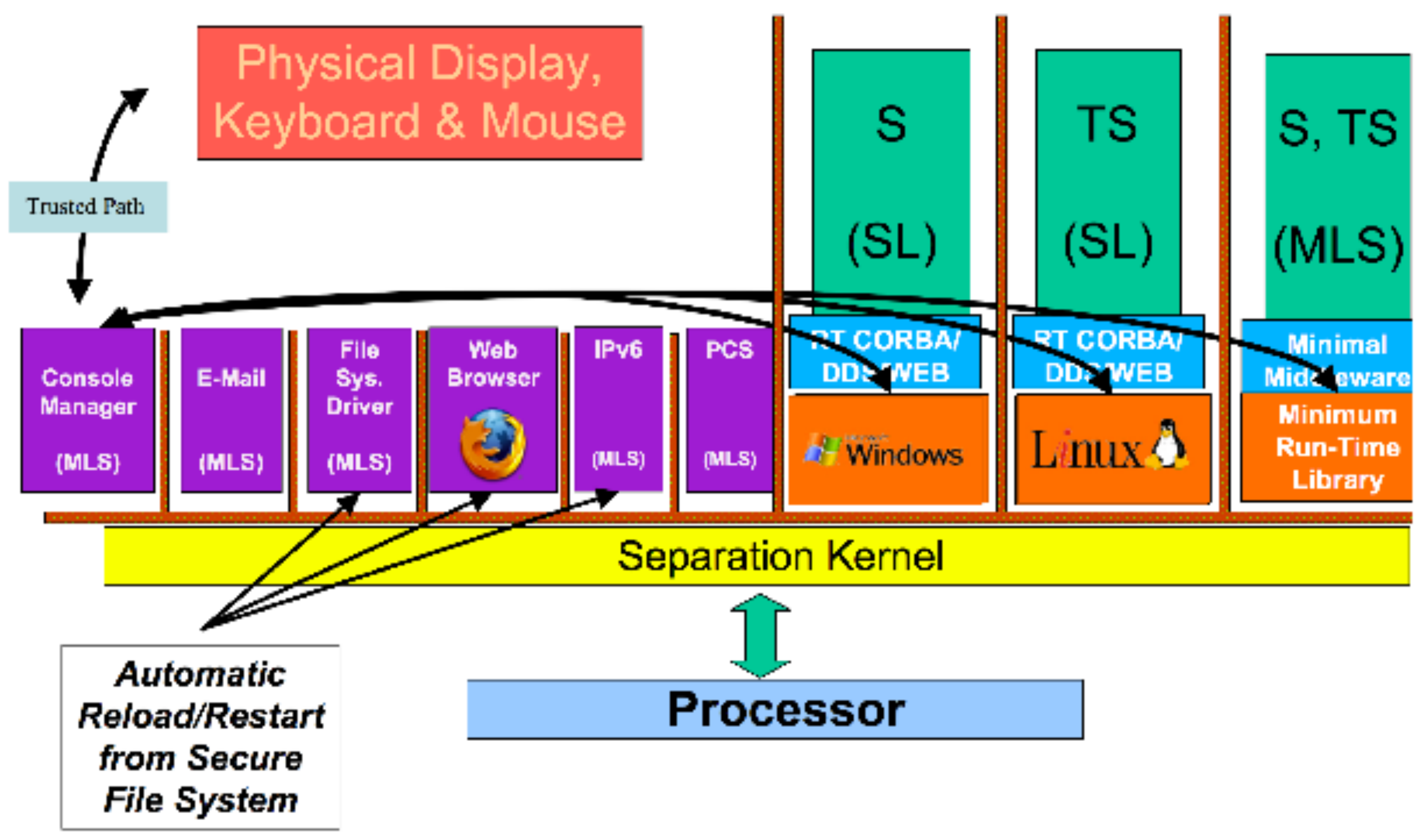
Future Mils™

Panel on the Future of Highly Trustworthy Systems, Networks, Apps , and Clouds

December 5, 2011

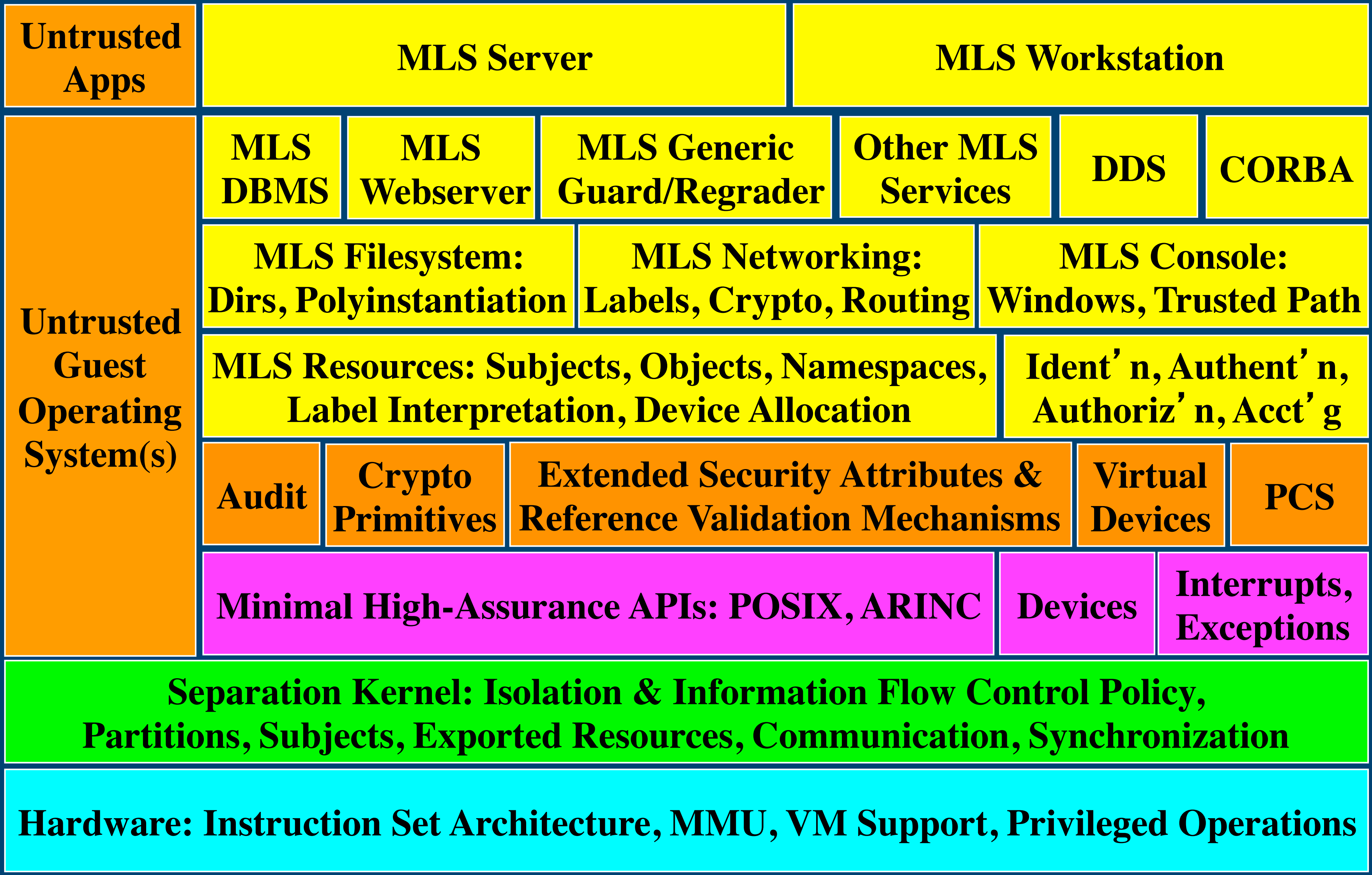
Rance DeLong
Staff Scientist, LynuxWorks
Adjunct Lecturer, Santa Clara University
Consulting Researcher
RDeLong@lnxw.com
RDeLong@engr.scu.edu
MILSresearch@me.com

MILS (the historical* view)



* MILS workstation concept, Calloni and others, circa 2004

A desired MILS goal – MLS Server / Workstation*



Untrusted Apps

MLS Server

MLS Workstation

Untrusted Guest Operating System(s)

MLS DBMS

MLS Webserver

MLS Generic Guard/Regrader

Other MLS Services

DDS

CORBA

MLS Filesystem: Dirs, Polyinstantiation

MLS Networking: Labels, Crypto, Routing

MLS Console: Windows, Trusted Path

MLS Resources: Subjects, Objects, Namespaces, Label Interpretation, Device Allocation

Ident’n, Authent’n, Authoriz’n, Acct’g

Audit

Crypto Primitives

Extended Security Attributes & Reference Validation Mechanisms

Virtual Devices

PCS

Minimal High-Assurance APIs: POSIX, ARINC

Devices

Interrupts, Exceptions

Separation Kernel: Isolation & Information Flow Control Policy, Partitions, Subjects, Exported Resources, Communication, Synchronization

Hardware: Instruction Set Architecture, MMU, VM Support, Privileged Operations

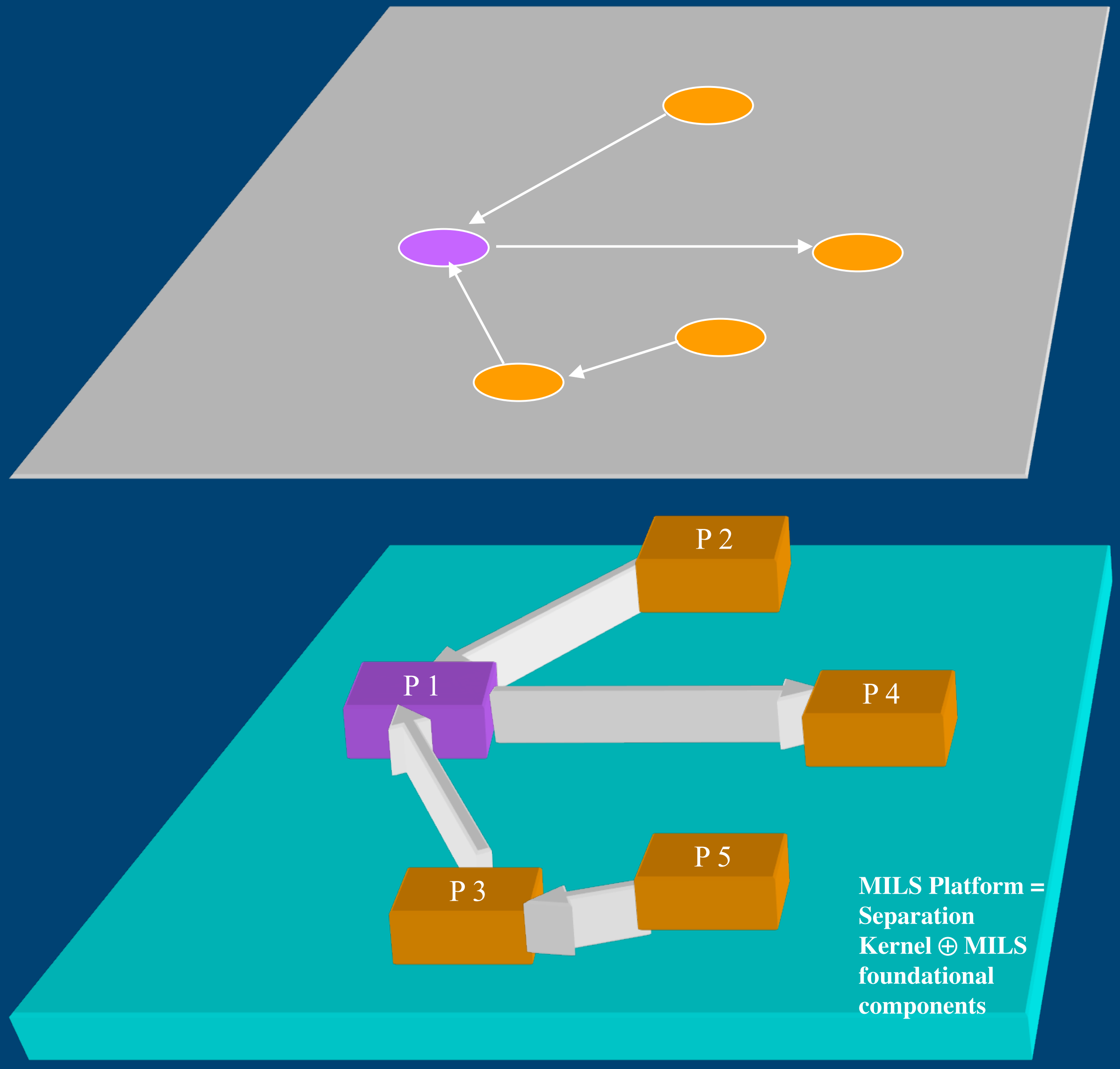
* MILS workstation/server notional architecture, DeLong January 2005

Some components needed for a high-assurance Server or Workstation . . .

- Console with trusted window system
- Trusted global naming service, identity/integrity attestation
- Trusted disk and other mass storage devices and filesystems
- Trusted networking
- PCS, DDS, CORBA
- System-level attestation services
- Session management (interactive sessions: command env, session lock/unlock, suspend/resume)
- Application management of MILS multi-resource applications (dynamic instantiation, dynamic resource mgmt)
- System management (user admin, app admin, dev mgmt, sys update, plugins)
- System operations management
- System self-test, integrity and recovery
- Auditing (daemon, storage, configuration, analysis)
- Security management (user/group security attributes, RBAC, label encoding admin)
- MLS objects, attributes and MLS policy arbiter (label interpretation and decision part of any MLS RVM)
- User IAAA - Identification, Authentication, Authorization, Accounting
- Cryptographic services support
- Generic guard/regrader (rule-driven, type-driven)
- DBMS
- Web server
- Web browser
- Daemons (system log, printer, e-mail)
- Hardware for high-performance trusted graphics
- MLS USB device management
- High-integrity programming language runtime support and MLS JVM
- Hardware micro-architecture resource partitioning support
- …

THE POINT IS: reliable composition of many components is needed.

Operational Component Architecture Implemented on MILS Foundational Components



MILS Platform = Separation Kernel ⊕ MILS foundational components

Operational Component Architecture

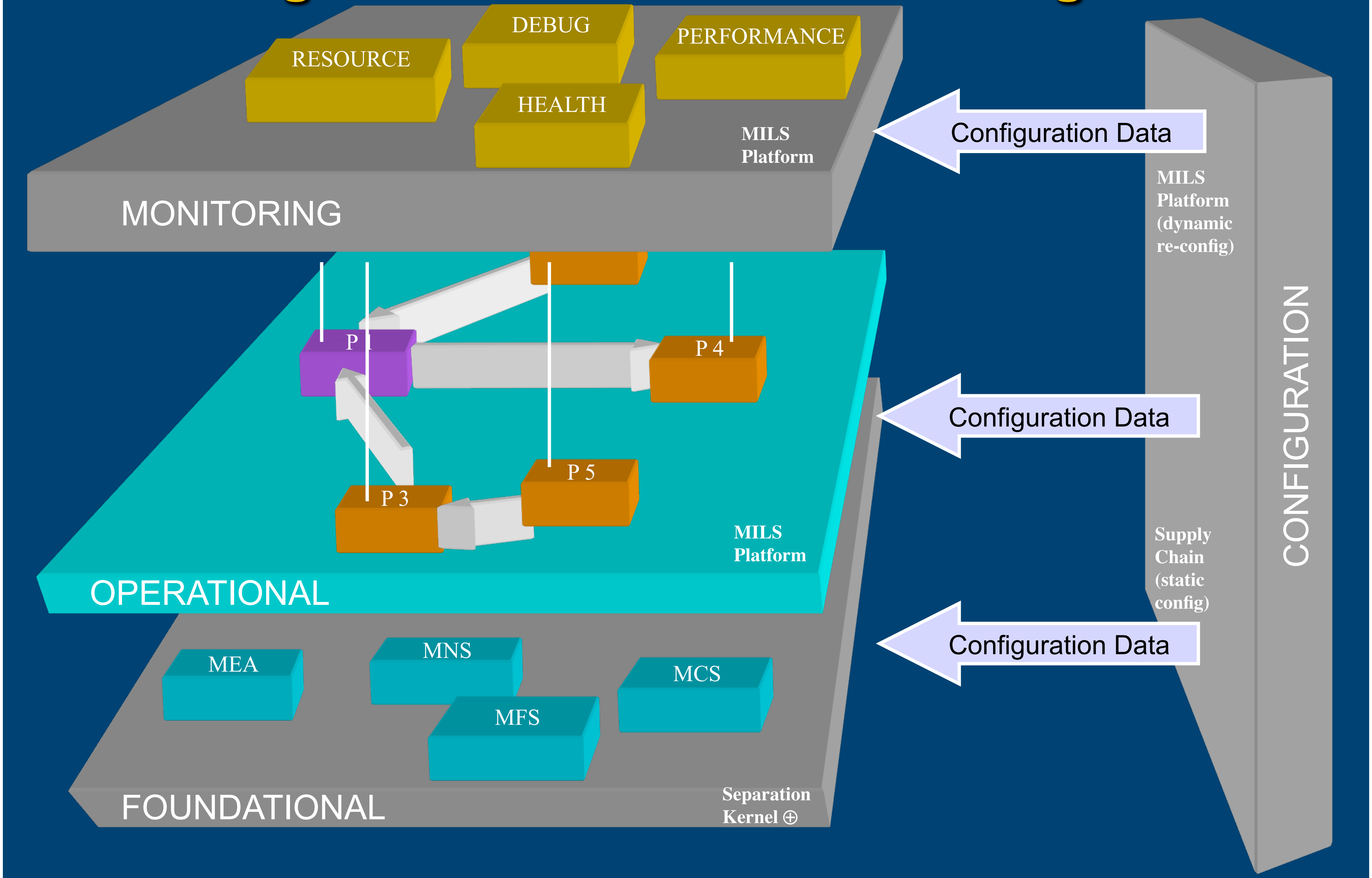
The "policy architecture" of a system

System Implementation*

SK ⊕ foundational components form a resource-sharing substrate, providing isolation and information flow control, *enforcing the architecture*

* MILS "two-level view", Rushby & DeLong, circa 2006

MILS Foundational, Operational, Monitoring, and Configuration Planes – other othogonal



“MILS”, “MILS Initiative”, and “Mils™”

- “MILS” – originally an acronym for “Multiple Independent Levels of Security”. Its usage 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, fostered within The Open Group, pursuing the “MILS idea” for nearly a decade. Upshot: to achieve its objectives, “MILS” must be refined and systematized.
- “Mils™” – Now used as a proper noun*, rather than an acronym, “Mils” refers to a refined set of concept definitions, architecture, doctrine, standards, practices and support for the development, evaluation, certification and deployment of Mils components and systems intended to achieve MILS’s original goals. “Mils™” is a trademark of The Open Group.

* What Rushby refers to as “Modern MILS”

The important thing about Mils™

- Mils™ can achieve more than MILS.
  It can achieve what MILS set out to do: verifiable and certifiable composition of component-based architecture, for properties and functions.
- Traditional MILS cannot achieve the integration, interoperability, and certification goals for a successful marketplace of components without the discipline of Mils™

* What Rushby refers to as “Modern MILS”

Where is Mils™ headed in the not to distant future?

Near-Term Mils™ includes: Technical Standards

- The Open Group Mils™ Protection Profiles
  - Community review, published by The Open Group
  - Adapted from "MILS" community and research PPs
  - Adapted from Separation Kernel Protection Profile v1.03
    - Mils™ Separation Kernel Protection Profile (MSKPP)
- TOG Mils™ Technical Standards
  - Mils™ Application Programming Interface (API) Standard
  - Mils™ Interoperability Standards
  - Mils™ Evaluation Methodology
  - Mils™ Compositional Certification Methodology
  - Mils™ Evaluation Laboratory Proficiency Standard

Near-Term Mils™ includes: Use of the Common Criteria

- CC Domain
  - Use the “vanilla” Common Criteria to greatest extent practical
- Mils™ Domain
  - Mils-specific, e.g., Assurance cases (Claims-Argument-Evidence Model)
  - Mils standards, e.g., APIs, interoperability standards
  - Mils compositional certification theory and practice
  - Other properties of concern in addition to Security covered by CC Domain

Near-Term Mils™ includes: Evaluation Approach

- Apply the international CC
  - Use the CC and CEM fully and consistently
  - Mils' high assurance does not conflict with CCRA (EALs 1-4)
  - Contribute to the ongoing development of the CC
- Augment with Mils-specific technical measures and methodology to support high-assurance evaluation and certification
  - Assurance case - linking product claims to product-based evidence
  - Tools to diminish labor and increase repeatability
  - Augmentation to CC supporting high assurance and composition
  - Interoperability standards for functional composability
- Make high-assurance evaluation objectively verifiable and more cost-effective with automation

Near-Term Mils™ includes: Component and Composite Validation

- Components validated to TOG Mils standards
  - Mils Protection Profiles
  - Mils API standards
  - Mils evaluation methodology and standards
- Composites validated to TOG Mils compositional certification guidelines
  - Mils compositional assurance
  - Confirmation that composition requirements met
- The Open Group maintains evaluation and certification evidence and results in escrow
  - Three-way contractual relationship TOG-Applicant-Lab
  - TOG reputation sufficient in ordinary cases
  - Escrow can be opened under extraordinary circumstances

A Five-year vision for Mils™ stakeholders

- Component developers
  - Interoperability standards
  - Techniques and tools
  - Engineering Handbook
- System Integrators
  - Component marketplace
  - Interoperability standards
  - Techniques and tools
  - Application Handbook
- Gov and industry customers
  - Understand capabilities and benefits of Mils™
  - Effective Mils™ integrators
  - Design patterns and pilots available
- Educators and trainers
  - Corpus of theory, design patterns, and engr practice
  - Mils™ handbooks
  - Theory and practice training materials
- System certifiers
  - Compositional certification science, stds, methodology
  - Certification Handbook
- Product evaluators
  - MIPP conformance
  - Mils™ Protection Profiles
  - Evaluation Handbook
- Researchers
  - Research opp'ties / wkshps

Let's assume that will all happen… then what could Mils™ go on to become?

"Future Mils™" *

Speculate what Mils™
could be in 2021 and beyond …

* Intended by the speaker only for the purpose of discussion.
Not purported to represent the intentions of The Open Group

Future Mils™

A vision of what Mils™ could be in 2021

- Distributed Mils™
- Mils™ Clouds
- Mils™ SOA
- Self-hosted Mils development in a Mils™ Cloud
- “Recursive” Mils™
- Mils™ IDE
- Certified-by-Construction Mils™
- Just-in-Time Certification of dynamic Mils™ systems

Future Mils™ (2)

A vision of what Mils™ could be in 2021

- Capability-based Mils™ dynamic separation kernels
- Mils™ -appropriate network link, e.g., TTEthernet
- Policy Domain hierarchies
- Visual architectural specification
- Coordinated formal methods languages and engines
- Synthesis of interface modules
- Pre-compute (once for all) bulk of the cert'n proof
- Compute proof conditions under actual parameters