Superior Products Through Innovation

MILS Architecture: A Solution Using COTS

Advanced Development Programs

Dr. Ben A. Calloni, P.E.

Research Program Manager and Principle Investigator

Lockheed Martin Aeronautics Company

Overview

- Introduction
- MIL-SPEC: Great “-ilities” but with a cost
- Embedded / RT cf. IT
- Commercial Off the Shelf and DoD
- MILS and Benefits
- Common Criteria, NIST, NSA and NIAP
- Foundational Principles
- Conclusion

- **Theory is when you know everything and nothing works.**
- **Practice is when everything works and no one knows why.**

- In our lab, theory and practice are combined:

  Nothing works an no one knows why!

The Information Assurance Challenge

- **We need to achieve "commodity", COTS Information Assurance**
  - ***Multi-Level Security, Cross Domain Systems, HIPAA, etc. systems***
- **The "Multiple Independent Levels of Security (MILS) Architecture" is about making it possible for application level processes to enforce the policy semantics specific to an organization**
  - ***… without trust concerns regarding the infrastructure upon which they operate***
- **MILS does this by distributing high confidence trusted enforcement mechanisms across multiple layers**
    - OS, Middleware, Applications
- **These independent layers must compose****
  - ***… preserve independent component properties***
  - ***… achieve desired emergent system properties***
  - ***… prohibit undesired emergent system properties***

Vietnam Era Pilot's Wrist Watch
$59 (1973) : $247.89 (2004)

- **Hand Wound, 15 Jewel Movement**
- **Radium Dial (glow in dark)**
- **+/- 60 Sec accuracy (Daily)**
  - *Morning update from Base Ops GMT Atomic Clock*
- **Water Proof to -30 feet**
- **Low Pressure**
  - *35,000 feet for minimum of 60 minutes*
- **Shock Resistant**
- **Magnetic Protection**
  - *14.5 to 15.5 gauss protection*
- **H3 & Radiation Markings (Tritium)**
- **Test for Radiation Leakage**
- **Order placed for Hundreds of Thousands**
  - *Warehouse the spares*

WATCH, WRIST: GENERAL PURPOSE
MIL-W-46374A
HAMILTON
6645-952-3767
MFG. PART NO. 39988
DAAA25-72-00458
APRIL 1973
US

Casio Calculator Watch ($14.95 in 1985)

- Digital Display
- 8-Digit Calculator
- Dual Time
- 1/100 Second Stopwatch w/ Net Time, Split Time, Lap Time
- Daily Alarm
- Auto-Calendar
- Water Resistant
- Accuracy: +/- 1 Seconds a Month
- Band Type: Resin
- Color: Black
- Battery Life: Approx. 1 Year

Flashing Blue Light

K-Mart Special: $9.95

MIL STD Version

- Same as commercial
- **PLUS**
- Water Proof to -30 feet
- Low Pressure
  - *35,000 feet for minimum of 60 minutes*
- Magnetic Protection
  - *125±1 gauss*
- ±0.7 seconds per day (@ 75°F)
- **Battery Life: 3 Years Minimum**

Instead of < $9.95 - $127.93 (1985)

$222.10 (2004)

Mil-Std vs. COTS Watches

5 year Cost of Ownership!

	Service Life	Unit Cost	Total Units	5 year cost
COTS	1 year	$ 9.95	15,750	$ 156,712.50
MIL STD	5 years	$ 127.93	3,000	$ 383,790.00

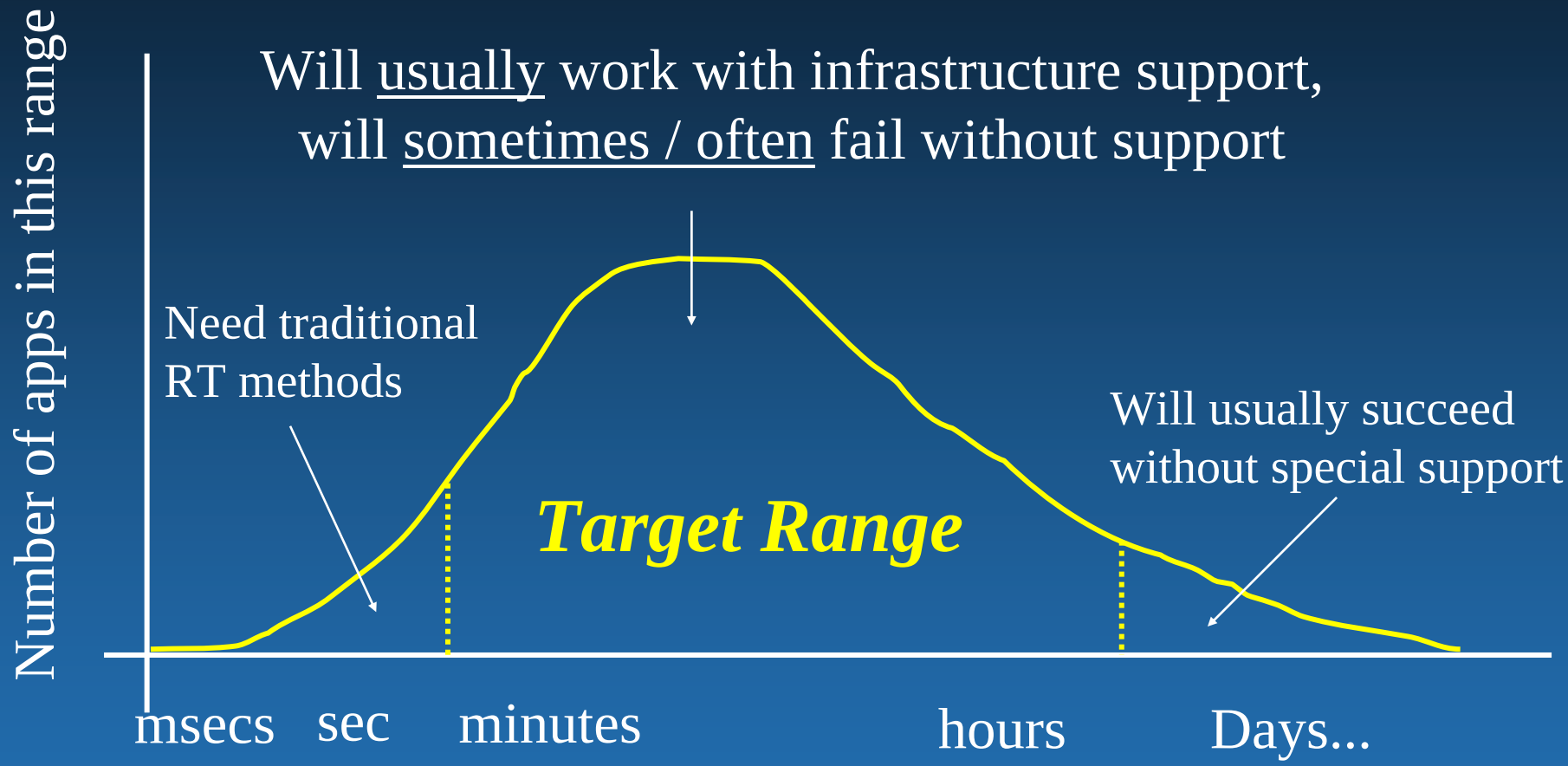
BUT…Single Board Computers for DoD

- *Assume an airframe life of 8,000 flying hours / service life of 25+ years*
- *Moore's Law ' ': 8 "tech doublings" during lifespan*
- *Why are boards components "spec'ed" to 15,000 hrs MTBF?*

What do people mean by Real-time?

- **"Near Real-Time" information is available (at your computer) "near" to the time when events occurred**
  - ***acceptable** temporal latency **of information delivery***
- **Interactive "Real-time" systems (usually human involved)**
  - ***acceptable** temporal responsiveness **between participants (humans-computer, computer-computer) to avoid timeouts***
- **Traditional "real-time" (the "embedded, R/T geek" definition)**
  - ***time critical data / operations - must meet a deadline***
- **There are other temporal concerns**
  - ***Temporal sensitive (window of validity) data/operations***
  - ***Representation of time and temporal relationships***
  - ***Correct temporal ordering of requests/data***
  - ***Temporal coherence of data/requests from different sources***
  - ***Temporal conditions in work flow***
  - ***Accuracy of global temporal views***
  - ***Remember the impact of fault tolerance on temporality***

Range of Timeliness Needs



Enterprise cf. Real Time

Criteria for real-time systems differ from that for time-sharing systems.

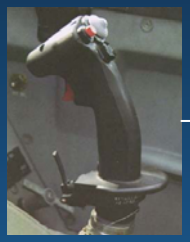
	Time-Share Systems	Real-Time Systems
Capacity	High throughput	Schedulability
Responsiveness	Fast average response	Ensured worst-case latency
Overload	Fairness	Stability

- *Schedulability* is the ability of tasks to meet all hard deadlines.
- *Latency* is the worst-case system response time to events.
- *Stability* in overload means the system meets critical deadlines even if all deadlines cannot be met.

Generic RTE Architecture

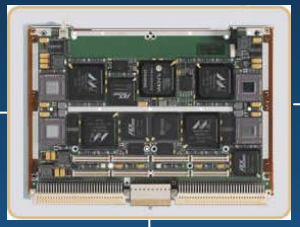
Pilot Commands

HOTAS



MFD & Display Computer

Avionics Mux BC



Avionics Computer

PPC 750's Or Higher

Common Processing Environment

On-board Processing

Appl. | Threats | Appl. | Appl. | ...

RT-CORBA

Real-Time OS

Device Drivers

Avionics Mux

LOS

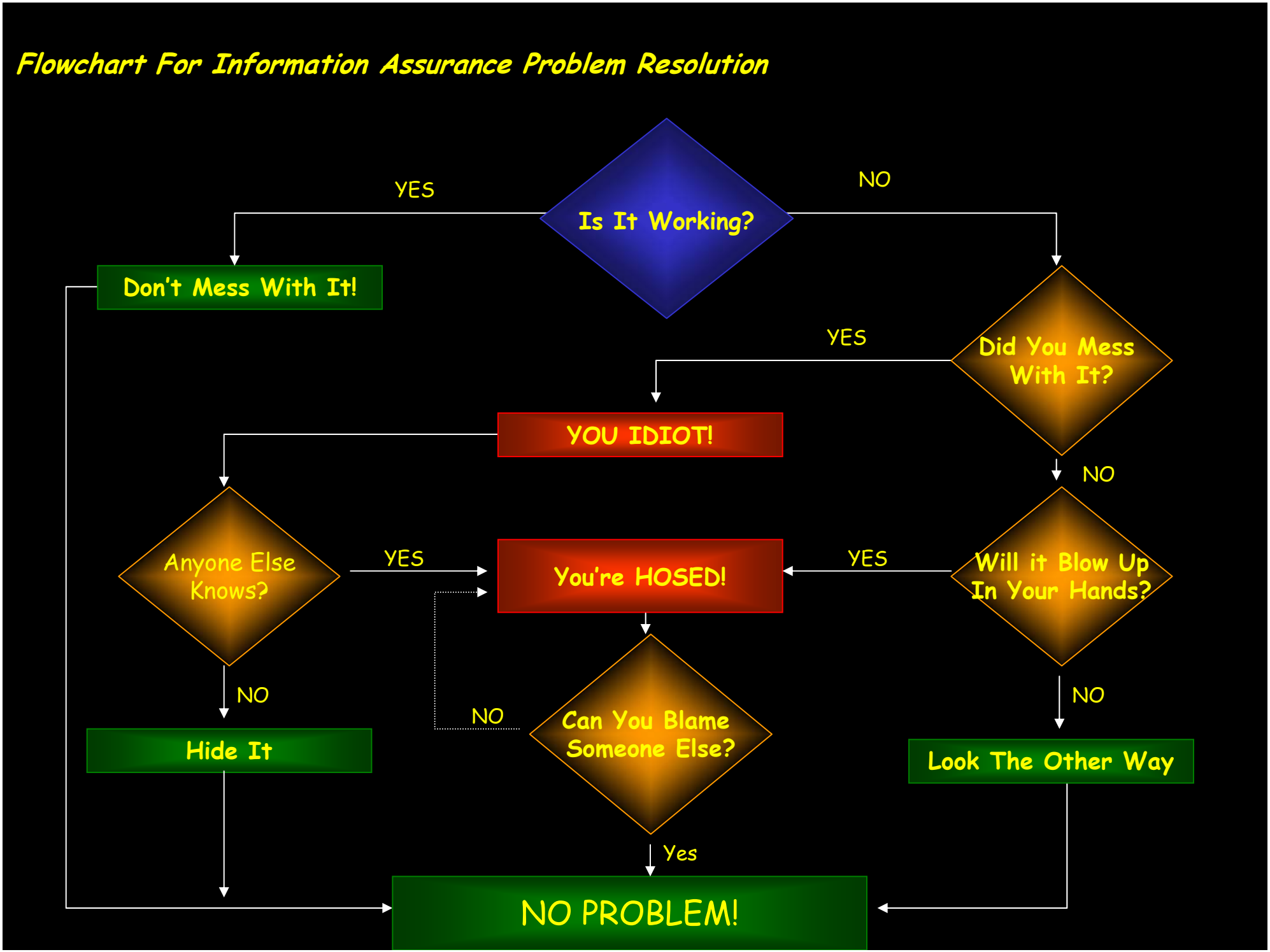
Line-of-Sight Data Link

BLOS

Beyond-Line-of-Sight Data Link

Why Security in Commercial Embedded Systems?

- **IEEE Computer Magazine, Jan 2006, "Security of Critical Control Systems Sparks Concerns"**
  - ***Slammer attacked Davis-Besse Nuclear Power Plant Safety Monitoring System: Nov 2003***
    - Network protected but contractor used modem (with Infected PC) : not contractor deliberate
  - ***Dept of Interior computer in Portland, OR, gaining access over computers controlling every dam in Northern California: Early 1990's***
  - ***Amundsen-Scott South Pole Station's Life Support System: 2003***
  - ***Sewage & Water treatment plant in Queensland, Austrailia: 2000***
    - "SCADA vs. the hackers", *Mechanical Engineering*, December 2002
- **Alan Paller, Director of Research, SANS Institute:**
  - ***"We will never know about most of the break-ins because the victims will never tell the public!"***


Flowchart For Information Assurance Problem Resolution
Is It Working?
YES
NO
Don't Mess With It!
Did You Mess With It?
YES
YOU IDIOT!
NO
Anyone Else Knows?
YES
You're HOSED!
YES
Will it Blow Up In Your Hands?
NO
Hide It
NO
Can You Blame Someone Else?
NO
Look The Other Way
Yes
NO PROBLEM!

Safety Assurance

- **Reliability, Availability, Dependability, etc**
- **The Safest Car in the World**
  - ***Safety is not necessarily achieved by these "…ilities"***

The C-I-A Triad

- ***There is no perfect security!!!***
- ***Only levels of Trust or Assurance!***

- **CIA**
  - ***Confidentiality - means that secret or private information remains that way.***
  - ***Integrity - refers to the completeness, correctness, and trustworthiness of the information***
  - ***Availability - means the authorized persons may access the information in a timely manner.***

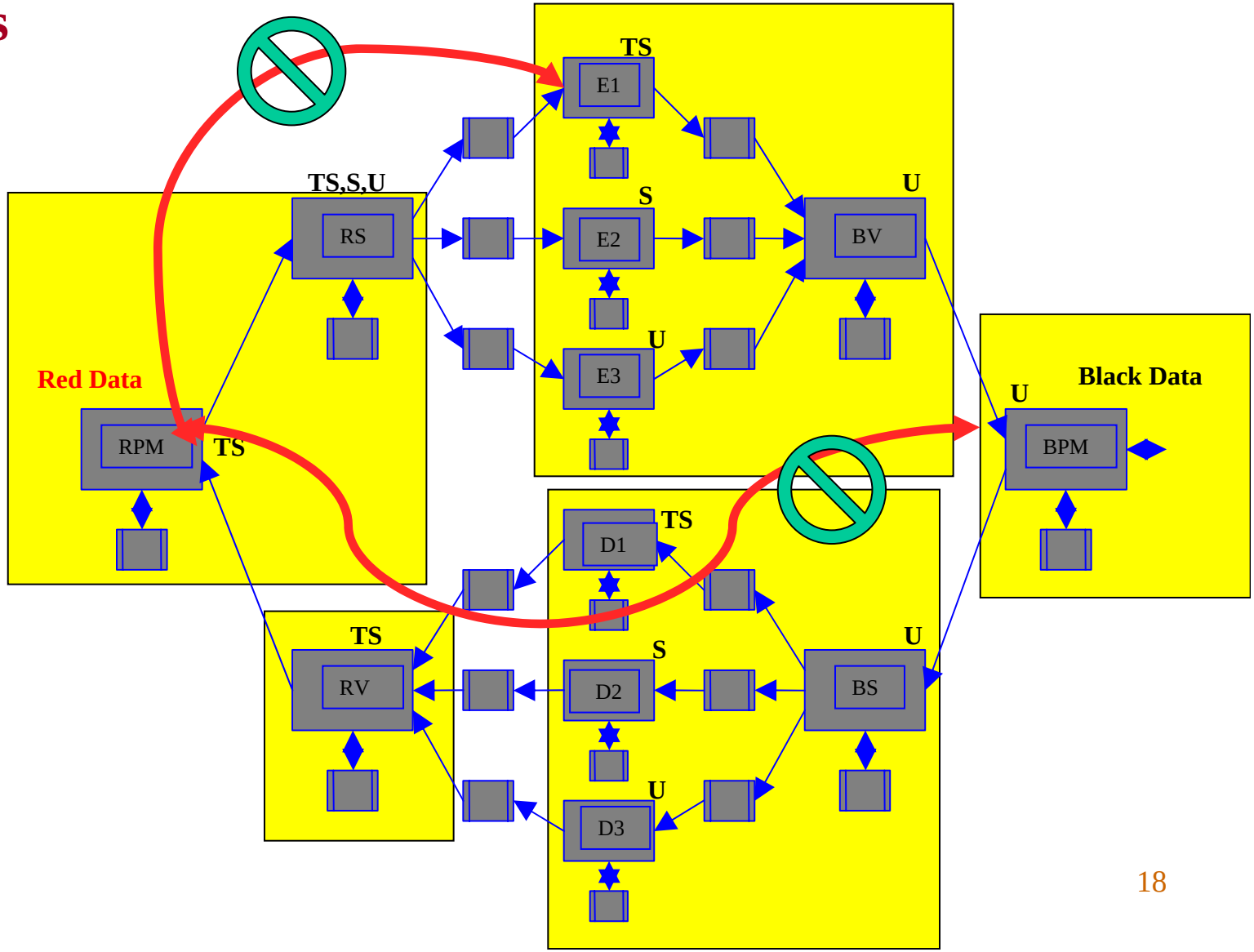
Foundational Threats

- Software can only be as secure as its foundation
- If the foundation can be successfully attacked, then any system security function that runs on that foundation can easily be rendered ineffective
- Foundational threats include:
  - Bypass
  - Compromise
  - Tamper
  - Cascade
  - Covert Channel
  - Virus
  - Subversion

Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

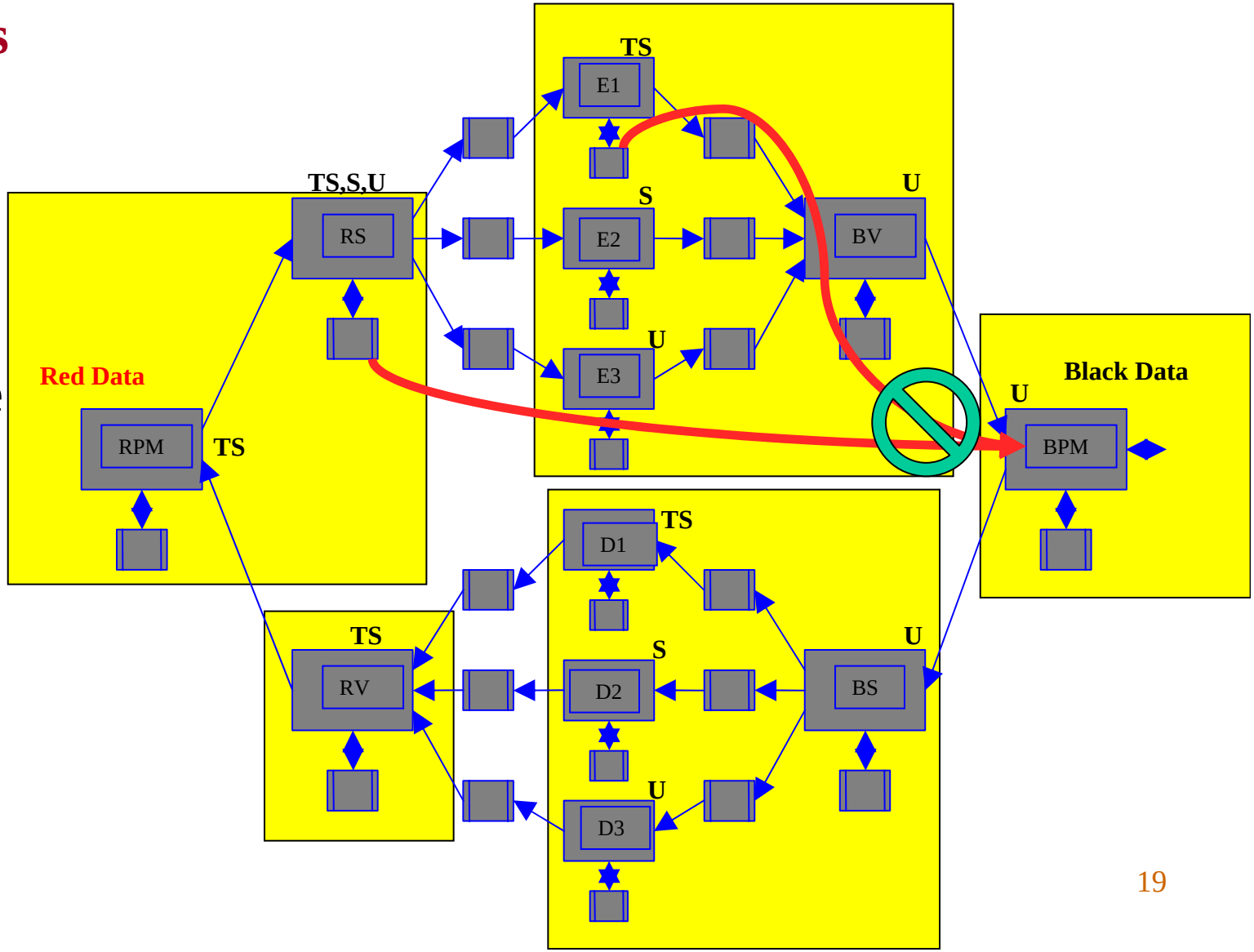
- ✓ **Bypass**
- ✓ **Compromise**
- ✓ **Tamper**
- ✓ **Cascade**
- ✓ **Covert Channel**
- ✓ **Virus**
- ✓ **Subversion**



Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

- ✓ Bypass
- ✓ **Compromise**
- ✓ Tamper
- ✓ Cascade
- ✓ Covert Channel
- ✓ Virus
- ✓ Subversion

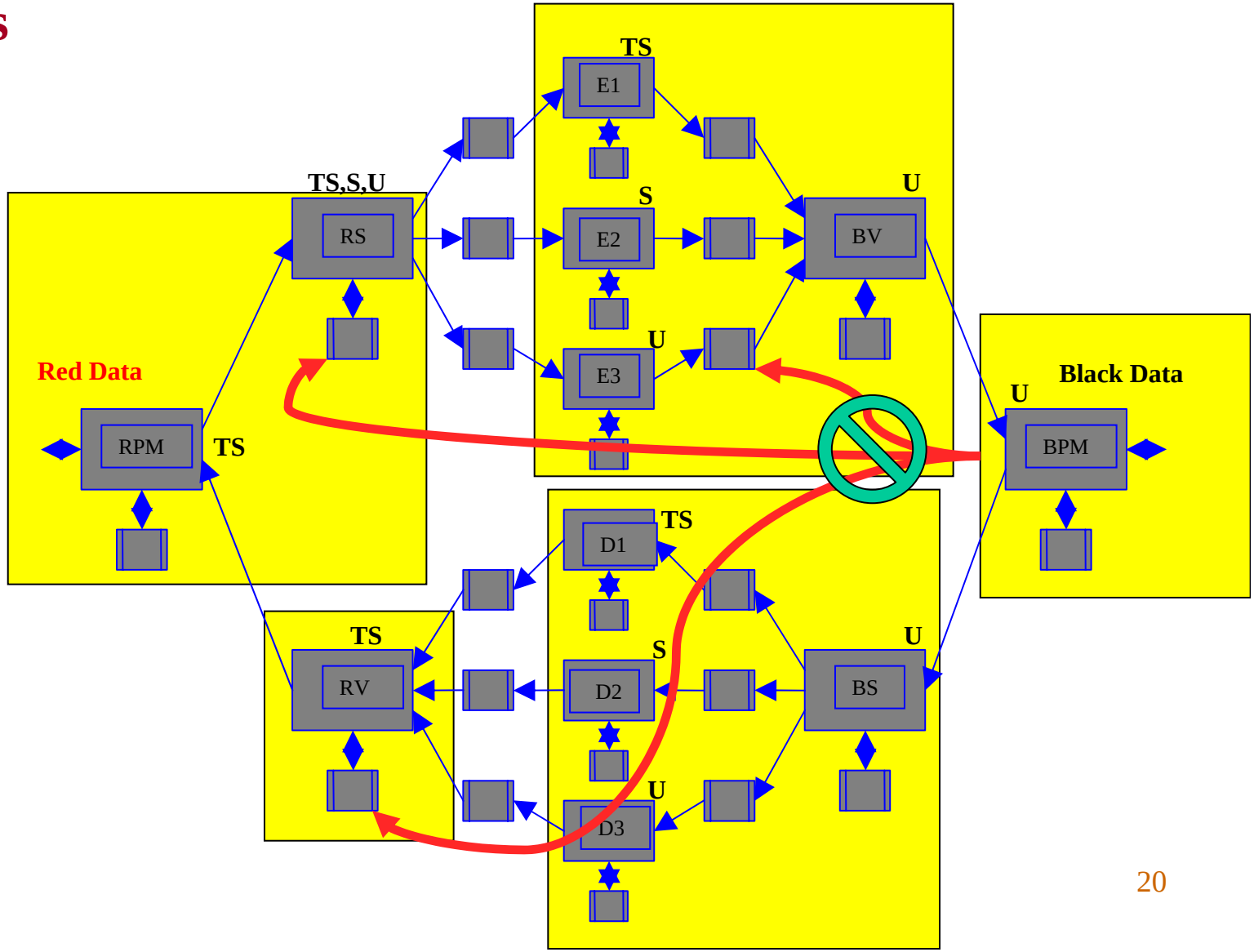


Foundational Threats
(That MILS Protects Against)

U.S. AIR FORCE

MILS provides mechanisms to counter Foundational Threats

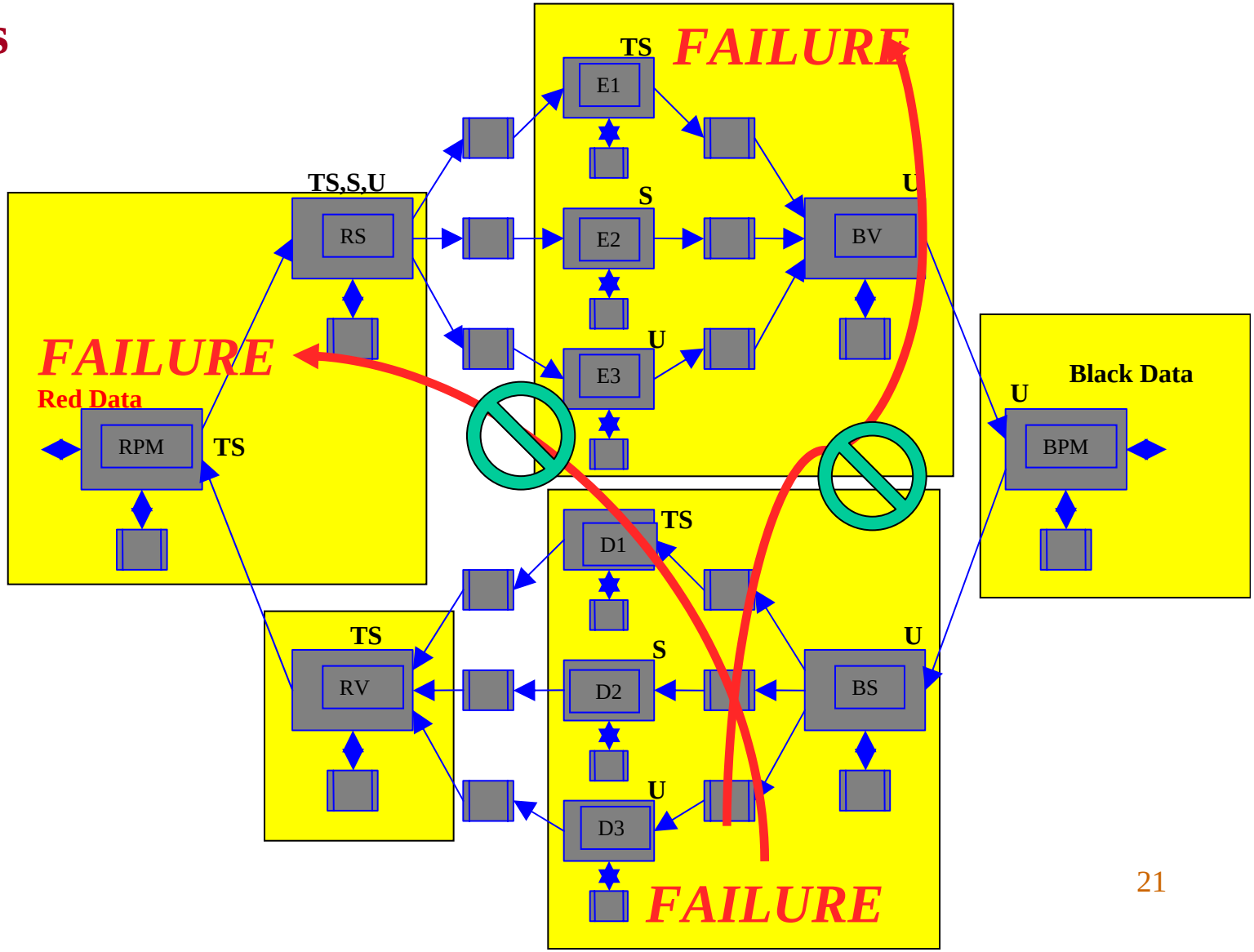
- ✓ Bypass
- ✓ Compromise
- ✓ **Tamper**
- ✓ Cascade
- ✓ Covert Channel
- ✓ Virus
- ✓ Subversion



Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

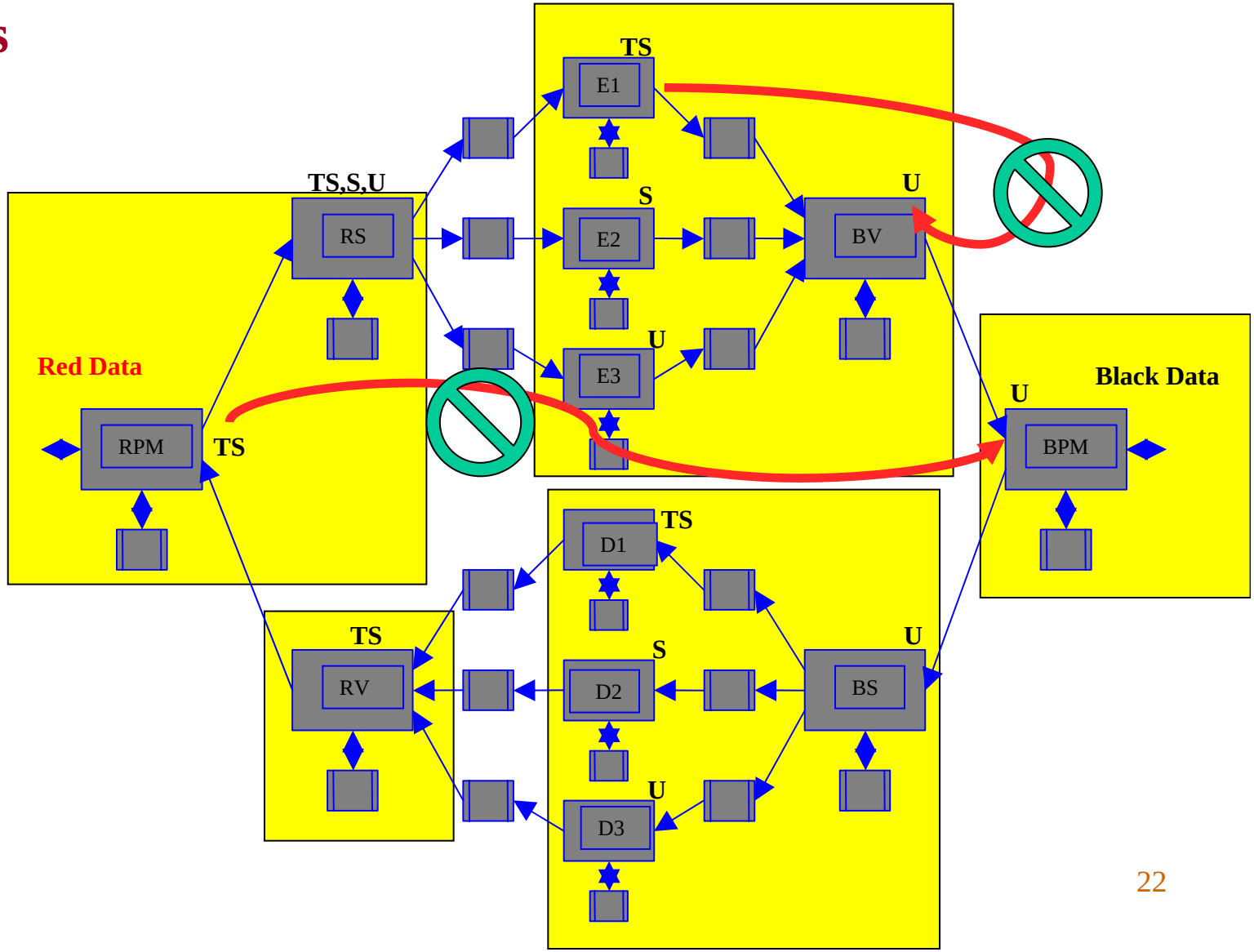
- ✓ Bypass
- ✓ Compromise
- ✓ Tamper
- ✓ **Cascade**
- ✓ Covert Channel
- ✓ Virus
- ✓ Subversion



Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

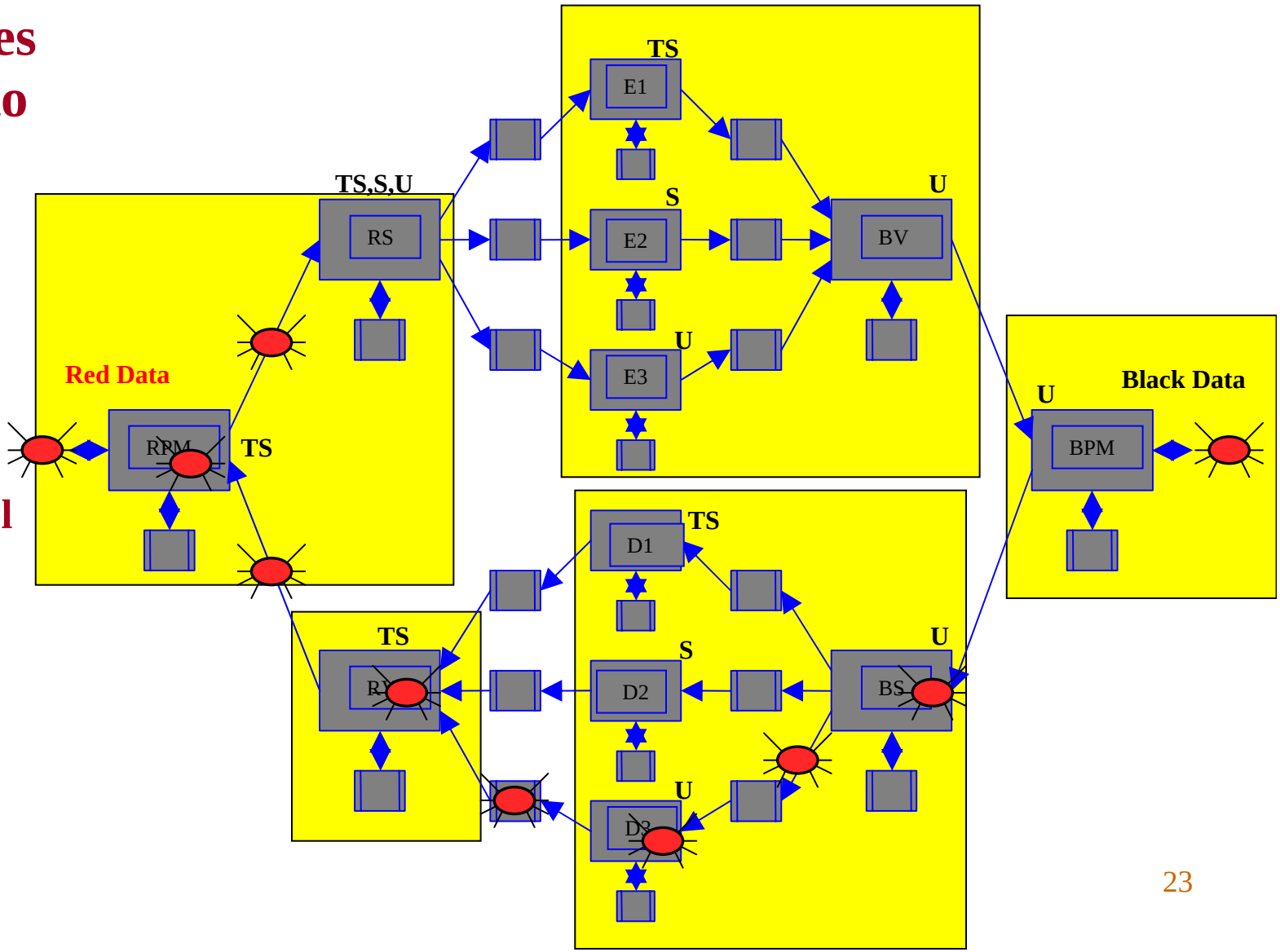
- ✓ Bypass
- ✓ Compromise
- ✓ Tamper
- ✓ Cascade
- ✓ Covert Channel
- ✓ Virus
- ✓ Subversion



Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

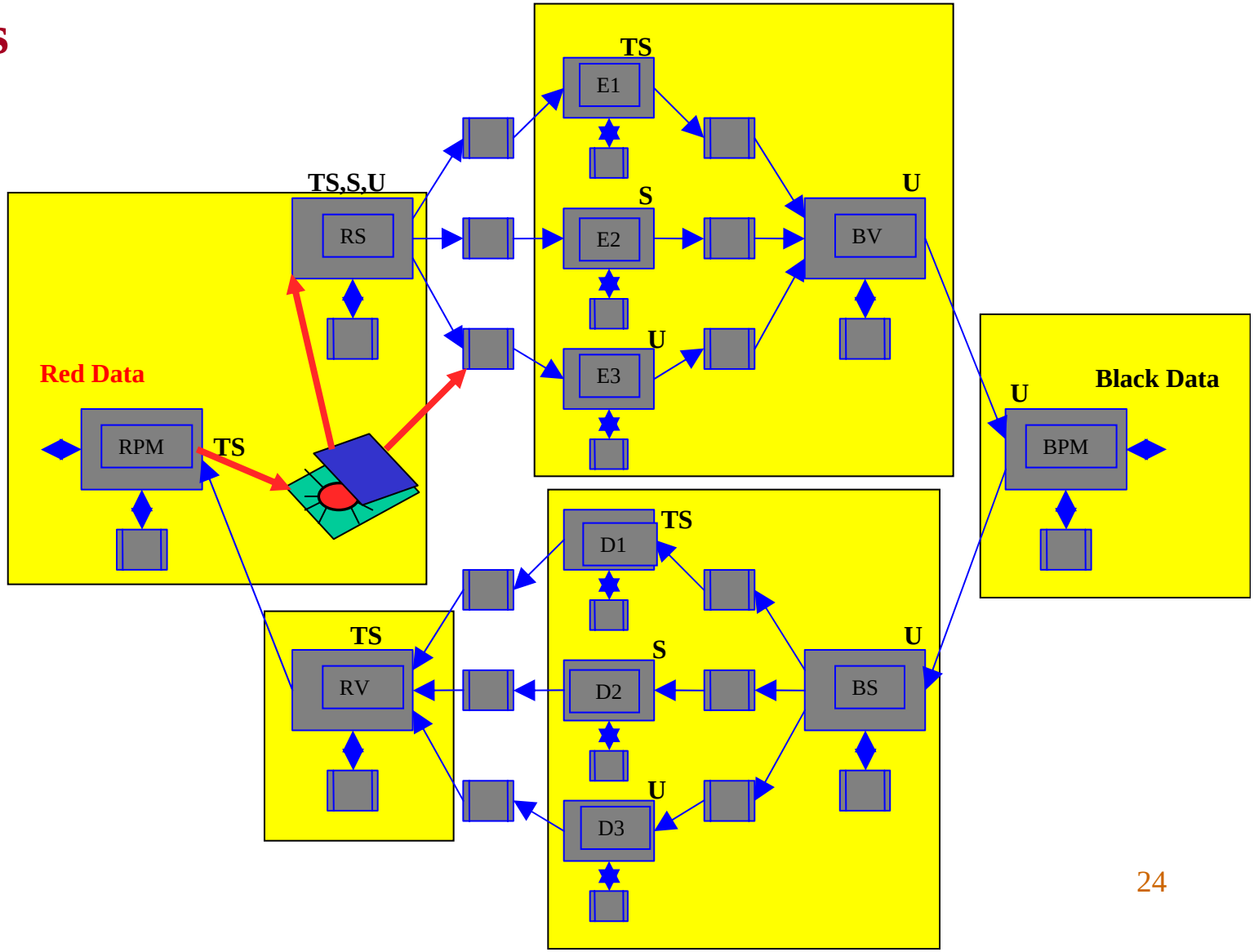
- ✓ Bypass
- ✓ Compromise
- ✓ Tamper
- ✓ Cascade
- ✓ Covert Channel
- ✓ **Virus**
- ✓ Subversion



Foundational Threats
(That MILS Protects Against)

MILS provides mechanisms to counter Foundational Threats

- ✓ Bypass
- ✓ Compromise
- ✓ Tamper
- ✓ Cascade
- ✓ Covert Channel
- ✓ Virus
- ✓ **Subversion**

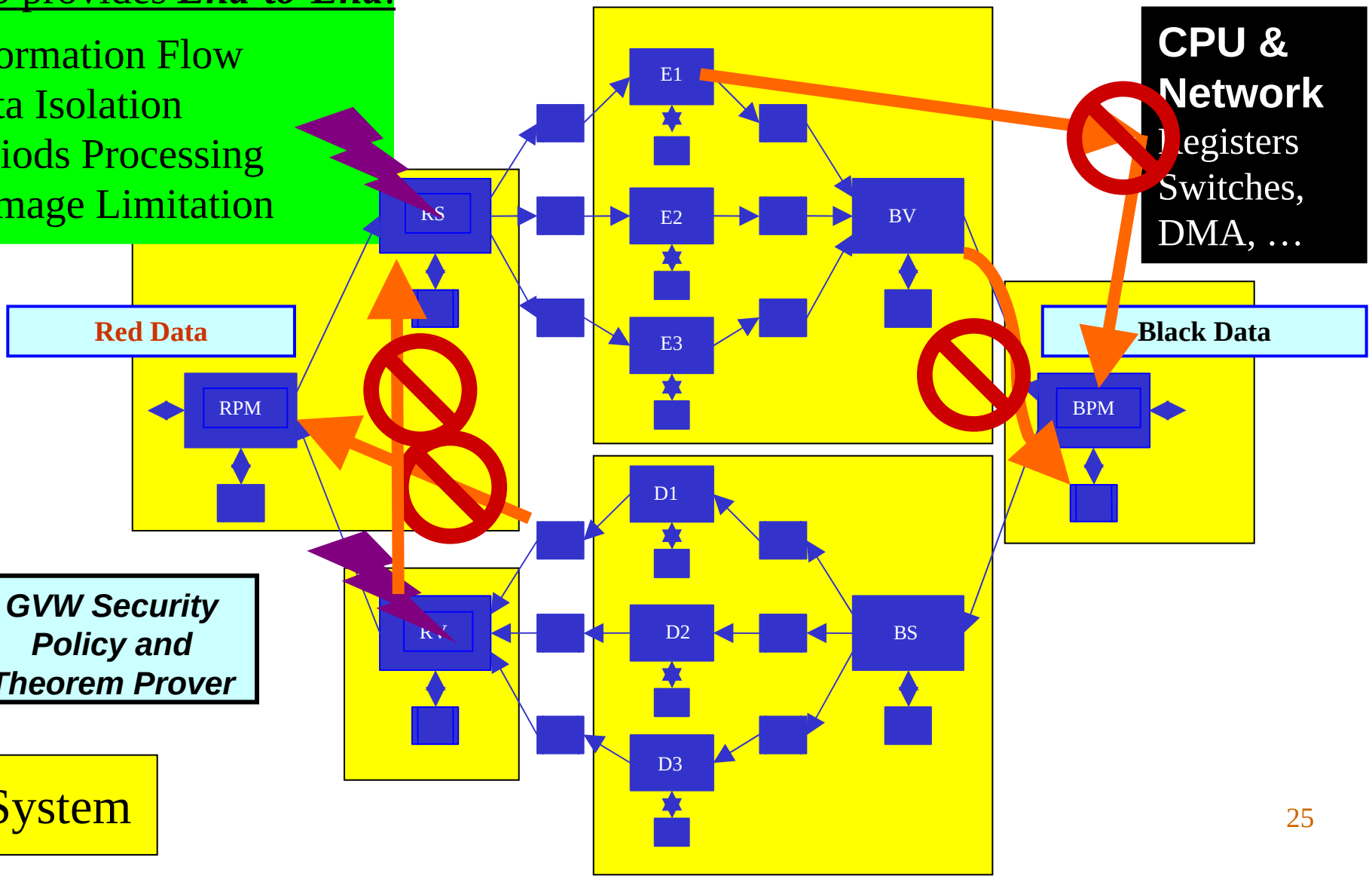


MILS PCS / CORBA / DDS Network Security Policy Example

Policy Enforcement Independent of Node Boundaries

MILS provides ***End-to-End***:

- Information Flow
- Data Isolation
- Periods Processing
- Damage Limitation



Processing Architecture Objectives

1) Layered Commercial Open System Standards

Enables HW Ease-Of-Change

2) Hardware / Software Change Isolation

Enables Proactive Technology Refresh

3) Modular, Portable Application Software

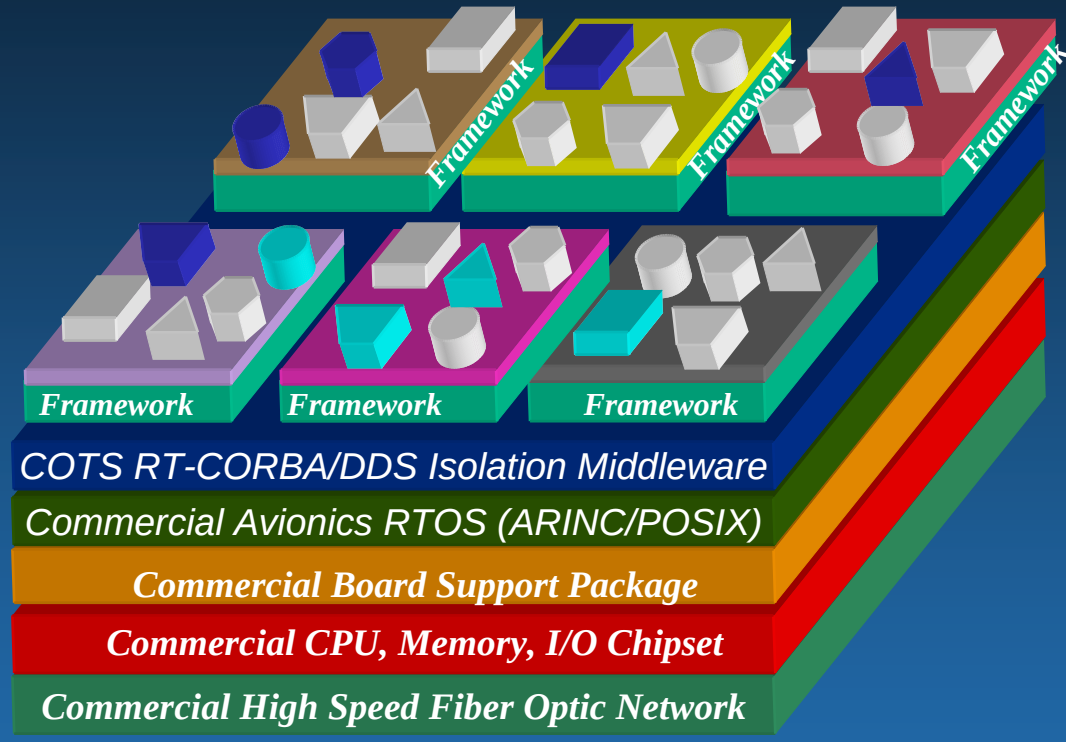
Domain Engineering & Object Oriented Design to Enable Software Reuse

4) High-Speed Network

Enables Distributed Processing

5) Common Processing H/W S/W Modules

Shared Cost … Economies of Scale



COTS H/W & S/W Infrastructure ➔ Commodity Pricing

Processing Architecture Objectives

NIAP Certified COTS Products are Needed

6) Task Scheduling

"Hard Real-Time" Processing Constraints Met Across Distributed Processors

7) Common Criteria COTS Data Security

Ability to Separate Processing at Multiple Levels of Classification or Safety Criticality

8) Programmable Communications

Ability to Interact within SoS

- Rapid Insertion of the Latest Commercial Technology … Continuous Modernization
- Makes DMS Transparent to Customer

How to work with COTS

- **The correct way for DoD (and primes) to use commercial technologies is to fund partner vendors to achieve necessary DoD capabilities that:**
  - ***Based on Open Standards or Specifications***
  - ***Make long term business sense to the vendor***
  - ***Are commercially sustainable through sales of product***
  - ***Meet specific needs of more than one program***
    - AND
  - ***DoD ASSUMES NO OWNERSHIP!!!!***
    - Intellectual Property rights are retained by the vendor.
    - Gov't Limited Use Rights

NSTISSP #11 (National Security Telecommunications and Information Systems Security Policy)

- National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
- IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information.
- Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products
  - *Limited only to those evaluated and validated via NIAP or FIPS*
  - *Initially interpreted to mean Desktop IT Centric Systems*
- Latest direction includes DoD Platforms

"The appropriate certification routing for Commercial Products for use in DoD systems is through a NIAP lab under Common Criteria. NSA does not certify products, the NIAP labs do.", July 2004

-- Mike Fleming, Deputy Director IAD

" NO WAIVERS!" : DHS-OSD Software Assurance Workshop, Oct 3, 2005

-- Daniel Wolf, Director IAD,

- http://niap.nist.gov/cc-scheme/nstissp11_factsheet.pdf

Evaluation and C&A Processes

- **Product Assurance**
  - ***Common Criteria Evaluation & Validation Scheme (CCEVS)***
    - Administered by the National Information Assurance Partnership (NIAP)
    - Evaluation activities executed by Common Criteria Testing Laboratories (CCTLs)
    - Evaluation oversight provided by NIAP representatives (Validators)
- **System Assurance**
  - ***DoD Information Technology Security Certification & Accreditation Process (DITSCAP)***
    - Process executed by the Program Manager leading a team that includes
      - *Designated Accreditation Authority (DAA)*
      - *Certifier and certification team(s)*
      - *User Representative*
  - ***Commercial via CIP and the CISSP personnel***

Key High Robustness Assurance Properties

- **Confidence that Trusted Security Functions (TSF) are**
  - ***Non-bypassable***
  - ***Evaluatable in regards to design/implementation***
  - ***Always invoked***
  - ***Tamper-proof***
- **Mathematical Verification of security policy model and external interfaces**
- **Reduction of size and complexity of the TSF**
- **Modular/layered approach to s/w component development, evaluation, integration**

MILS Concept Objectives

- At the component level
  - *Accommodate trusted components evaluatable to the level of high robustness*
    - *Reduce the amount of security critical code*
    - *Increase the scrutiny of security critical code*

What is the MILS Architecture?

- **A "layered" architecture concept targeted at enabling the composition of system properties from trusted components**
  - ***Layered functionality & assurance***
- **Defines 4 conceptual layers based on the 3-level Rushby* architecture (*John Rushby, PhD)**

1. Separation Kernel & Hardware (single node)

2. Distributed Communication (multiple nodes)

3. Middleware Services (single node)

4. Trusted Applications (as required) (single node)

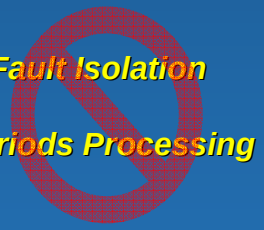
Orange Book Approach

Monolithic Applications

Monolithic Application Extensions

User Mode

MLS Requires Evaluatable Applications!



Kernel

Network I/O

DAC

MAC

File systems

Information Flow

Data isolation

Device drivers

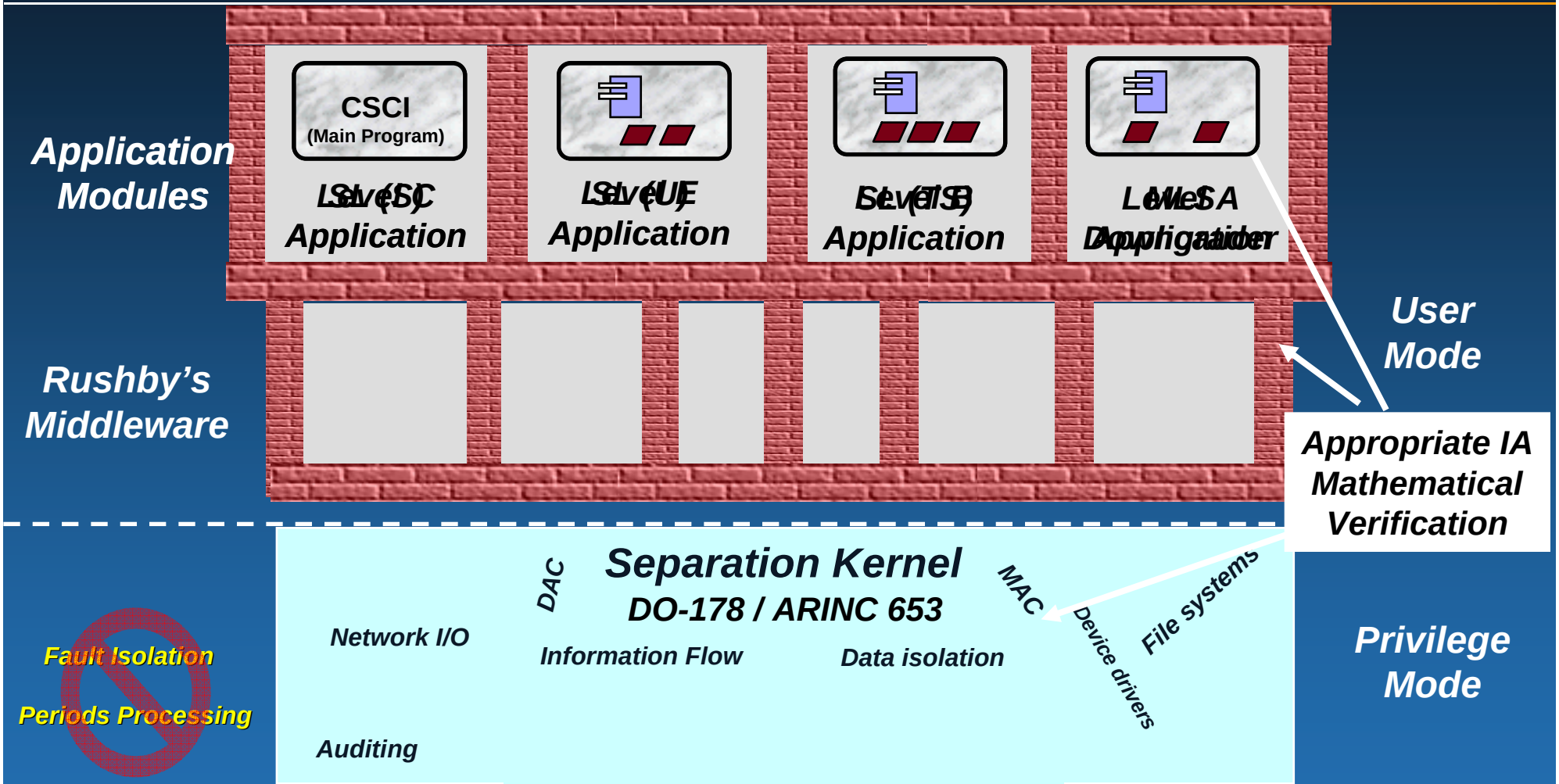
Auditing

Monolothic Kernel

Privilege Mode

Too Large to fully Evaluate!!!

MILS Architecture Evolution



Evaluated Applications on an Evaluated Infrastructure

MILS Separation Kernel Security (High Assurance)

High Assurance Kernel

- ***Remove RTOS Services, e.g., Device Drivers, File System***
- ***Develop Formal Methods Artifacts***

Separation Kernel Functionality (ARNIC 653), i.e.

- ***Time and Space Partitioning***
- ***Data Isolation***
- ***Inter-partition Communication***
- ***Periods Processing***
- ***Minimum Interrupt Servicing***
- ***Semaphores***
- ***Timers***
- ***Instrumentation***

<u>And NOTHING else!!!</u>

Middleware Functionality, e.g.

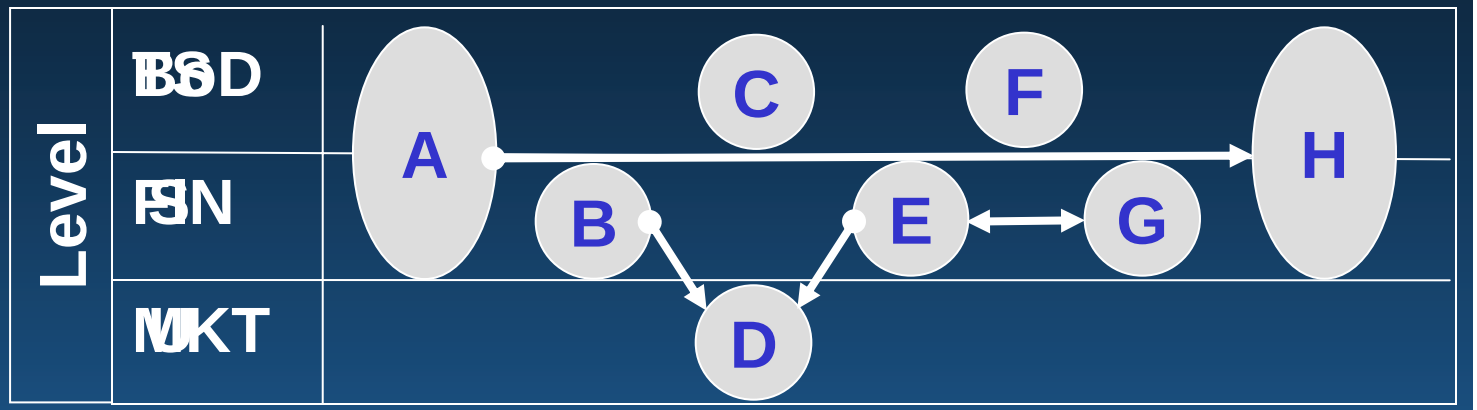
- OS Services
- MLS Virtual Device Drivers
- Inter-processor Communication **(PCS)**
- MLS Rapid-IO / ASM-NIU
- MLS RT-CORBA/DDS/Web Services, etc.
- MILS IPv6
- MLS File System
- MAC / DAC

Middleware Security Policy

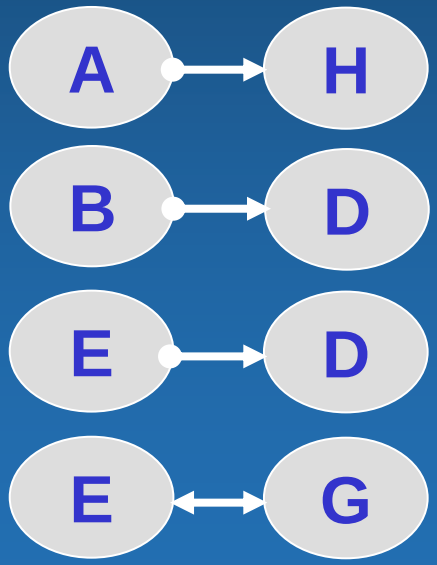
- End to End Information Flow
- End to End Data Isolation
- End to End Damage Control, Detection, Isolation, Recovery

Flow Policy Enforcement: User and Separation Kernel View

The user view of the Operational Policy to be enforced …



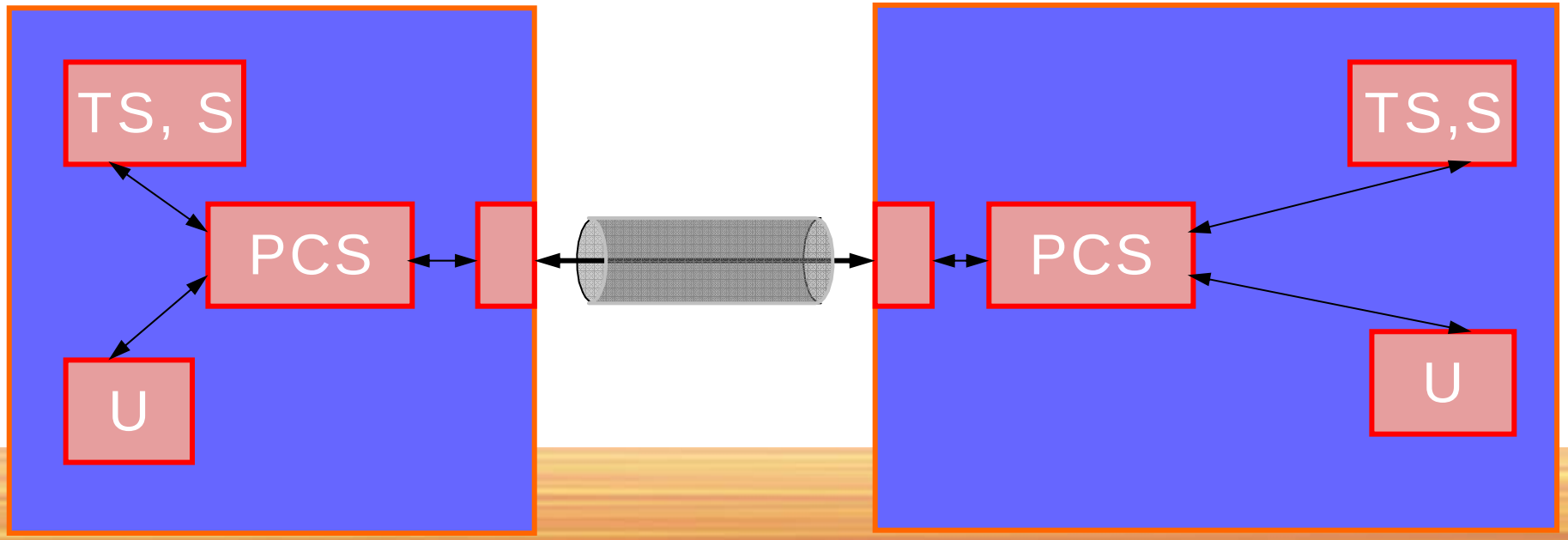
… what the Separation Kernel enforces …



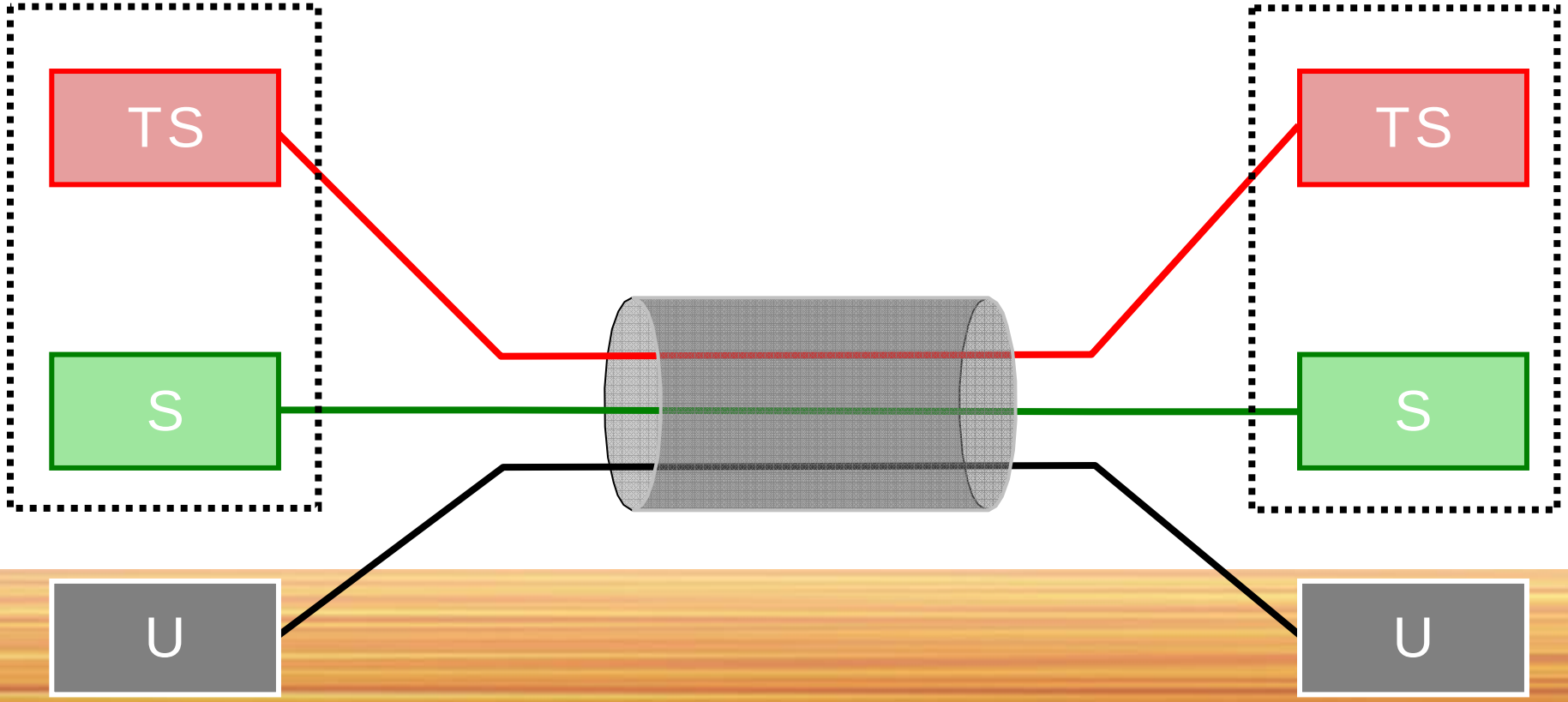
Distributed Communication Objectives

- Extend single node security policies to multiple nodes
  - Information Flow
  - Data Isolation
  - Resource Sanitization
  - Damage Limitation

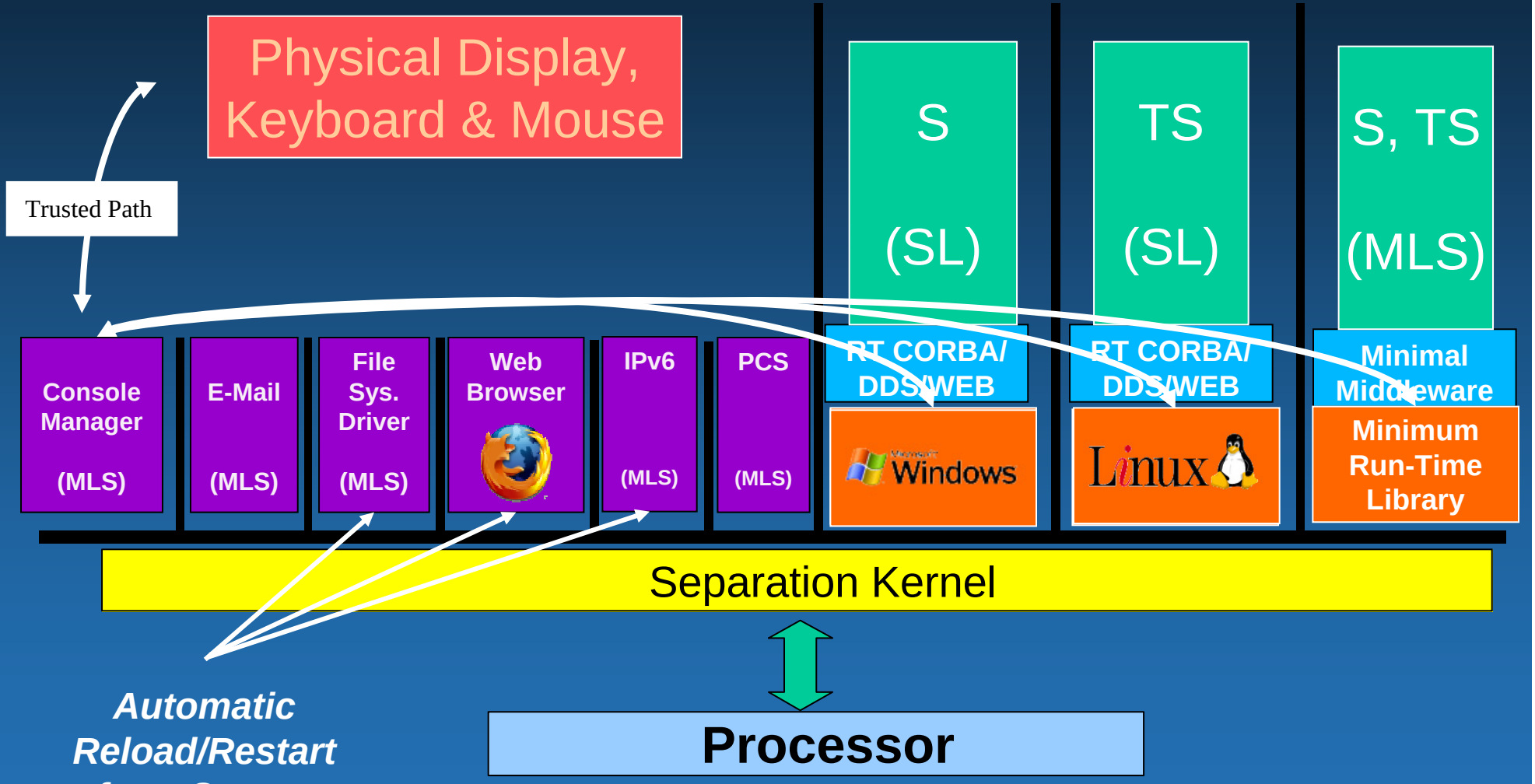
  … while preserving single node properties of the SK
- **NEAT** distributed communication Reference Monitors


TS, S
PCS
U
PCS
TS,S
U

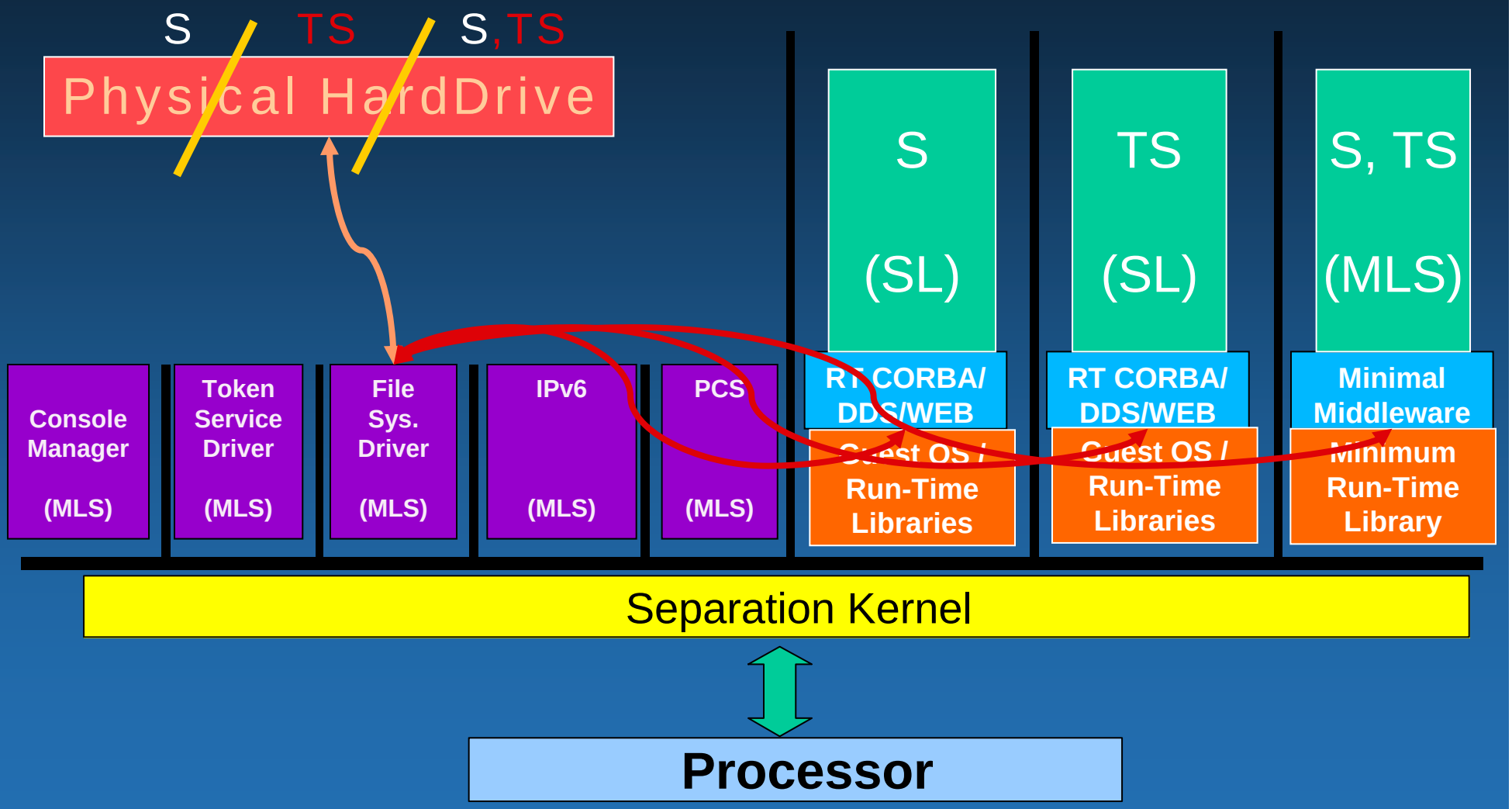
Partitioned Channel View Inter-node Communication



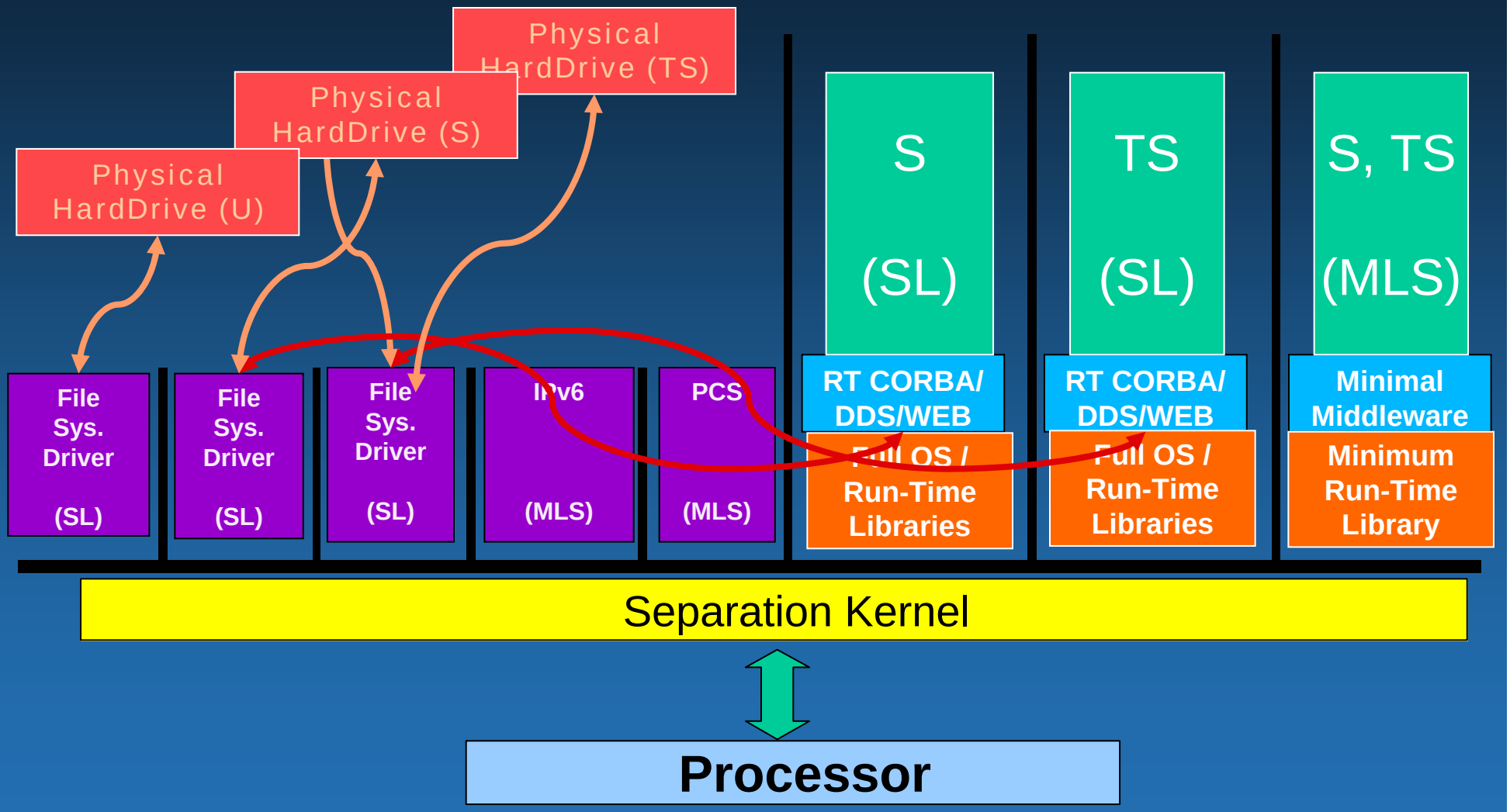
MILS Workstation: with Guest OS



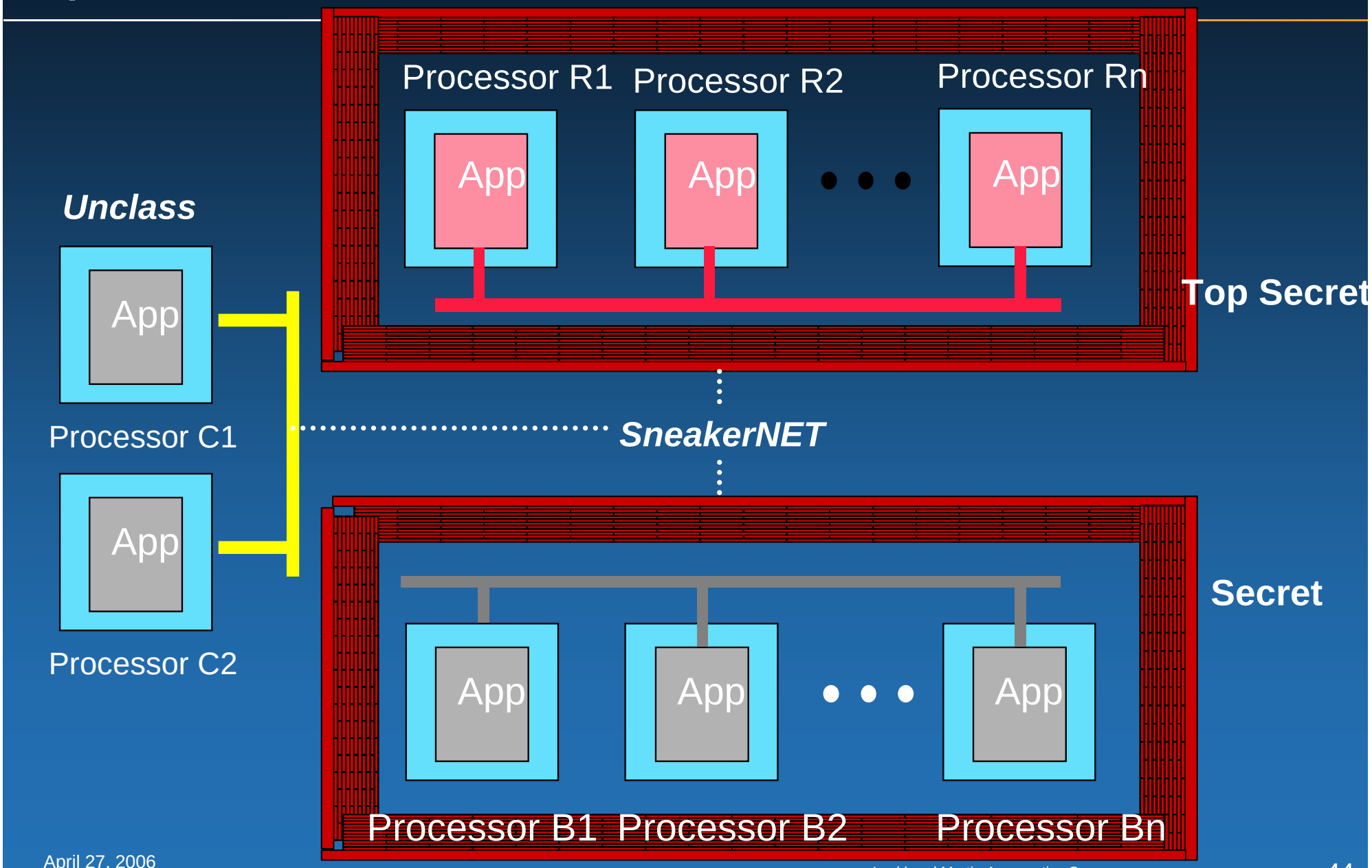
MILS Server: Disk Access (MLS Disk)



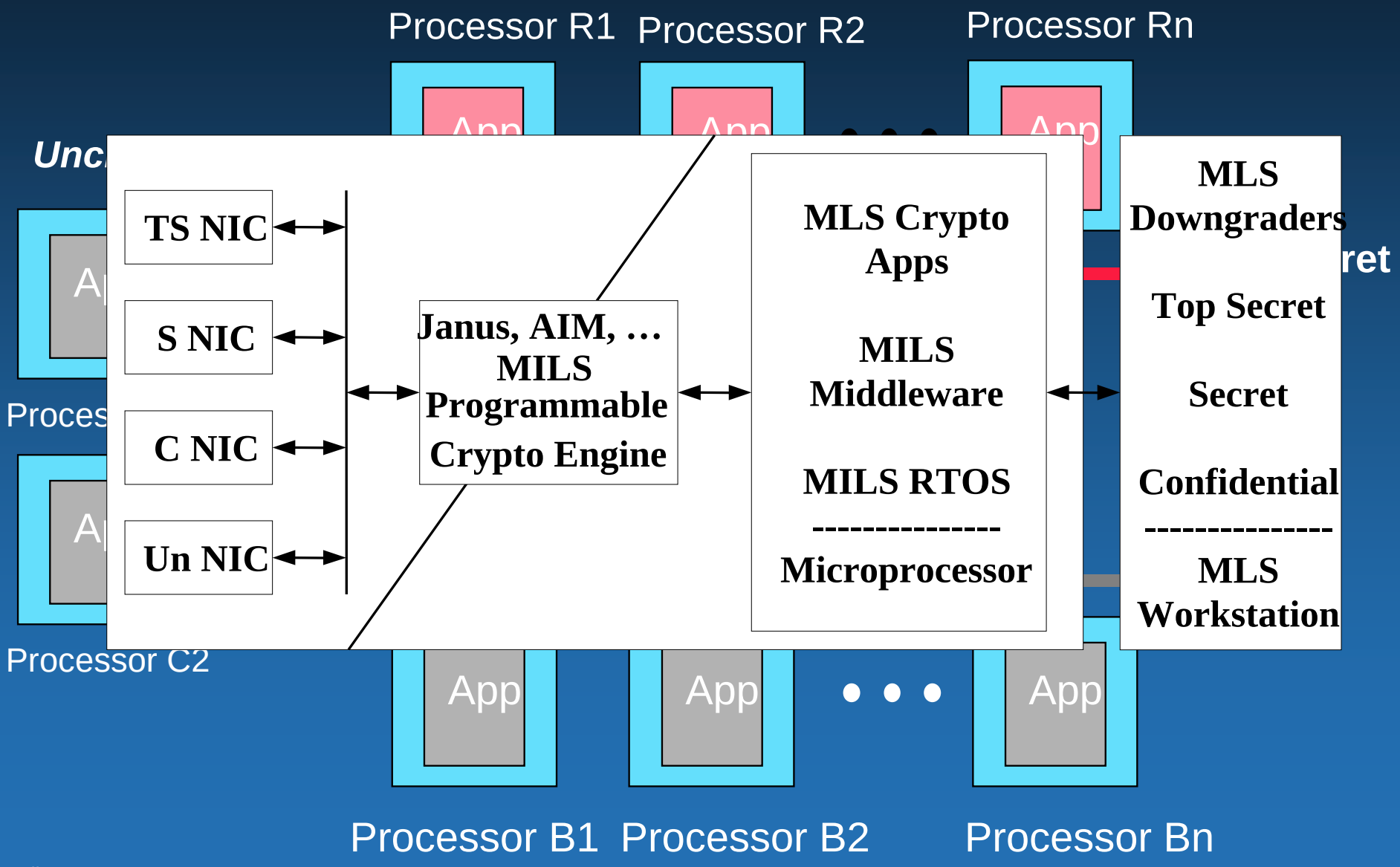
MILS Server: Disk Access (MLS Disk)



Current Security/Safety is Physical



Legacy Systems Don't have to be Rebuilt!!!



Component PP's for MLS Workstations

MLS Server		MLS Desktop	
MLS Applications - Web Server, Guard, etc.		MILS DownGrader	MILS CORBA/DDS
MLS Filesystem	MLS Networking – IPv6	MLS Console - Trusted Path	
MILS Rapid IO	Validation Mechanism MAC, DAC, Roles, Priviledges	MLS Resources - Devices, Pseudo-devices	
POSIX Interfaces and Libraries		PCS	
Separation Kernel - Isolation, Explicit Information Flow, Messages, Shared Mem, Synchronization			
Hardware - MMU, Supervisor Mode, Privileged Instructions			

Product Cert Underway | Profiles In Public Review | Profiles to Public Review

Questions?

- **Dr. Ben Calloni**
  - ***Lockheed Martin Aeronautics Company***
  - ***Fort Worth,TX***
  - ***ben.a.calloni@lmco.com***
  - ***817-935-4482***

  - ***OMG RTESS Task Force Chair***
  - ***OMG Board of Directors***
  - ***Open Group Board of Directors***