aesec™

The power of verifiable protection™

Dramatically Reducing Attack Surface Using Integrity MAC Security Kernel

Dr. Roger R. Schell, PhD
President and founder of Aesec Corporation
roger.schell@aesec.com
(831) 657-0899

CERIAS 2020 Seminar
Purdue University
West Lafayette, IN
Streamed live on the Web
September 2, 2020
4:30pm EDT

Presentation Outline

- Problem: national existential risk

- Towards a Reusable Trusted Device (RTD)

- Control Systems: PLC Commercialization

Presentation Outline

aesec™

- **Problem: national existential risk**
  - Poor Cyber Physical Systems (CPS) resilience
  - Vulnerable critical cyber-physical components
- Towards a Reusable Trusted Device (RTD)
- Control Systems: PLC Commercialization

National Existential Risk
Poor CPS Resilience

- Leon Panetta, former SecDef & CIA Director
  - "Biggest nightmare is of a computer virus
    - that attacks and disables US infrastructure"
  - "Could result in millions of lost lives" [Mar 2019]
- EO 13920 – US Bulk Power: National Emergency
- National Commission on Grid Resilience (NCGR)
  - "OEMs are targets for malware that can lie in wait"
  - Cyberthreat electric sector investment [Aug 2020]
- Washington Post – "Power Grid Collapse"
  - "Russia cause[d] physical damage from afar"
  - "China has already implanted malware" [Aug 2020]

National Existential Risk
Critical Device **Physical** Damage

- Computer systems all use operating system(OS)
  - Programmable Logic Controllers (PLC) have an OS
- Science: secure system requires trustworthy OS
  - Must withstand witted adversary cyber attacks
- Current commercial PLCs use untrustworthy OSs
  - One of a few common OSs – none trustworthy
  - Evident by stream of regular "security patches"
- Cyberattacks inflict permanent physical damage
  - STUXNET destroyed Iranian enrichment centrifuges
  - Crash Override for physical Ukraine grid destruction
  - Triton aimed for Saudi refinery destruction

Presentation Outline

aesec™

- Problem: national existential risk

- **Towards a Reusable Trusted Device (RTD)**
  - Security kernel technology
  - Verifiable Integrity Mandatory Access Control (MAC)
  - OpenPLC on GEMSOS demonstration
  - Mature subversion mitigation

- Control Systems: PLC Commercialization

Security Kernel Technology
Solution Concept Introduction

aesec™

- Seminal (1972) concept description
  "*a compact security 'kernel' of the operating system and supporting hardware – such that an **antagonist could provide the remainder** of the system without compromising the protection provided.*"
- Early (1983) IEEE article characterization
  "*the security kernel approach provides controls that are effective against most internal **attacks** – including some that many **designers never consider**.*"
- Consistent history of mitigating attacks
  "*half dozen security kernel-based operating systems ran for years (even decades) in the face of nation-state adversaries **without a single reported security patch***"

Security Kernel Technology
Solution Concept Introduction

aesec™

"The only way we know . . . to build highly secure software systems of any practical interest is the kernel approach."

-- ARPA Review Group, 1970s (Butler Lampson, Draper Prize recipient)

Still true today. Codified in TCSEC Class A1

TCSEC Glossary: "***Security Kernel*** *- The hardware, firmware, and software elements of a Trusted Computing Base that* ***implement the reference monitor*** *concept."'*

Security Kernel Technology
Solution Concept Introduction

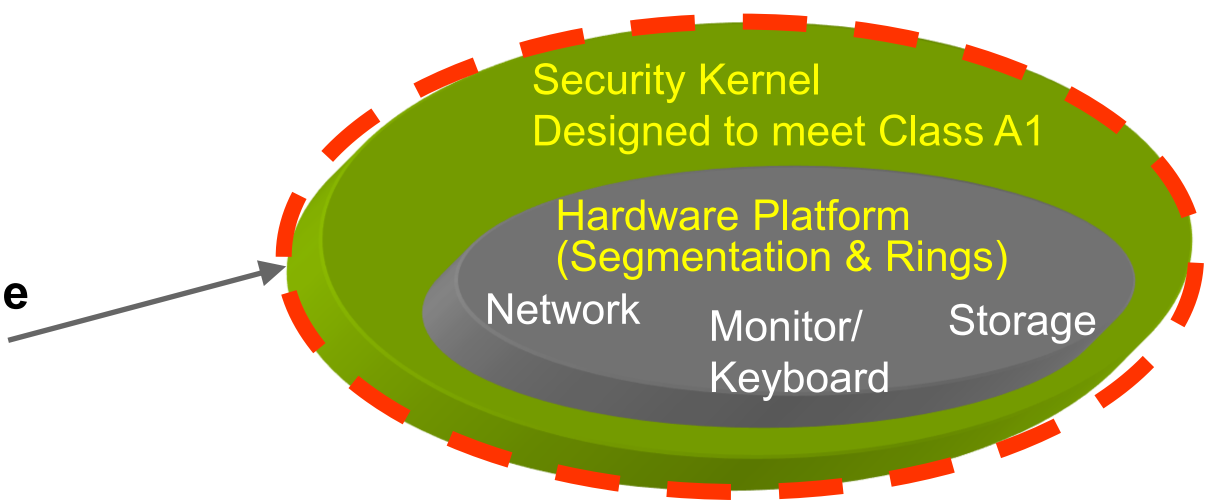
"The only way we know . . . to build highly secure software systems of any practical interest is the kernel approach."

-- ARPA Review Group, 1970s (Butler Lampson, Draper Prize recipient)

Still true today. Codified in TCSEC Class A1

> **Reusable Trusted Device**: "*The hardware, firmware, and software elements* ***implement the reference monitor*** *concept.*"

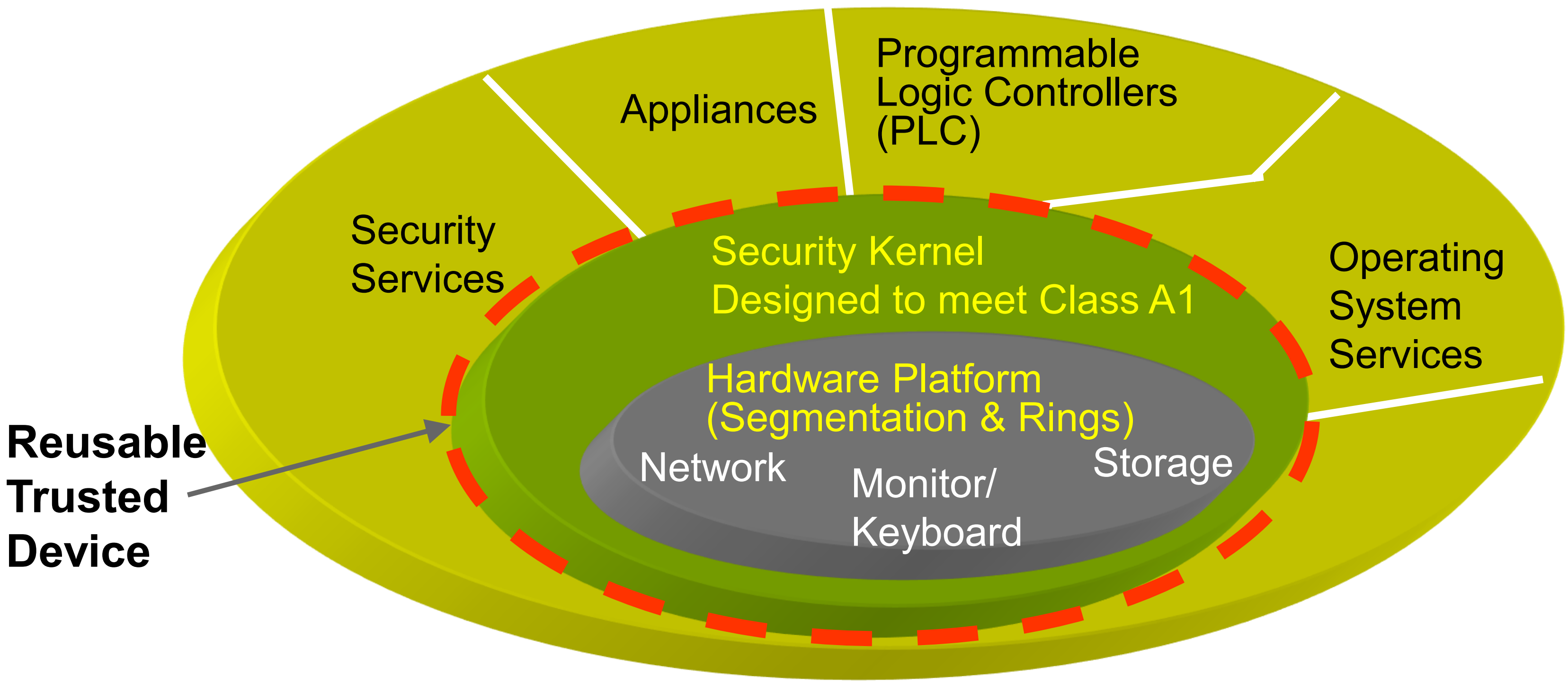
Reusable Trusted Device



Security Kernel Technology
Solution Concept Introduction

“The only way we know . . . to build highly secure software systems of any practical interest is the kernel approach.”

-- ARPA Review Group, 1970s (Butler Lampson, Draper Prize recipient)



Truly a paradigm shift: no Class A1 security patches for kernel in years of use

Security Kernel Technology
Strategic Approach to Protection

aesec™

- Controlled sharing between integrity domains
  - Enforce Mandatory Access Controls (MAC) policies
- Verifiable Design required for MAC enforcement
  - **Add on** security by test and analysis has failed
    - Threat/vulnerability detection & response never finish
  - **Build in** security by Construction is successful
    - Reference Monitor basis of the TCSEC Class A1 approach
- Mitigate subversion, e.g., malware (STUXNET)
  - To protect distribution of software & commands
    - Protect installed code, configuration settings & data

All required for Secure Operating System

Security Kernel Technology
Cyber Defense Triad

- MAC policies required
  - To secure information flows
- Reference Monitor
  - Only known <u>verifiable</u> protection technology
- Deal with Subversion
  - tool of choice for witted adversaries

Verifiable Design for MAC
NIST: Reference Monitor Concept

- NIST highlights in flagship SP-800-160v1
  - "Trustworthy Secure System Development "

- Reference Monitor Concept
  "*provides an abstract security model of the* ***necessary and sufficient*** *properties that must be achieved by any system mechanism claiming to securely enforce* ***access controls****.*"

- Security Kernel **defined** as its implementation

- Integrity-MAC is access control policy

Verifiable Design for MAC
Secure by Construction

Mappings

E.g., Hardware Segmentation

System Specifications
- Security Policy
  - Philosophy and Design of Protection
- Formal Security Policy Model **[linchpin]**
  - (**FSPM**) For Reference Monitor. i.e., security kernel API

Development Specifications
- Formal Top Level Level Spec (FTLS)
  - With hardware properties visible at interface
- Descriptive Top Level Spec

Product Specifications
- Implementation Design Documents
  - Source Code
  - Layering & info hiding
  - Code correspondence
  - Covert channel analysis

Deliverable Product
- Product End Item
  - Trusted Distribution
  - Security Features Users Guide
  - Trusted Facility Manuals

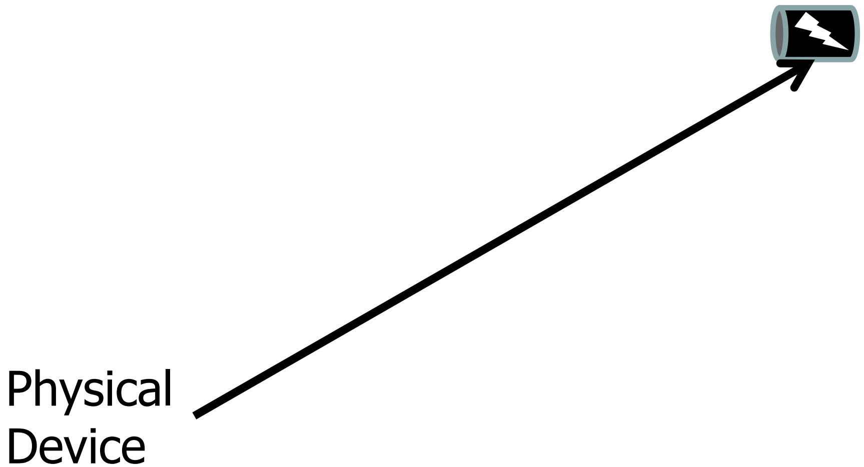
Verifiable Design for MAC
Ineffective Shortcuts

aesec™

- Reference Monitor & **FSPM** are long, hard work
  - Omitted by unwary/lazy for "plausible" shortcuts
- "Verified OS" – for functionality, not policy FSPM
  - Example: seL4 – need to verify info flow outside OS
- "Partition Kernel" lacks FSPM for kernel API
  - Example: MILS – explicitly excludes from kernel
- "Verified capability hardware" – missing a FSPM
  - Examples: DARPA-sponsored CRASH and CHERI
- Static code analysis – lacks FSPM for API of OS
  - Example: LDRA Testbed
- Shortcuts cannot **enforce** Integrity MAC for PLC

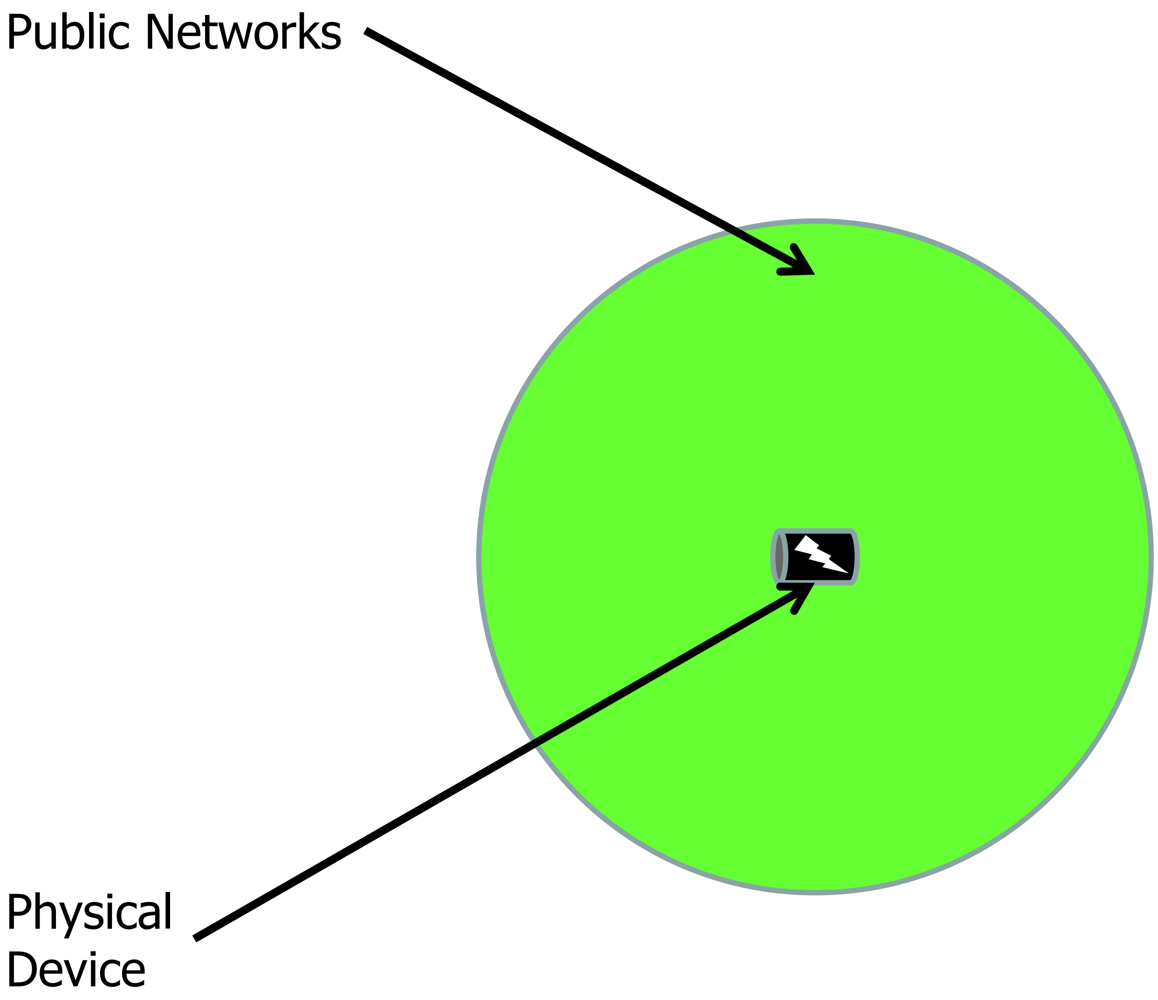
Verifiable Integrity MAC

MAC Reduces CPS Attack Surface



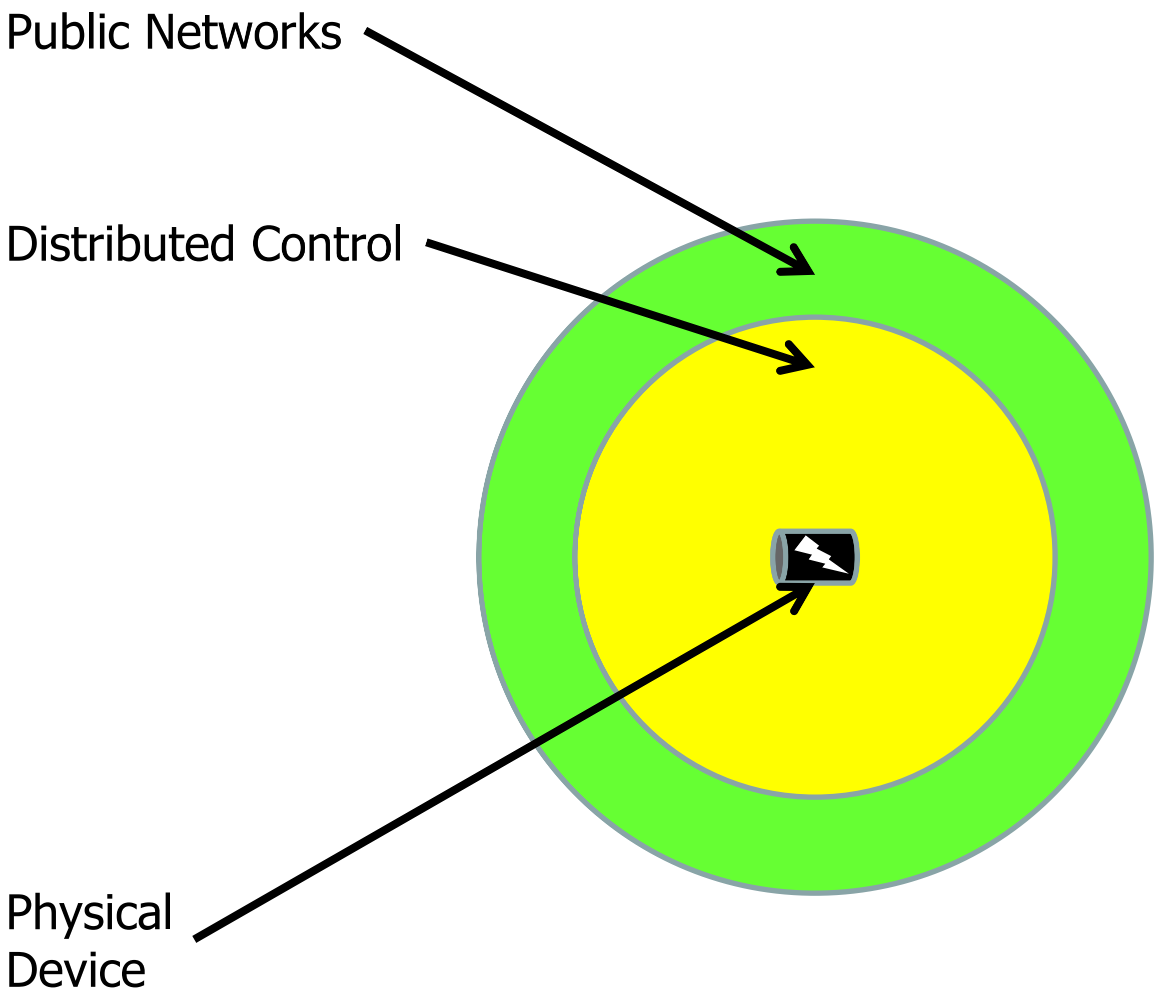
Verifiable Integrity MAC

MAC Reduces CPS Attack Surface



- **Public Networks** access of any kind gives adversaries a huge attack surface

Verifiable Integrity MAC
MAC Reduces CPS Attack Surface



- **Public Networks** access of any kind gives adversaries a huge attack surface
- **Distributed control** is vulnerable to insider attack

Verifiable Integrity MAC
MAC Reduces CPS Attack Surface

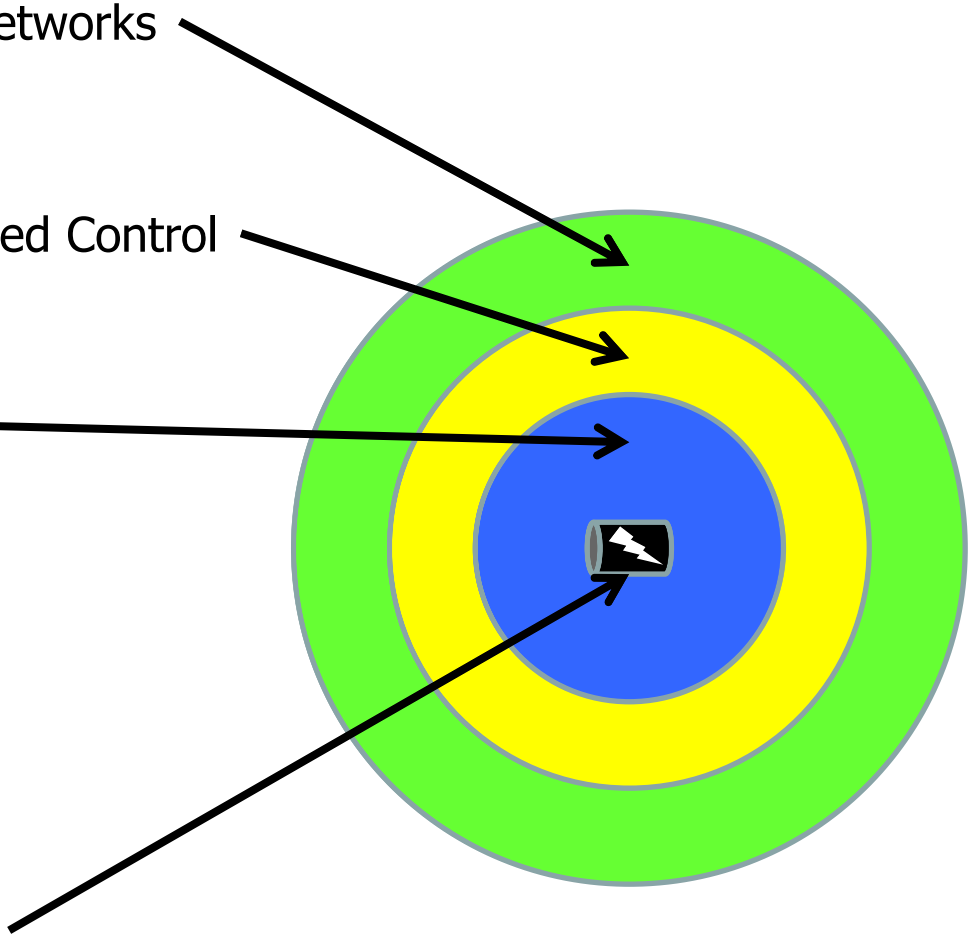
aesec™

Public Networks

Distributed Control

SCADA

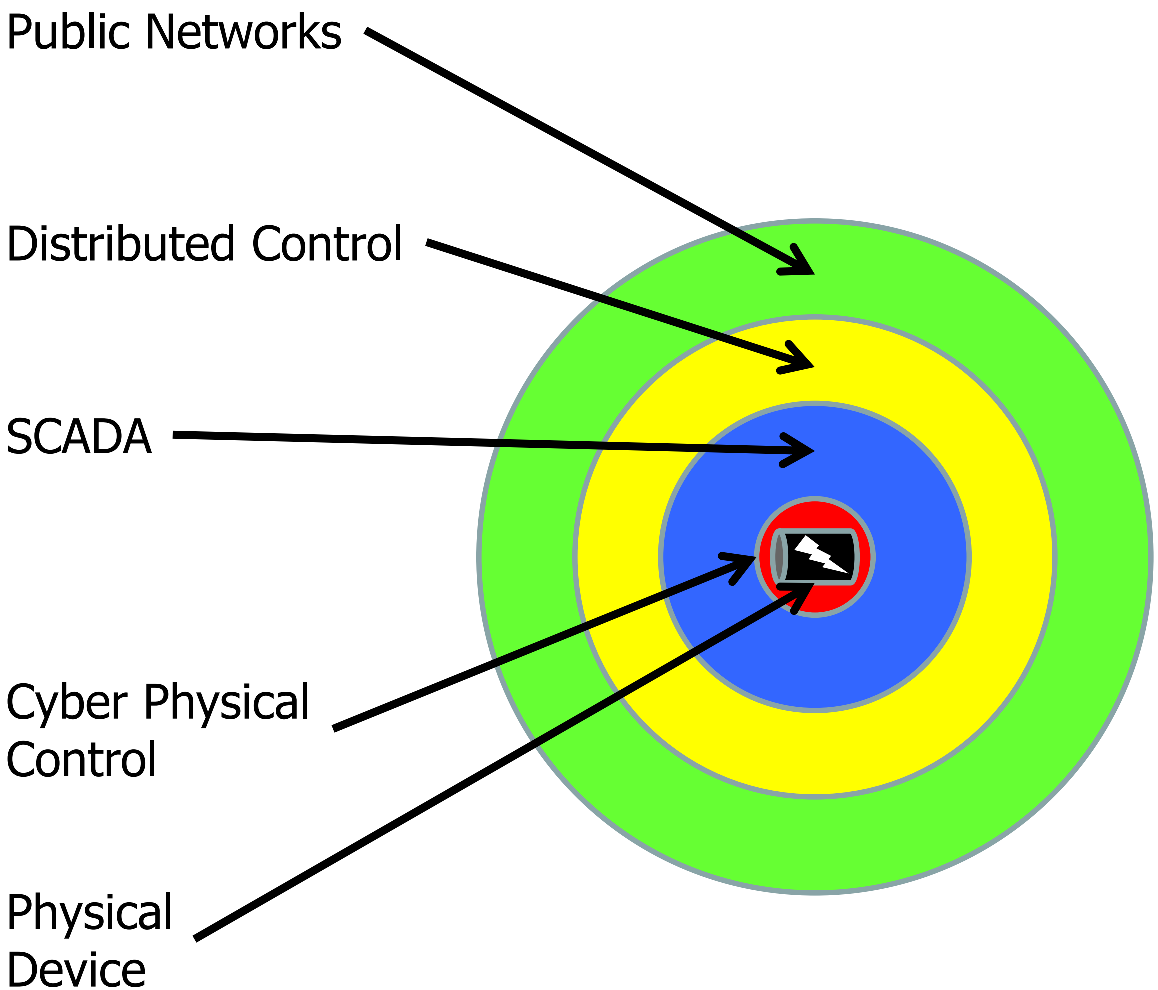
Physical Device



- **Public Networks** access of any kind gives adversaries a huge attack surface
- **Distributed control** is vulnerable to insider attack
- **SCADA** and other adaptable control systems can be sabotaged

Verifiable Integrity MAC
MAC Reduces CPS Attack Surface

aesec™



- **Public Networks** access of any kind gives adversaries a huge attack surface
- **Distributed control** is vulnerable to insider attack
- **SCADA** and other adaptable control systems can be sabotaged
- **Cyber Physical Control** requires protection of Safe Regions (e.g., Power System Settings) only Mandatory Access Controls provide

OpenPLC on GEMSOS
NIST Calls Out Solution Concept

aesec™

NIST calls out "kernel" in flagship SP-800-160v1

– "Electric Grid – Industrial/process control systems"

- PLC typically controls critical physical component

  "*Trustworthy components within ICS, including for example, highly assured, **kernel-based** operating systems in **Programmable Logic Controllers***" [PLC]

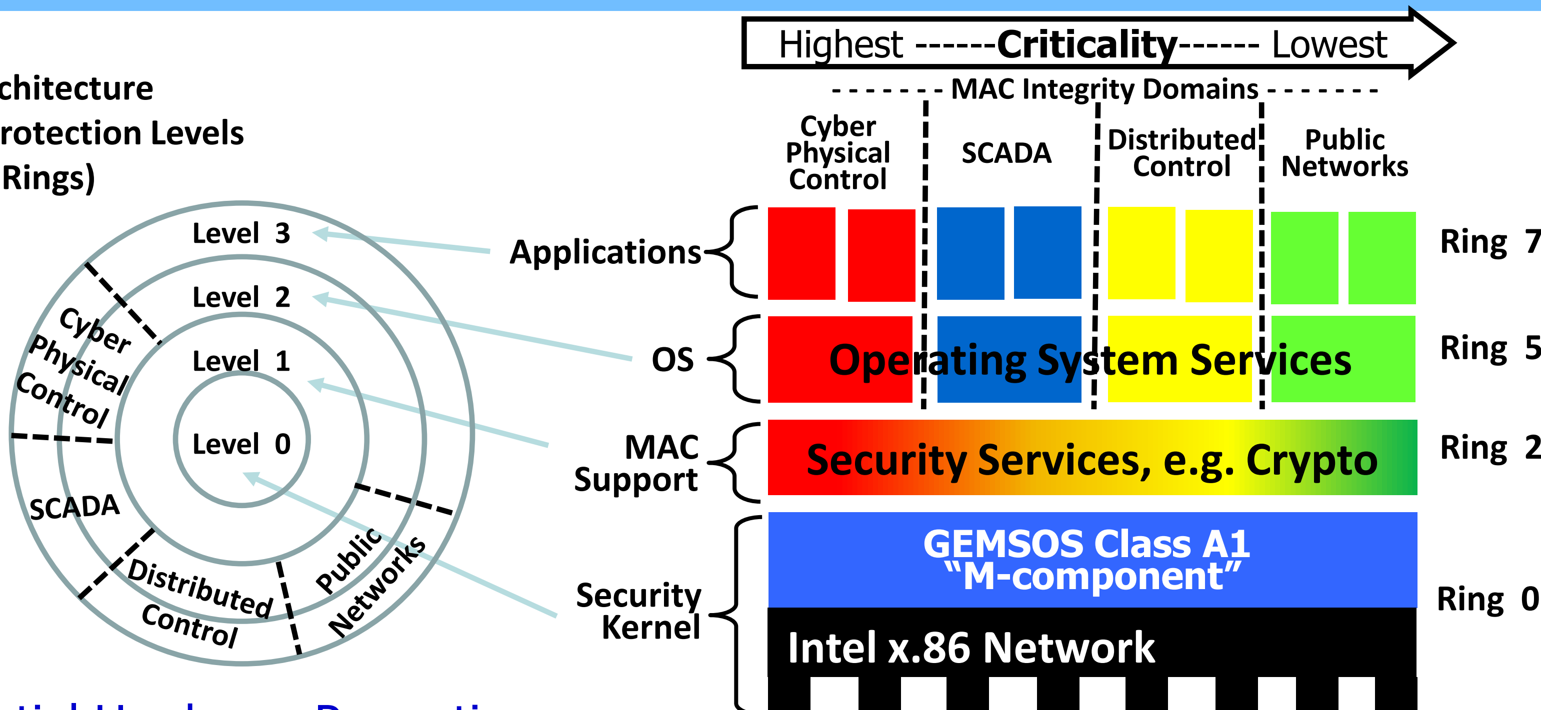
- Kernel MAC controls integrity security domains

  "*can help achieve a high degree of system **integrity** and availability through **domain** separation with control over cross-domain flows and use of **shared** resources.*"

OpenPLC on GEMSOS
Reproducible Research Setup

aesec™

Intel x86 Architecture Hardware Protection Levels (Protection Rings)



- Essential Hardware Properties
  - Hardware Rings – more than 2
  - Memory Segmentation vs Paging
  - Strong Process Model
- NSA TCSEC/TNI Class A1 – Verified Design

MAC Integrity Domains	Criticality	Attack Surface
Cyber Physical Control	High	Very Small
SCADA	Medium	Small
Distributed Control	Medium-low	Moderate
Public Networks	Low	Very Large

Concentric ring diagram taken from Intel® 64 and IA-32 Architectures Software Development's Manual, Volume 3A: System Programming Guide, Part 1, (order number 253668)

OpenPLC on GEMSOS
Demonstration Approach

Four distinct **hierarchical** integrity domains

1. Cyber physical system (CPS) control
   - **Only** domain with I/O access to physical hardware
   - Enforces "Pierson Safe Region" for physical device
2. Supervisory Control and Data Acquisition
   - SCADA domain – main PLC "Logic Loop"
3. Distributed control
   - Integrity-protected network interfaces
4. Untrusted public networks (e.g., Internet)

OpenPLC on GEMSOS
Open Source Research PLC

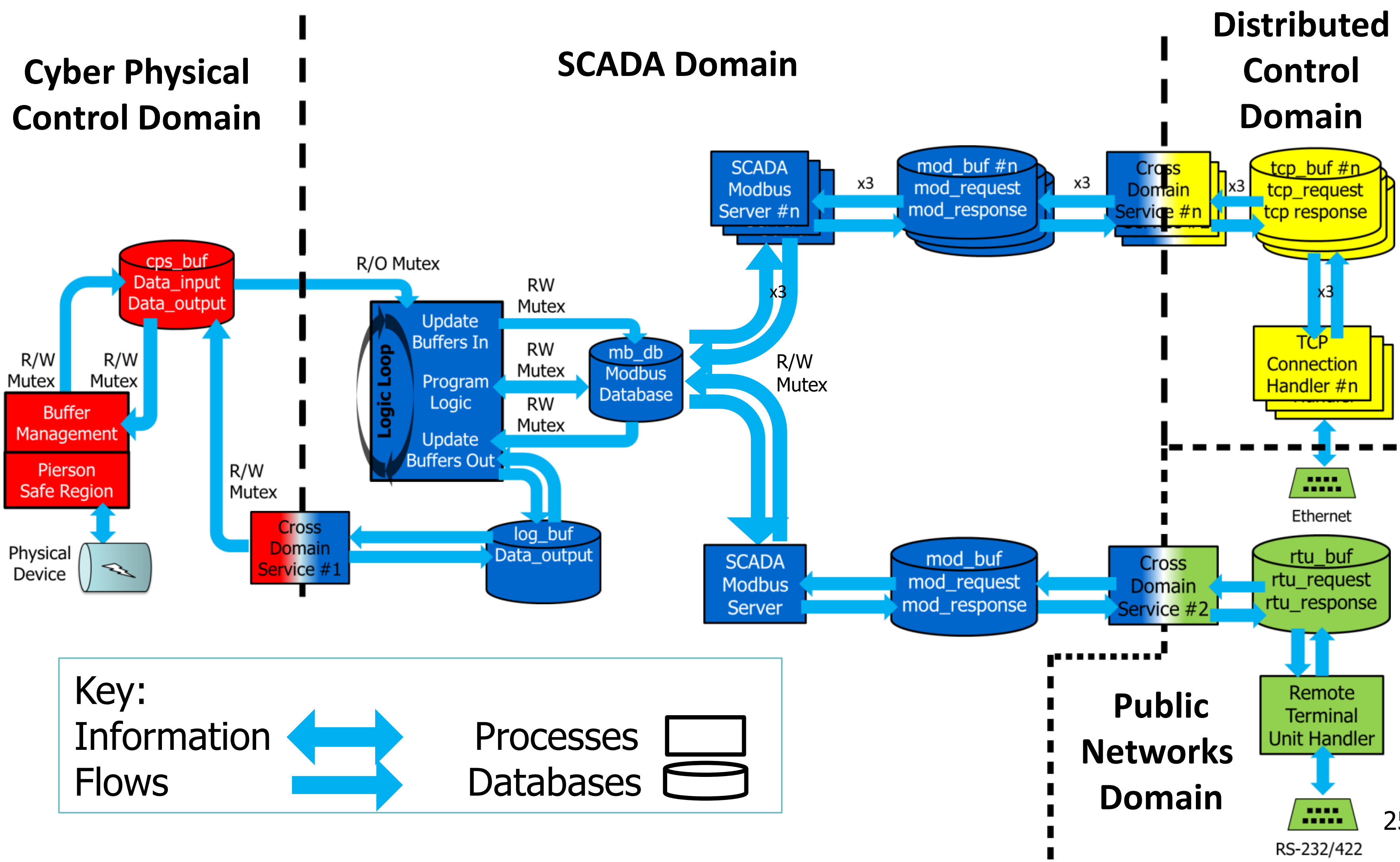
- Originated with Thiago Alves, Brazil
  - Developed at University of Alabama in Huntsville
    - Prof. Tommy Morris-led team
  - https://www.openplcproject.com

- Highly functional PLC for Windows, Linux, etc.

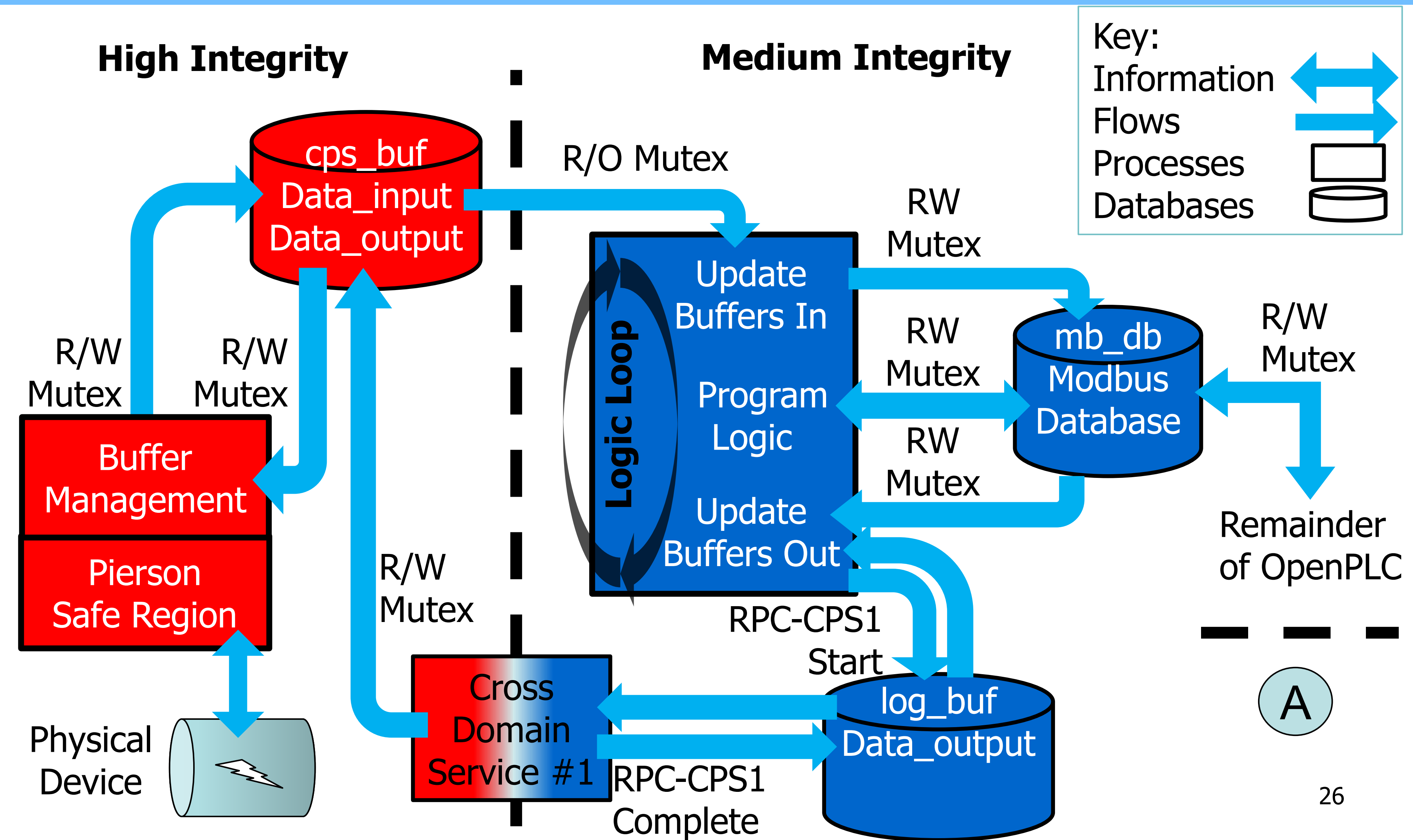
- Some commercial PLC vendors using

- Installed in Matt Bishop's UCDavis Security Lab
  - On GEMSOS Developer's Kit

OpenPLC on GEMSOS
4-Domains and CDS Transfers



OpenPLC on GEMSOS
Cyber Physical System Control



OpenPLC on GEMSOS

Reduced Attack Surface

Domain	Processes	Stripped Size (bytes)	Percentage of whole
Cyber Physical Control	Phys Device Ctl	14,556	0.7%
	CDS #1	31,100	
SCADA	Logic Loop	1,022,900	20.2%
	Modbus RPC	275,732	
	CDS #2	31,396	
Distributed Ctl	TCP/IP Stack	144,960	2.7%
	CDS #3	31,100	
Public Networks	RTU Handler	25,032	76.4%
	External Network	> 5,000,000	

Mature Subversion Mitigation

NIST: Class A1 for Subversion

aesec™

- NIST cites "Class A1" in flagship SP-800-160v1
  - "Application . . . to Commercial Products"

- Products are worked examples and use cases

  "*highly trustworthy components and systems that have been verified to be highly resistant to **penetration** from determined adversaries*"

- TCSEC **Class A1** distinguished

  "*by substantially dealing with the problem of **subversion** of security mechanisms.*"

Mature Subversion Mitigation
Trusted Device Protects Itself

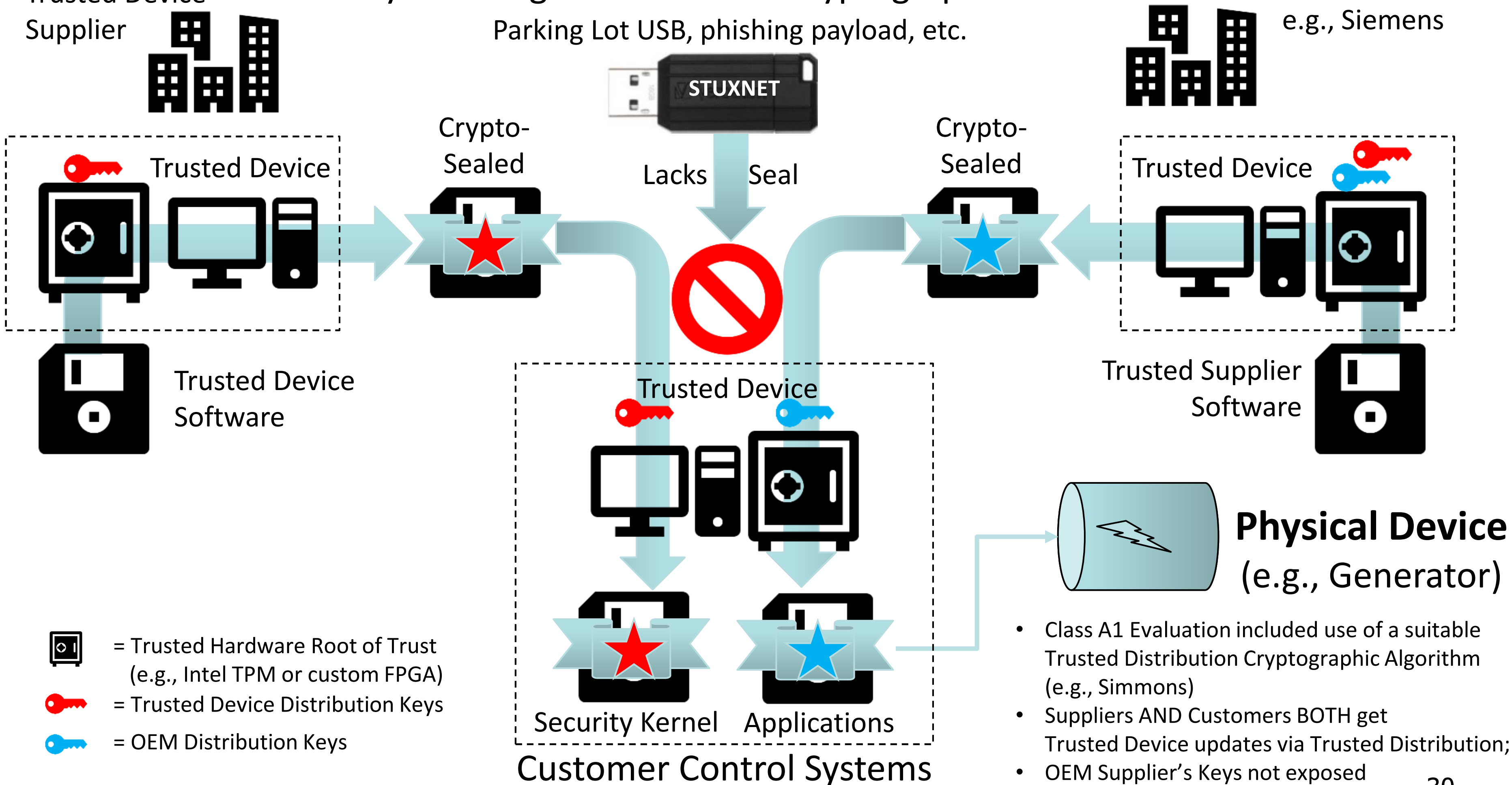
aesec™

- Trusted Boot for software/configuration settings
- Vet Trusted Devices for unauthorized behavior
- Code Correspondence stop “dead code” malware
- Trusted Distribution avoids supply chain attacks
- Media integrity mitigates “parking lot” attacks

Mature Subversion Mitigation

Illustrative STUXNET Mitigation

Class A1 Trusted Distribution rejects installation of untrusted software (malware) by checking for authorized cryptographic seal



- Class A1 Evaluation included use of a suitable Trusted Distribution Cryptographic Algorithm (e.g., Simmons)
- Suppliers AND Customers BOTH get Trusted Device updates via Trusted Distribution;
- OEM Supplier's Keys not exposed

Presentation Outline

aesec™

- Problem: national existential risk

- Towards a Reusable Trusted Device (RTD)

- **Control Systems: PLC Commercialization**
  - Original Equipment Manufacturer (OEM) model

PLC Technology Transfer
Traditional OEM Model

- Security kernel vendor offers Trusted Device
  - Hardware & software domain-specific platform, e.g., motherboard, SOC
  - Trusted distribution, system security certification
- OEMs & manufacturers build PLC platforms
  - Trusted Device is part of any hardware product configuration
- VARs, ISVs, appliance vendors
  - Add applications and system services software, use OpenPLC source
- Solution providers and system integrators
  - Customization and integration for customers
  - Deliver complete solutions

PLC Technology Transfer
Previous Evaluations Accelerate

aesec™

- Former DIRNSA LtGen Linc Faurer note [2007]
- "very high priority problem area"
  - "vulnerability of our network components and
    - electronic credentials to software **subversion**"
  - "convinced that an IC disaster looms"
- "demands that the first set of solutions"
  - "directly leverage the designs, architectures and
    - rating maintenance plans [RAMP] which NSA has
    - previously evaluated at the **Class A1** level of assurance"
  - "this is the **only** practical way to be confident the
    - needed solutions can be operationally deployed in the
    - next **couple of years**."

Presentation Outline Summary

aesec™

- **Problem: national existential risk**
  - Poor Cyber Physical Systems (CPS) resilience
  - Vulnerable critical cyber-physical components
- **Towards a Reusable Trusted Device (RTD)**
  - Security kernel technology
  - Verifiable Integrity Mandatory Access Control (MAC)
  - OpenPLC on GEMSOS demonstration
  - Mature subversion mitigation
- **Control Systems: PLC Commercialization**
  - Original Equipment Manufacturer (OEM) model

Verifiable CPS Bottom Line

- Critical *physical* components need verifiable PLC
  - Limited system risk from remaining components
- Kernel makes CPS attack surface much smaller
  - Each *integrity MAC* domain protected from lower
  - Security kernel *verified design* for unknown attacks
  - Deals with *subversion* of security mechanisms
- PLC performance & functionality retained
  - OEM host PLC on *trusted device* with secure OS
  - PLC manufacturers can use OpenPLC prototype
- Mature OEM business model & support approach
  - Successful security kernel OEM delivery history

CPS Cybersecurity Conclusion

aesec™

Clear **NEED** for resilient CPS

Commercial **TECHNOLGY** available

Need PLC manufacturer **ADOPTION**

The power of verifiable protection™

Dramatically Reducing Attack Surface Using Integrity MAC Security Kernel

Dr. Roger R. Schell, PhD
President and founder of Aesec Corporation
roger.schell@aesec.com
(831) 657-0899

CERIAS 2020 Seminar
Purdue University
West Lafayette, IN
Streamed live on the Web
September 2, 2020
4:30pm EDT