



Partitioning Communications System
for
High Availability Systems

Partitioning Communications System

*for
High Availability Systems*

Gordon M. Uchenick
Senior Mentor / Principal Engineer

410-256-7102

gordon.uchenick@ois.com



Agenda

Partitioning Communications System for High Availability Systems

- The MILS Architectural Foundation
- MILS Distributed Systems
- Partitioning Communications System
- PCS Protection Profile



The Whole Point of MILS

Partitioning Communications System
for
High Availability Systems

Really very simple:

- Dramatically **reduce the amount of** *safety and security critical code*

So that we can

- Dramatically **increase the scrutiny of** *safety and security critical code*

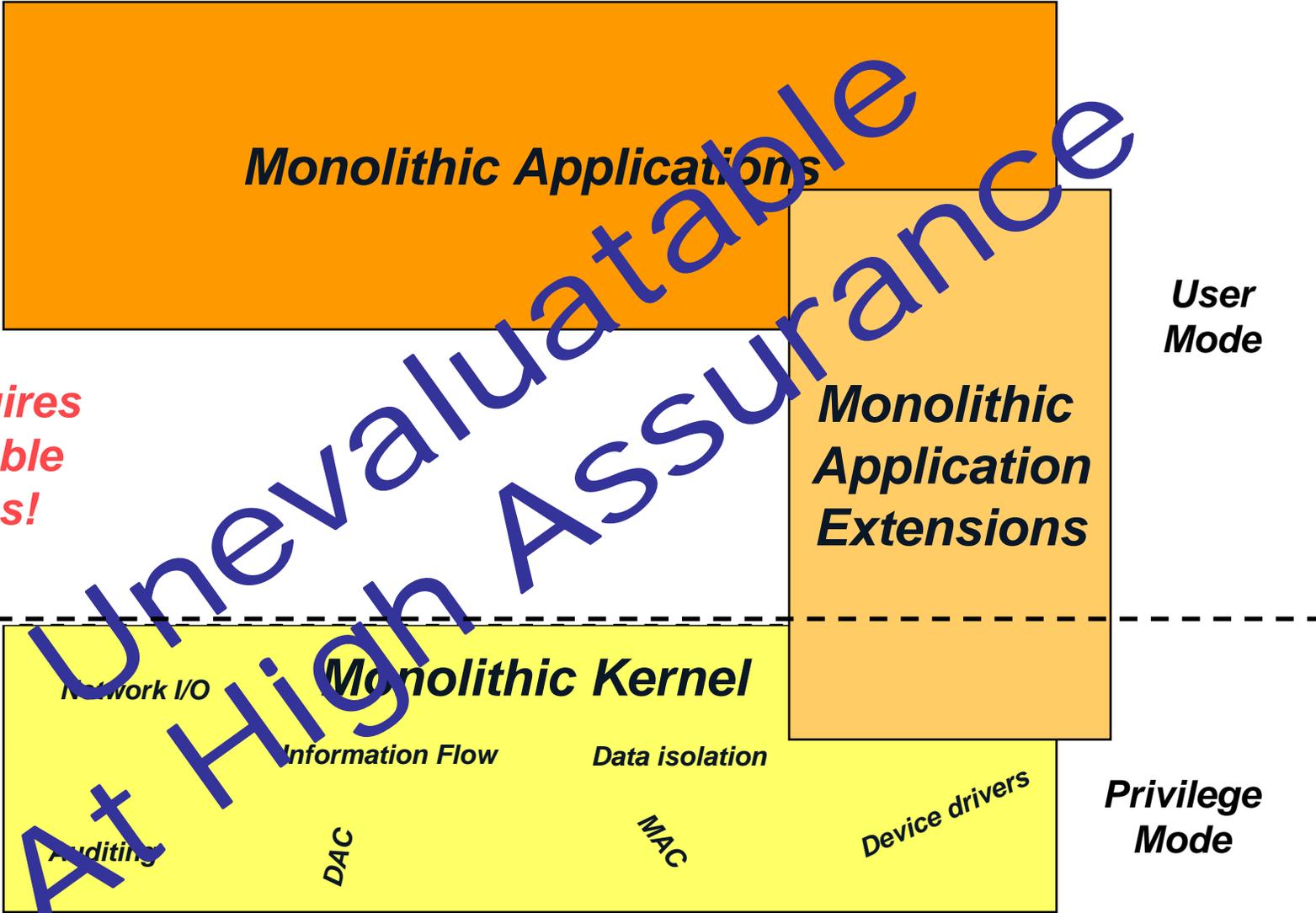
To make

- Development, certification, and accreditation more **practical, achievable, and affordable.**



Where We've Been:
Starting Point for Architectural
Evolution

Partitioning Communications System
for
High Availability Systems



**IMA Requires
Evaluatable
Systems!**

At High Assurance

Fault Isolation
Periods Processing
Kernel

**User
Mode**

**Privilege
Mode**



MILS Architecture Evolution

Partitioning Communications System
for
High Availability Systems

Application
Modules

CSCI
(Main Program)

Level E
Application



Level C
Application



Level A
Application



Multi-Level
Guard

Rushby's
Middleware

Fault Isolation
Periods Processing

Kernel

Network I/O

Separation Kernel

Information Flow

Data Isolation

Auditing

DAC

MAC

File systems
Device drivers

User
Mode

Appropriate
Mathematical
Verification

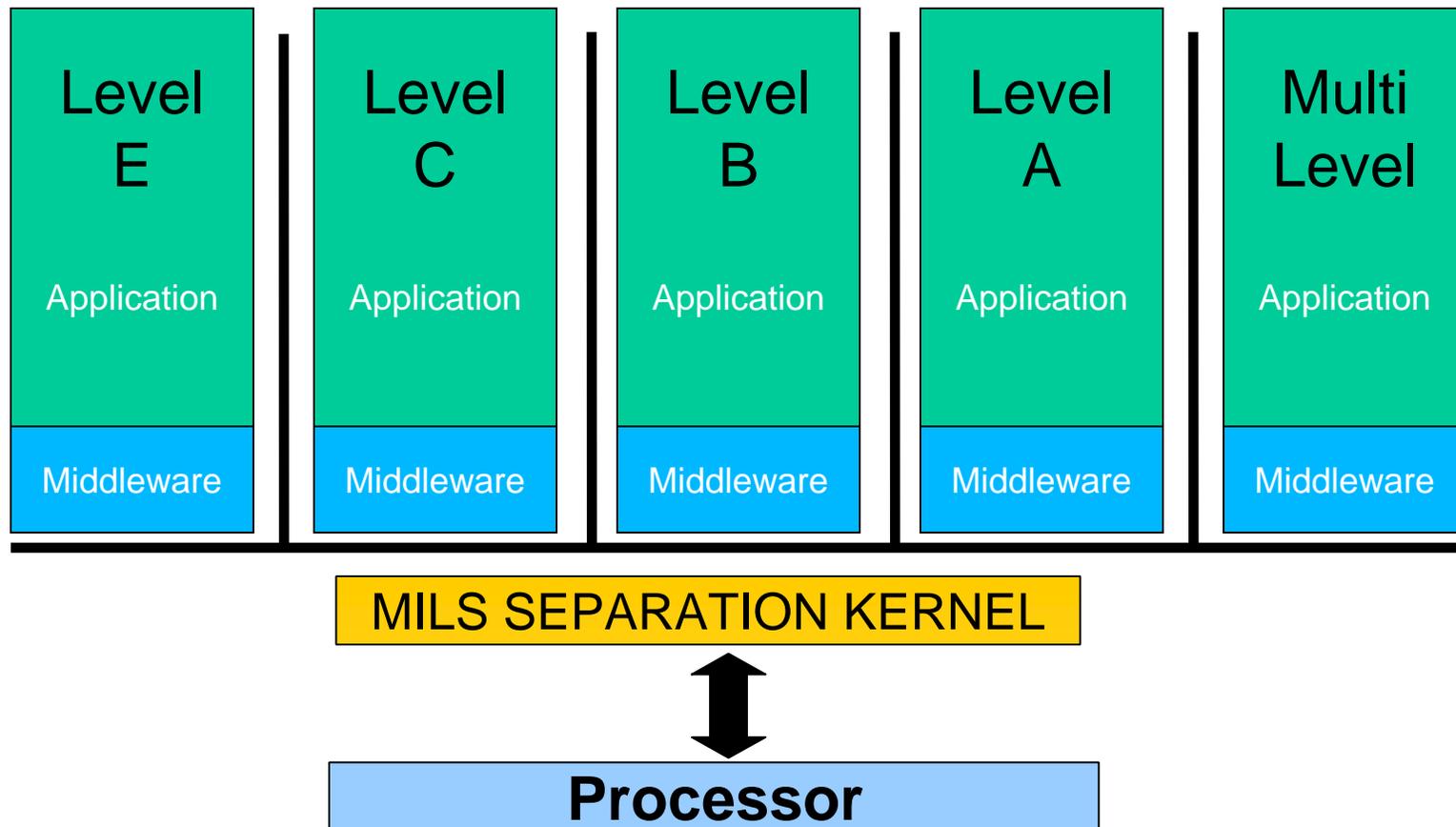
Privilege
Mode

Evaluatable Applications On an Evaluatable Infrastructure



The MILS Architecture

Partitioning Communications System
for
High Availability Systems



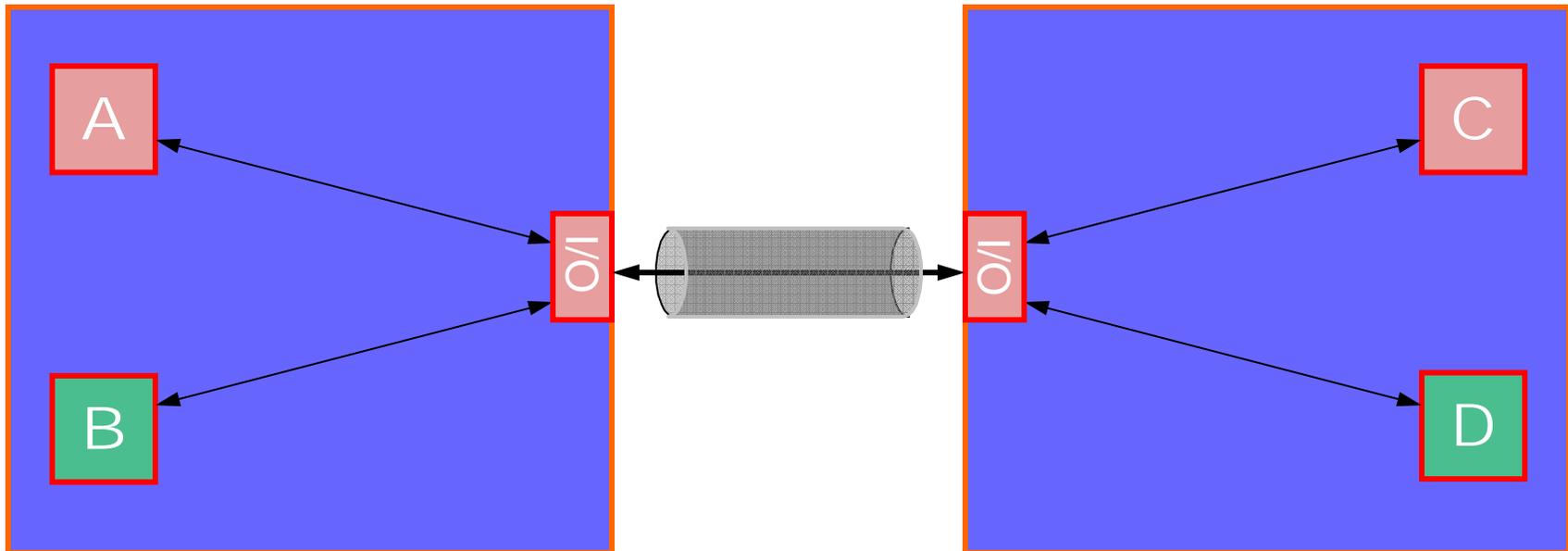


- **Information Flow**
 - Restrictive flow policy
 - Information originates only from authorized/authenticated sources
 - Information is delivered only to intended recipients
 - Source of Information is authenticated to recipient
- **Data Isolation**
 - Information in a partition is accessible only by that partition
 - Private data remains private
- **Periods Processing**
 - The microprocessor itself will not convey corrupting information from one partition to another as it switches from partition to partition
- **Damage Limitation**
 - A failure in one partition will not cascade to another partition
 - Failures will be detected, contained, & recovered from locally



MILS Distributed Systems

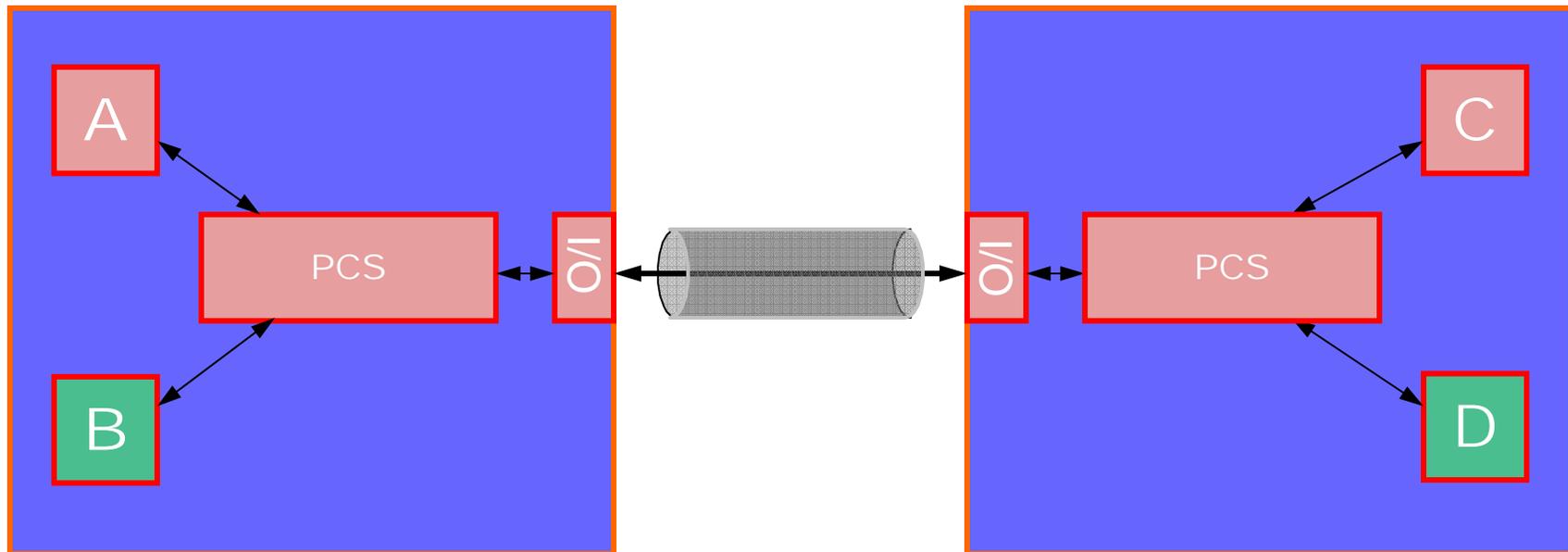
Partitioning Communications System
for
High Availability Systems





Partitioning Communications System

Partitioning Communications System
for
High Availability Systems





PCS Specific Requirements

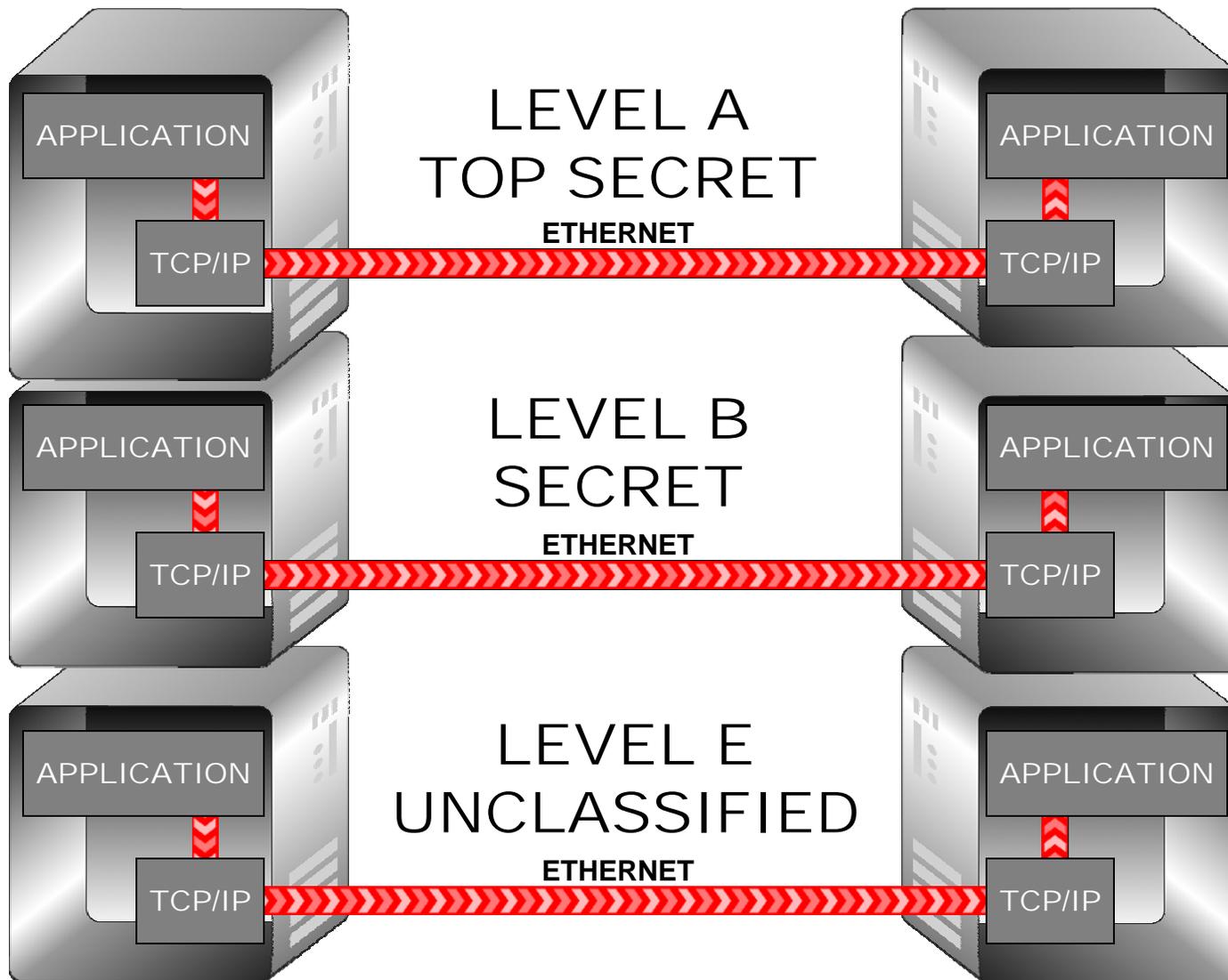
Partitioning Communications System for High Availability Systems

- Strong Identity
 - Nodes within enclave
- Separation of Levels/Communities of Interest
 - Strong cryptographic separation
- Secure Configuration of all Nodes in Enclave
 - Federated information
 - Distributed (compared) vs. Centralized (signed)
- Secure Loading: signed partition images
- Secure Clock Synchronization
- Bandwidth provisioning & partitioning
 - Network resources: bandwidth, hardware resources, buffers
- Suppression of Covert Channels



*Air Gap Works But...
Costly, Inflexible, & Awkward*

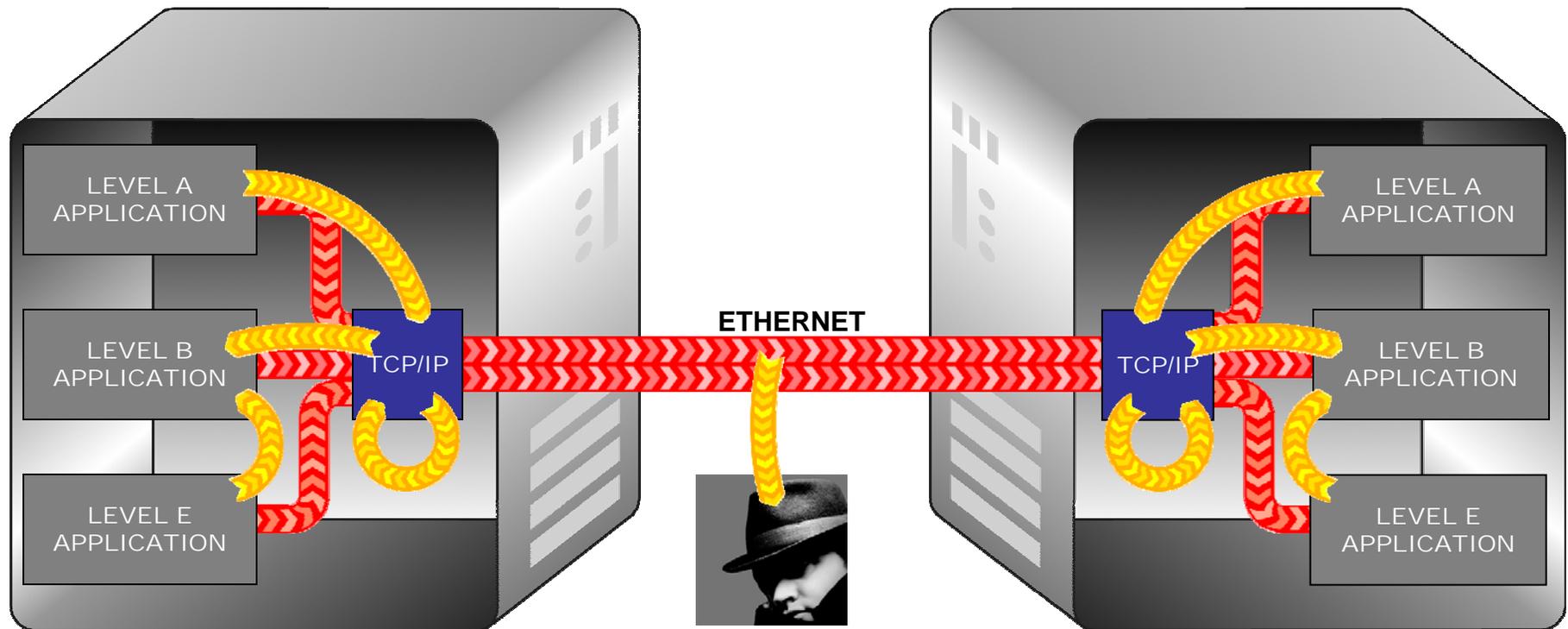
Partitioning Communications System
for
High Availability Systems





Combining Levels On Medium Assurance Platforms Is Unsafe

Partitioning Communications System for High Availability Systems



LEGEND

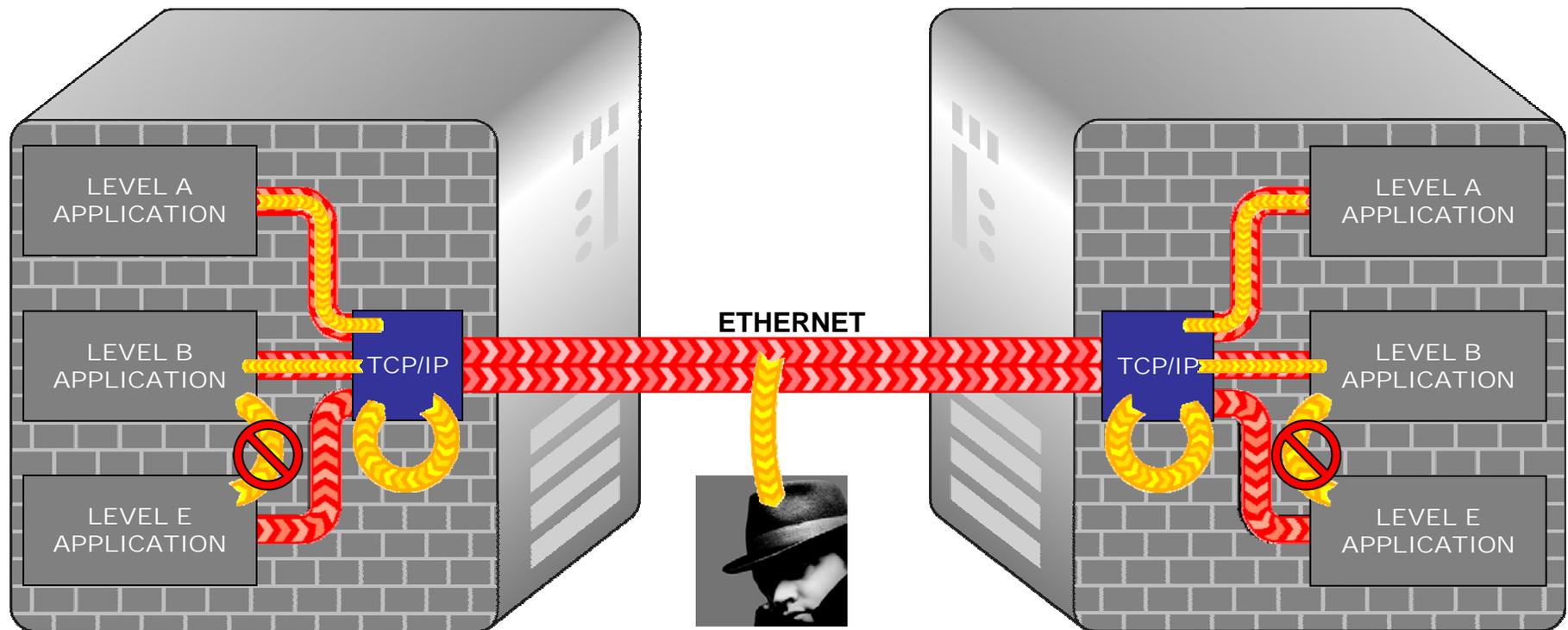


Vulnerabilities



MILS Separation Kernels Counter Most Internal Threats

Partitioning Communications System
for
High Availability Systems



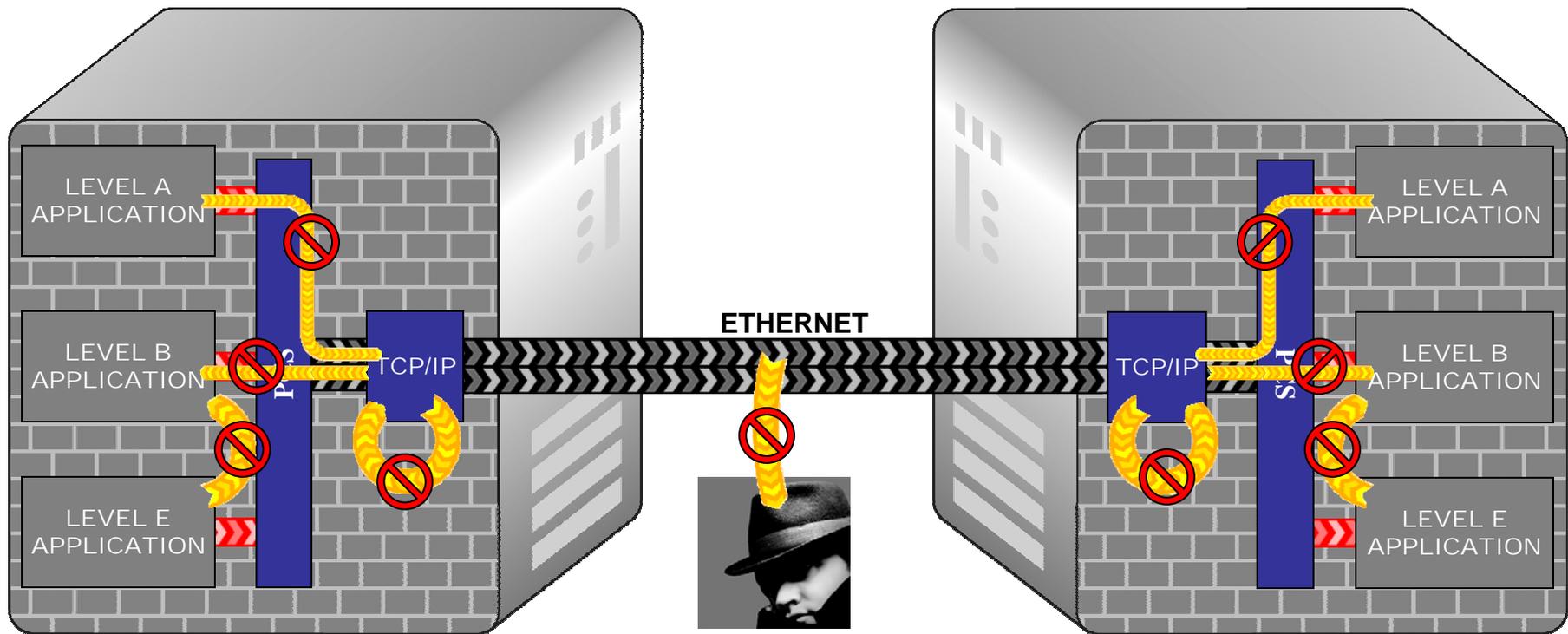
LEGEND

- Vulnerabilities
- Reduced Vulnerabilities



PCS Completes MILS Separation Kernel

Partitioning Communications System for High Availability Systems



LEGEND

- Vulnerabilities
- Reduced Vulnerabilities



Why PCS?

Partitioning Communications System for High Availability Systems

- Protect investment in legacy applications
 - Communication safety and security policy enforcement transparent to application, middleware, and protocols
- Simplify secure distributed application development
 - Developers do not have to focus on data flow identification & authorization
- Enable agile networking
 - Able to bridge between networks and across domains
- Quick reaction to changing requirements
 - Changes to infrastructure and safety/security policy enforcement transparent to applications
- Reduce Certification & Accreditation risk
 - Reusable safety and security evaluation artifacts



What PCS IS and IS NOT

Partitioning Communications System for High Availability Systems

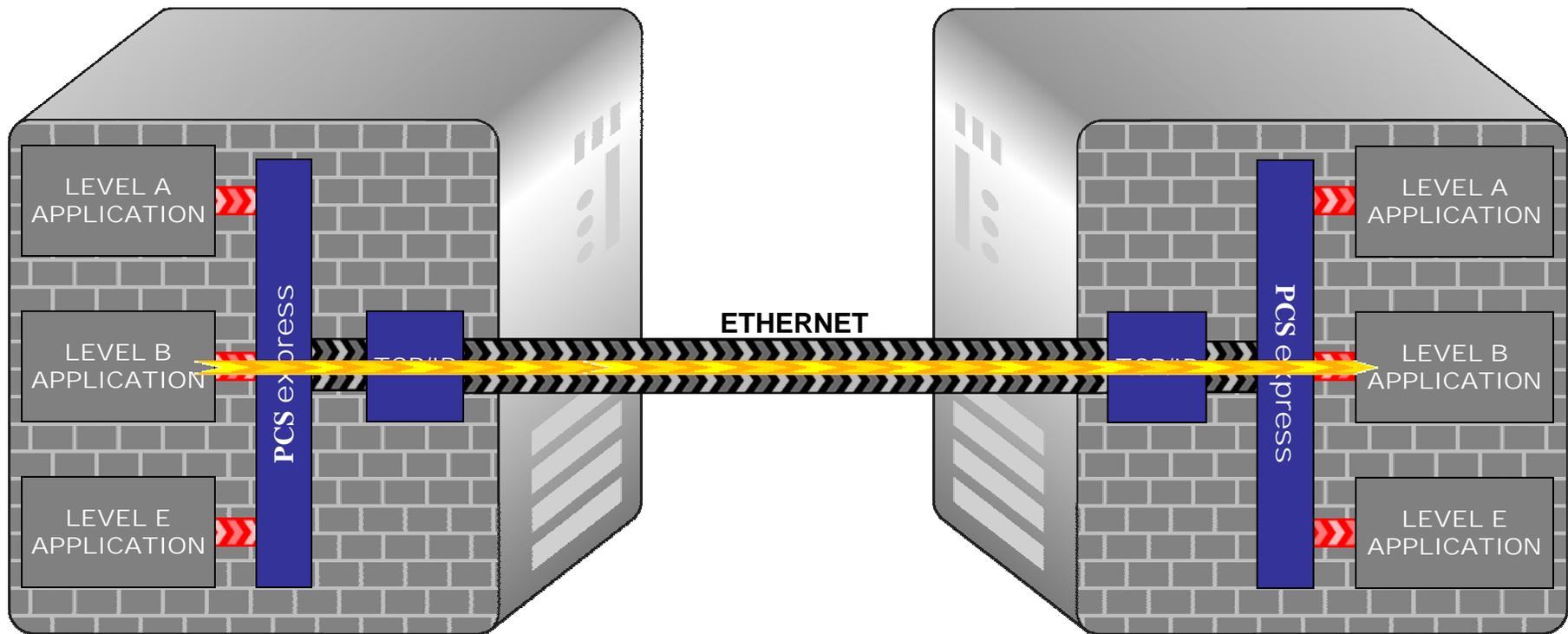
- **PCS *IS***
 - Like a super VPN configured between partitions in distributed nodes
 - Adds techniques for covert storage and time channel suppression
 - Very flexible and dynamic configuration
 - More expressive than IPSec or SSL policy capabilities

- **PCS *IS NOT***
 - Applications middleware like CORBA, DDS, or Web Services
 - A Guard or Application Firewall
 - Doesn't examine message content
 - Can't enforce security policies delegated to the application layer
 - A total, end-to-end security solution
 - Foundation for application level security
 - *Not a replacement* for application level security



Guards Still Needed for Content Attacks

Partitioning Communications System for High Availability Systems



LEGEND

➡ Data Vulnerability



- PCS assumes the network can't be trusted
 - Leverage COTS stacks, NICs, media, switches, and routers
- PCS provides trusted data flow among distributed applications and guards
 - Code that was typically duplicated from partition to partition
 - *NEAT*ness is guaranteed
- Access guards and data guards can be tightly focused on the data owner's specific requirements
- Trusted data flow enables higher guard assurance
 - Smaller code body
 - Simpler logic
 - Formal methods more practical when required



PCS Protection Profile

Partitioning Communications System
for
High Availability Systems

- Developed as part of the AFRL MILS program
- Objective Interface is the developer
- Sponsorship from Objective Interface Systems, Lockheed Martin, Raytheon Company and the J-UCAS program
- First public draft circulated for comment January, 2005
- Second public draft circulated July, 2006
 - Request download at <http://www.ois.com/download.asp>
- Current status
 - PP being upgraded to SKPP V1.0 and CC V2.3
 - Comments being reviewed and integrated
 - Ongoing rigorous internal review



Questions?

Partitioning Communications System
for
High Availability Systems