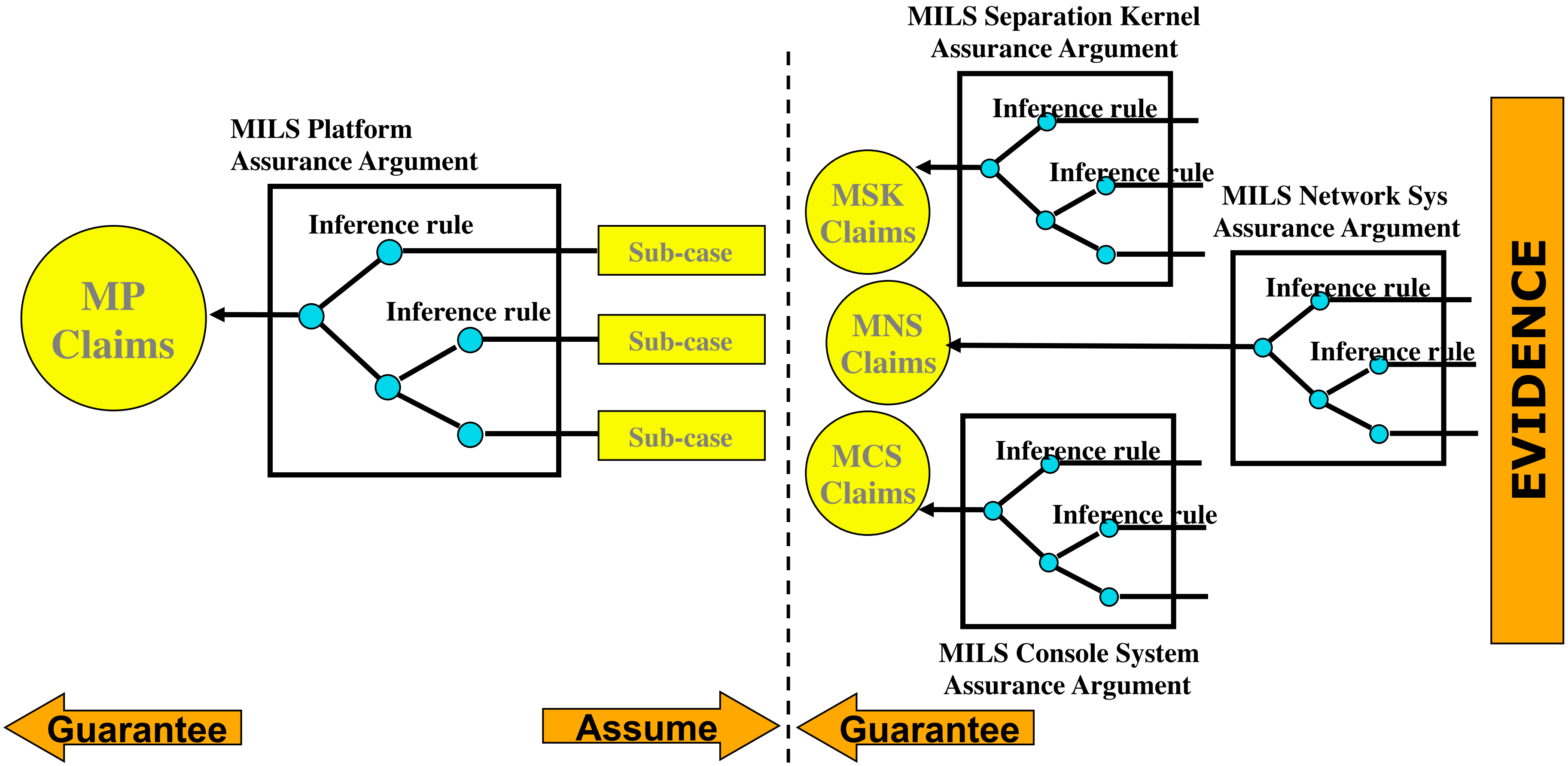
MILS System Assurance Case

- Compose assurance cases using Assume-Guarantee Reasoning
- MILS System assurance requires the validity of three sub-cases
- Assumptions from MILS System assurance case become obligations on the sub-cases

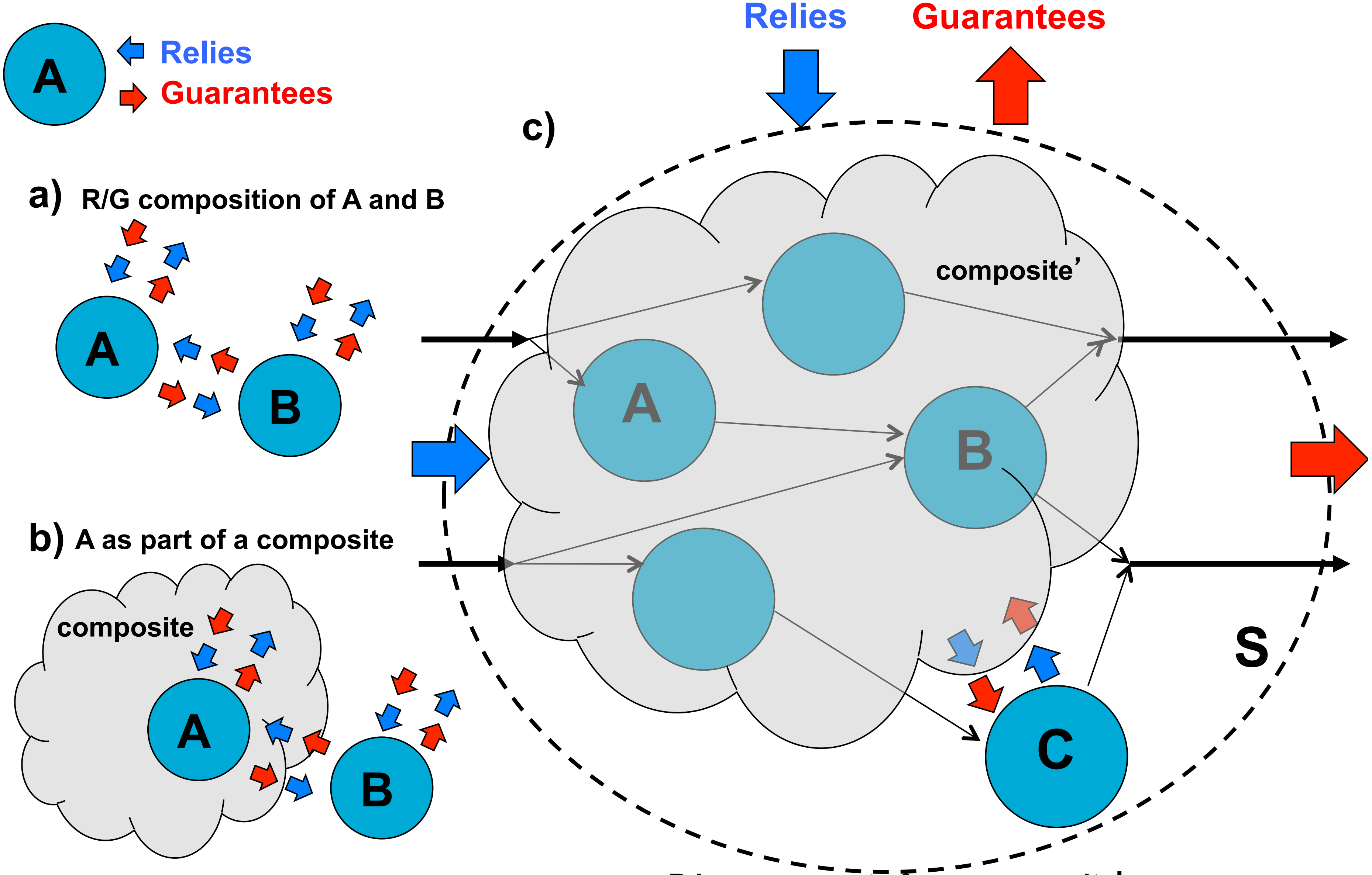


MILS Platform Assurance Case

- The MILS Platform is composed of the MILS foundational components (only 3 shown here)
- Assumptions from MILS Platform assurance case become obligations on the components
- Assured Claims from component assurance cases become evidence for MIPP sub-cases
- Evidence provides the ultimate justification for the assurance case



Policy Architecture Assurance – Incremental Rely/Guarantee Compositional Reasoning



B becomes part of new composite' which is then composed with C to form S

Mils™ Corpus

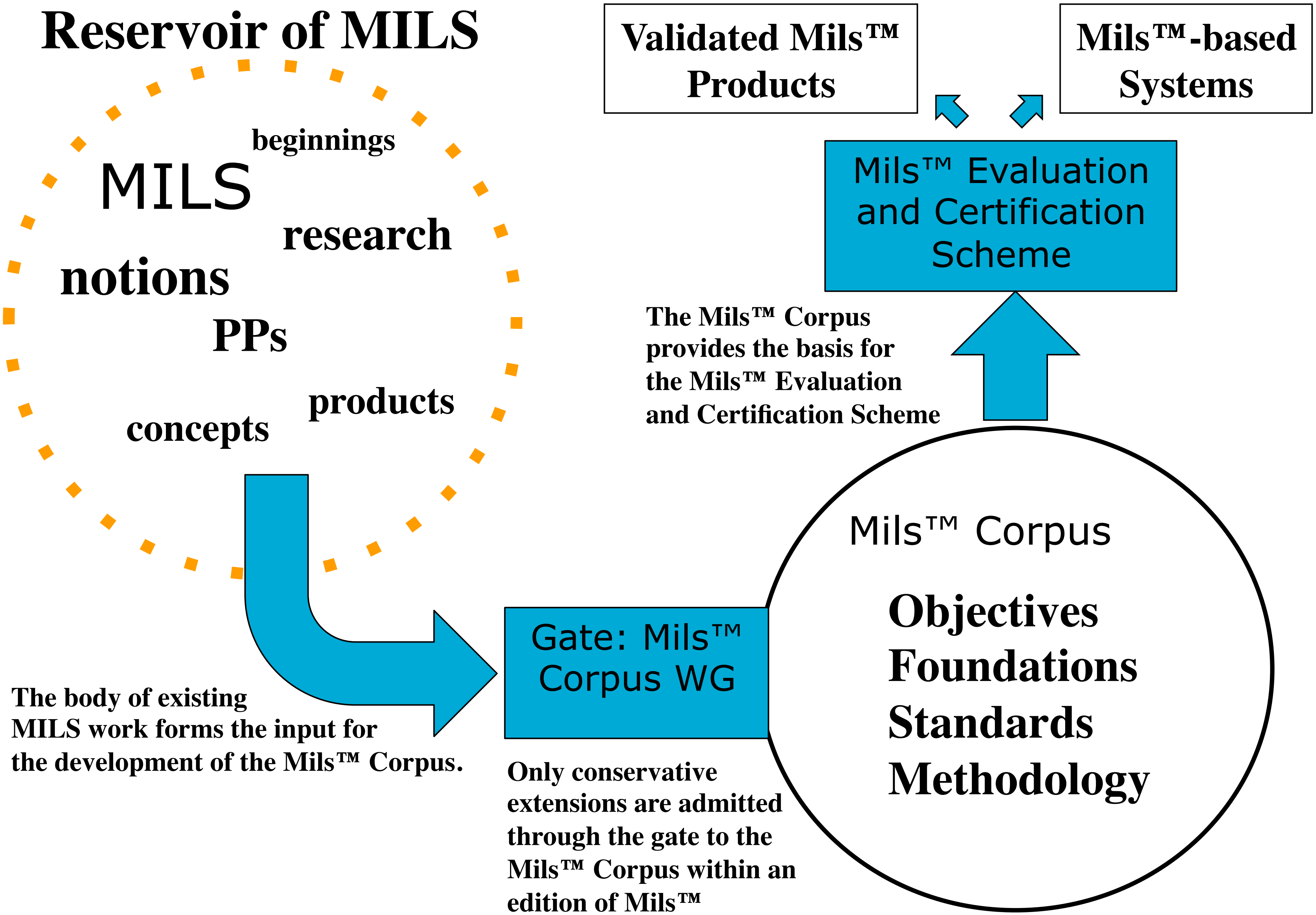
Why Mils™ ?

- To enable achievement the earliest goals of MILS Initiative (vendors, integrators, system owners), viz.,
  - "A marketplace of interoperable and substitutable commercial (COTS) high-assurance MILS components"
- Can't be achieved without strict standards
- And a means of demonstrating compliance

Mils™ Corpus

- Several years ago, the RTES forum moved to trademark the name Mils™
- At the 2012 SF meeting of the RTES Forum, the attendees provisionally approved the formation of a Mils™ governance working group
- The working group would have the responsibility of constructing the set of Mils™ standards
  - Consistency would be affirmatively maintained
  - The Mils™API Standard to be the first
  - Others would include protection profiles adopted from the community and strictly harmonized
- The Mils™ Standards would serve as the basis for the Mils™ Evaluation/Certification Scheme
- The standards are referred to as the ***Mils™ Corpus***

Mils™ Corpus: from MILS to Mils™



The body of existing MILS work forms the input for the development of the Mils™ Corpus.

Only conservative extensions are admitted through the gate to the Mils™ Corpus within an edition of Mils™

The Mils™ Corpus provides the basis for the Mils™ Evaluation and Certification Scheme

Open Group Mils™ Standards Documents (1)

- The Open Group Mils™ Corpus
  - Constructed and qualified by the Mils™ working group
  - Includes Open Group Mils™ Standards
    - OG Community reviewed, published by The Open Group
- The Open Group Mils™ Protection Profiles
  - Adapted from “MILS” community and research PPs
    - Mils™ Platform Protection Profile (MPPP)
    - Mils™ Network System Protection Profile (MNSPP)
    - Mils™ Console System Protection Profile (MCSPP)
  - Adapted from Separation Kernel Protection Profile v1.03
    - Mils™ Separation Kernel Protection Profile (MSKPP)
  - Other Mils™ protection profiles to be developed
    - Mils™ File System Protection Profile (MFSPP)
    - Mils™ Extended Attributes Protection Profile (MEAPP)
    - Mils™ Audit System Protection Profile (MASPP)

Open Group Mils™ Standards Documents (2)

- The Open Group Mils™ Standards
  - Mils™ Application Programming Interface (API) Standard
  - Mils™ Interoperability Standards
  - Mils™ Product Evaluation Methodology
  - Mils™ Compositional Certification Methodology
  - Mils™ Evaluation Laboratory Proficiency Standard
- The Open Group Mils™ Development Standards
  - Mils™ Assurance Cases
  - Mils™ Development Environment and Support Tools

Mils™ Evaluation and Certification Support Scheme

THE Open GROUP
Making standards work®

What is Mils™ Evaluation and Certification?

How terms are being used:

- Mils™ Component – a foundational or operational component, potentially consisting of software, firmware, and hardware, conforming to a Mils™ component PP.
- Mils™ Evaluation – technical assessment of Mils™ components to ISO 15408 and Mils™ standards
- Mils™ System – a composition of Mils™ components and other components, constructed according to Mils™ principles, created to serve an intended purpose within an intended environment
- Mils™ Certification Support – technical assessment of Mils™-based composites according to Mils™ compositional certification methodology
- System Certification & Accreditation (C&A) – a technical and risk-based assessment used to reach a decision to deny or approve a system to operate in an environment (NOT within the scope of the Mils™ Evaluation and Certification Support Scheme)

Need for a Mils™ Evaluation and Certification Support Scheme

- ISO 15408 evaluation alone is not adequate for Mils™
  - No consistent elevated assurance among National Schemes
  - No way for The Open Group to bring unity
  - Lack of proficiency in Mils™ technology or standards
- Mils™ Scheme can bring constructive and cooperative relationship among developers and evaluators to facilitate Mils™ success
  - Evaluation activities span product development process
  - Certification activities span system development process
  - Avoids costly backtracking during evaluation
  - Avoids tendency to accept something that's "too late to fix"

Mils™ Evaluation and Certification

- Establish an ***independent Scheme for Mils™ product evaluation and Mils™ system certification support***
  - Product evaluation and system certification are distinct activities
  - In Mils™ these share common foundations
  - Mils™ objectives span both of these activities
    - Mils™ components are intended to achieve composable systems and compositional system certification
- Mils™ component evaluation
  - Mils™ foundational component PPs and the Mils™ Platform PP
  - Mils™ operational component PPs
  - Vendor's PP-conformant STs and TOEs evaluated by the Scheme
  - Based on ISO 15408 with MILS augmentation
- Mils™ compositional system certification *support*
  - Not intended to supplant existing C&A regimes
  - Provide assessment of Mils™-specific aspects of a system *effectively*
  - C&A regimes decide the weight to be given Mils™ certification

Mils™ Scheme Approach – Validation

- Components validated to The Open Group Mils™ Standards
  - Mils™ Protection Profiles
  - Mils™ API standards
  - Mils™ Evaluation methodology and standards
  - Mils™ Development standards
  - The Open Group issues a component validation certificate
- Composites validated to The Open Group Mils™ Compositional Certification guidelines
  - Mils™ compositional assurance theory
  - Confirmation of composition requirements
  - The Open Group issues a Mils™ composite validation report
- The Open Group maintains evaluation and certification evidence and results in escrow
  - Three-way contractual relationship The Open Group-Applicant-Lab
  - The Open Group's reputation sufficient in ordinary cases
  - Escrow can be opened under extraordinary circumstances

Evaluation and Certification Support Scheme Summary (1)

- The Open Group would be the Mils™ Certifying Body
  - Publish Mils™ Standards
  - Run accreditation program for Mils™ evaluation laboratories
  - Enter 3-Party Contract with product vendor and evaluation lab
  - Provide escrow of evaluation / certification artifacts
- Evaluate products for Mils™ conformance according to
  - Mils™ Protection Profiles
  - Mils™ Application Programming Interface Standard
  - Mils™ Product Evaluation Methodology
- Certify compositions of Mils™ components
  - Using Mils™ component evaluation results
  - Mils™ Compositional Certification Methodology
  - Results may support national system Certification and Accreditation

Evaluation and Certification Support Scheme Summary (2)

- Leverage “MILS” research and development, e.g. research sponsored by US and the EC, and MILS product development by vendors, e.g.
  - “Separation Kernel Protection Profile”
  - “MILS Compositional Certification”
  - “MILS” Protection Profiles and Supporting Documents
  - “MILS” Assurance and Toolchain
  - Distributed MILS (D-MILS)
  - EURO-MILS
- Leverage worldwide ISO 15408/18045 (Common Criteria) evaluation laboratory infrastructure
  - Currently accredited CC evaluation labs are candidates
  - Incremental Mils™ Evaluation Lab accreditation requirements

Mils™ API for Assured Subjects

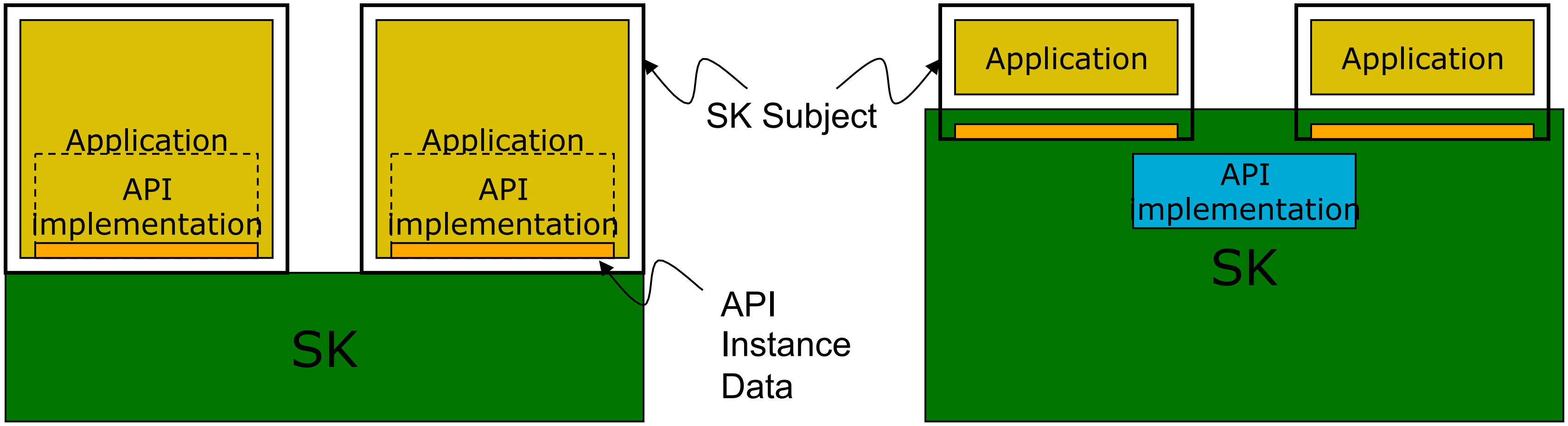
API for development of Mils™
high-assurance subjects
Mils™ API Working Group

THE Open GROUP
Making standards work®

Mils™ API Goals and Objectives

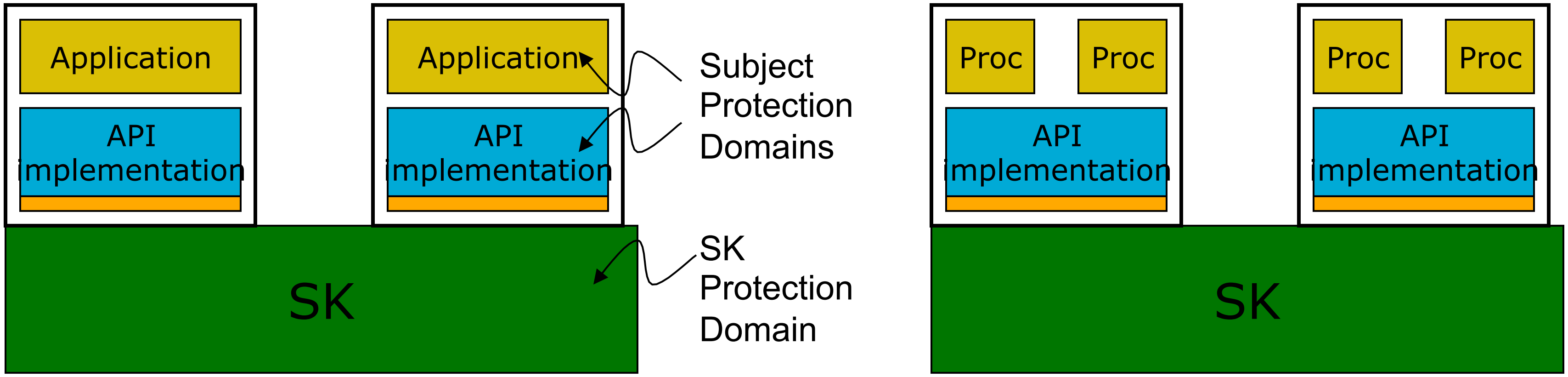
- Provide a standard API for Mils™.
- The Mils™ API is intended to provide a common API for the development of assured subjects, including the Mils™ foundational components and trusted operational components in a Mils™ environment.
- The Mils™ API is intended to catalyze the commercial marketplace for assured software products for Mils™ platforms provided by multiple vendors.
- The Mils™ API Standard should identify the interfaces that must be provided by implementations. If there optional APIs or packages of APIs those should be identified by the Standard
- The Mils™ API Standard should precisely specify the semantics of the interfaces provided to facilitate analysis of using programs.
- The Mils™ API Standard should provide sufficient information to enable implementations of the Standard to conform to the specified semantics regardless of the underlying hardware architecture or the chosen Mils™ Platform.

Some* Mils™ API Architectural Insertion Alternatives



1. The implementation and the instance data reside in the application’s domain. Single POSIX process per SK subject.

2. The implementation and the instance data reside in the SK’s domain. Single POSIX process per SK subject.



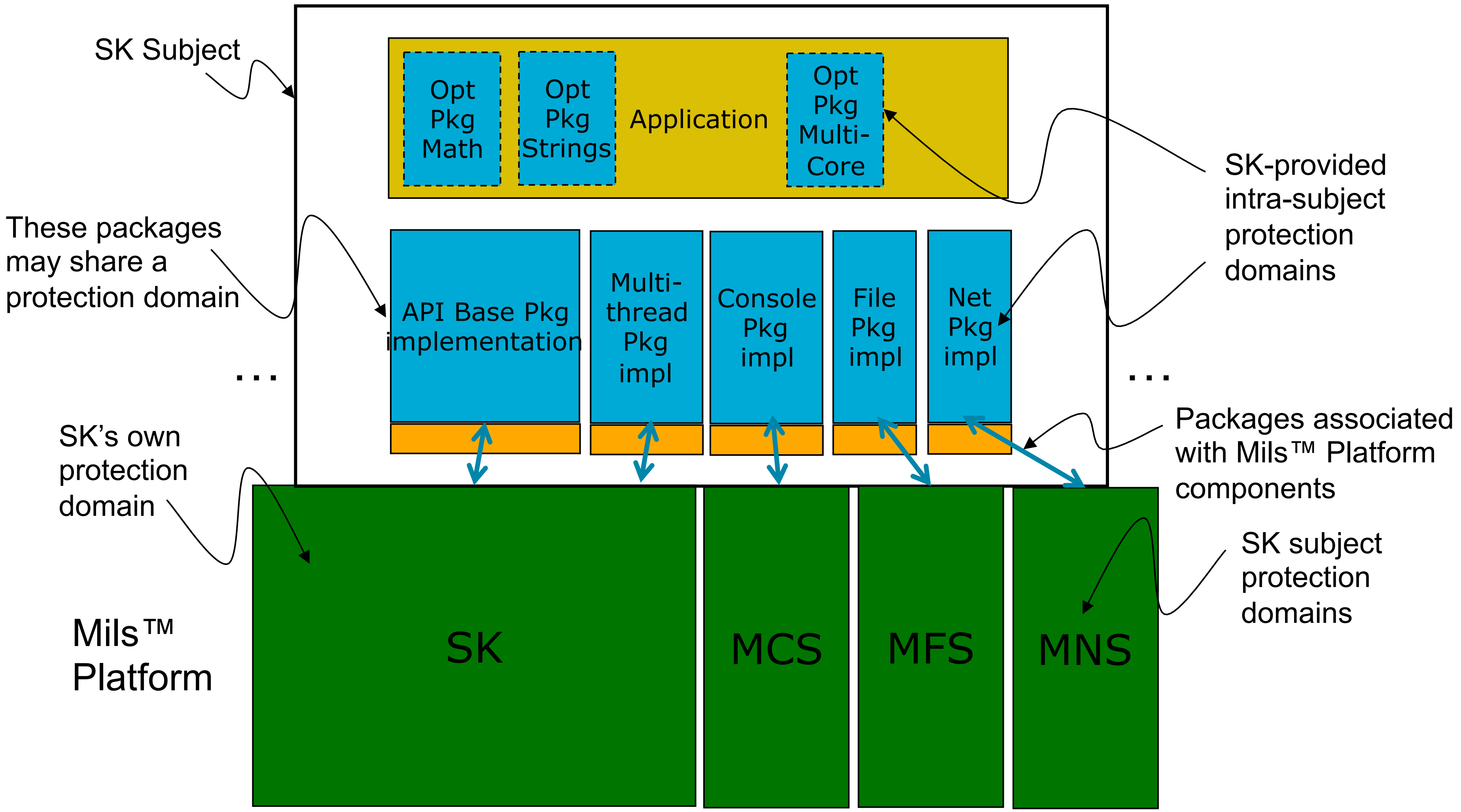
3. The implementation and the instance data reside in a distinct protection domain within an SK subject. Single POSIX process per SK subject.

4. The implementation and the instance data reside in a distinct protection domain within an SK subject; multiple POSIX processes per subject are permitted.

* Other variations are possible

Mils™ API packages

Using #3 from Architectural Insertion Alternatives:



SK Subject

These packages may share a protection domain

SK's own protection domain

Mils™ Platform

SK-provided intra-subject protection domains

Packages associated with Mils™ Platform components

SK subject protection domains

Mils™ Platform: Interface Summary

MILS foundational component	Primitive resources managed	Interface abstraction provided by	Low-level mechanisms utilized by implementation
Mils™ Separation Kernel (MSK)	Processor, Memory, Intrinsic Devices (e.g. clock)	Application programming language	ISA, MMU, IOMMU, timers, clocks
Mils™ File Subsystem (MFS)	Mass Storage Devices	File Package APIs (Mils™ API standard)	Mem structs, SK-calls, msgs
Mils™ Console Subsystem (MCS)	Human Interface Devices	Console Package (Mils™ API standard)	Mem structs, SK-calls, msgs
Mils™ Network Subsystem (MNS)	Network Interface Devices	Network Package (Mils™ API standard)	Mem structs, SK-calls, msgs
Mils™ Extended Attributes Subsystem (MEA)	Memory and File Storage exported resources	MILS Attribute Package(extended Mils™ API Standard)	Mem structs, SK-calls, msgs, file system API, resource identifiers
Mils™ Audit Subsystem (MAS)	SK audit record buffer, File Storage	Mils™ Audit Package (extended Mils™ API Standard), inter-subsystem query	Mem structs, files, SK-calls, msgs, file system API, resource ids, SK audit primitives

Mils™ Development Environment

Standards for tools and techniques

THE Open GROUP
Making standards work®

Mils™ Development Environment

- A recently formed activity within The Open Group Real Time and Embedded Systems Forum – The Mils™ Development Environment Working Group
- Identify categories of automation support to make MILS™ development more cost efficient, e.g.
  - Declarative languages (e.g. AADL)
  - Verification framework
  - Assurance case
- Develop standards for Mils™ Development Environment tools to encourage development of tool products that are consistent with a common approach (still allows specialisation and innovation)

Thank You

Rance J. DeLong
r.delong@opengroup.org

THE Open GROUP
Making standards work®