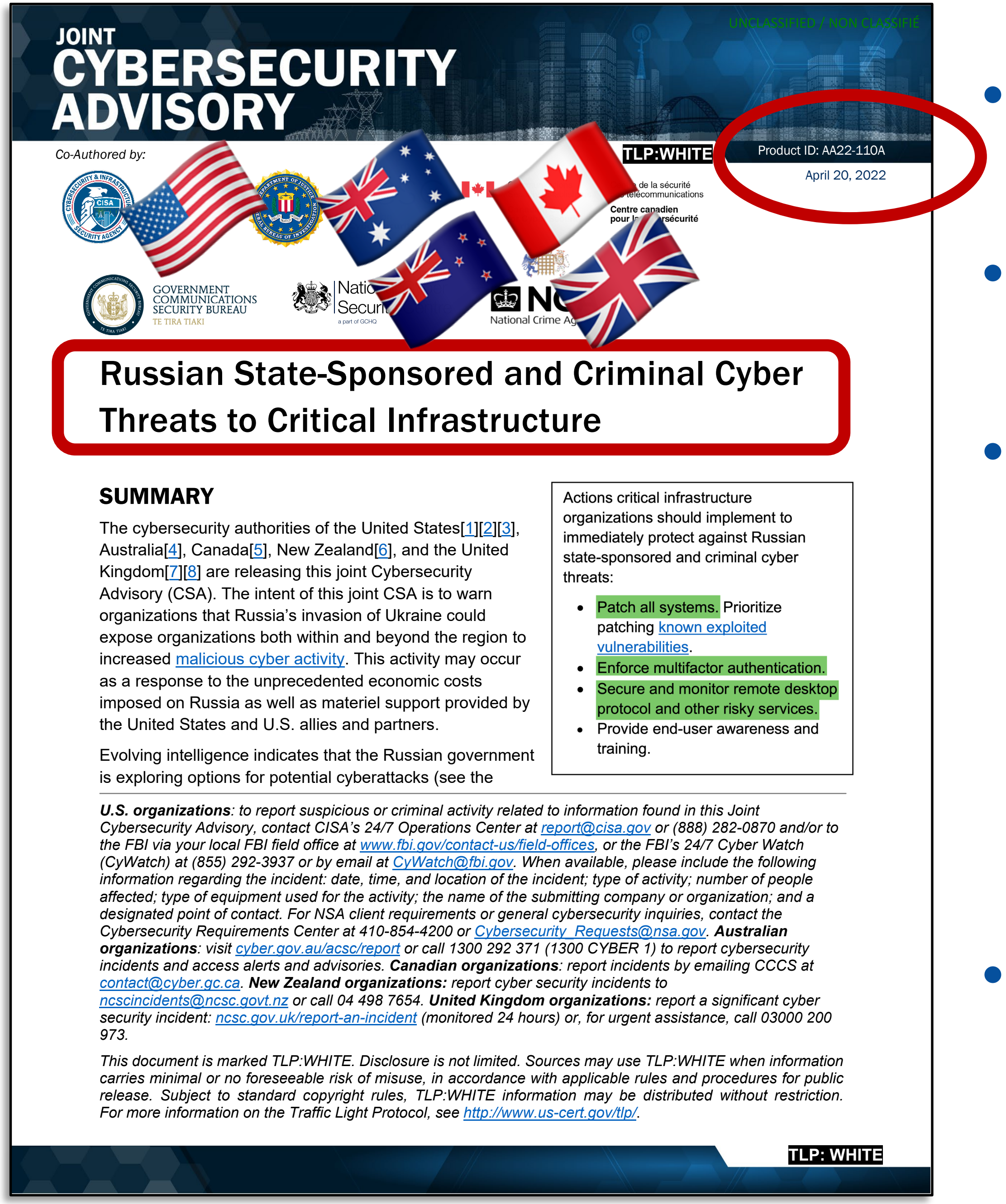
Assured Reserve Modes (in Action)

Dr. Lance Joneckis & Dr. Ihor Kuz

INL Idaho National Laboratory

KRY10



UNCLASSIFIED / NON CLASSIFIÉ

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-110A

April 20, 2022

de la sécurité
télécommunications
Centre canadien
pour la rsécurité

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

Natio
Securi
a part of GCHQ

NC
National Crime Ag

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

SUMMARY

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the

Actions critical infrastructure organizations should implement to immediately protect against Russian state-sponsored and criminal cyber threats:

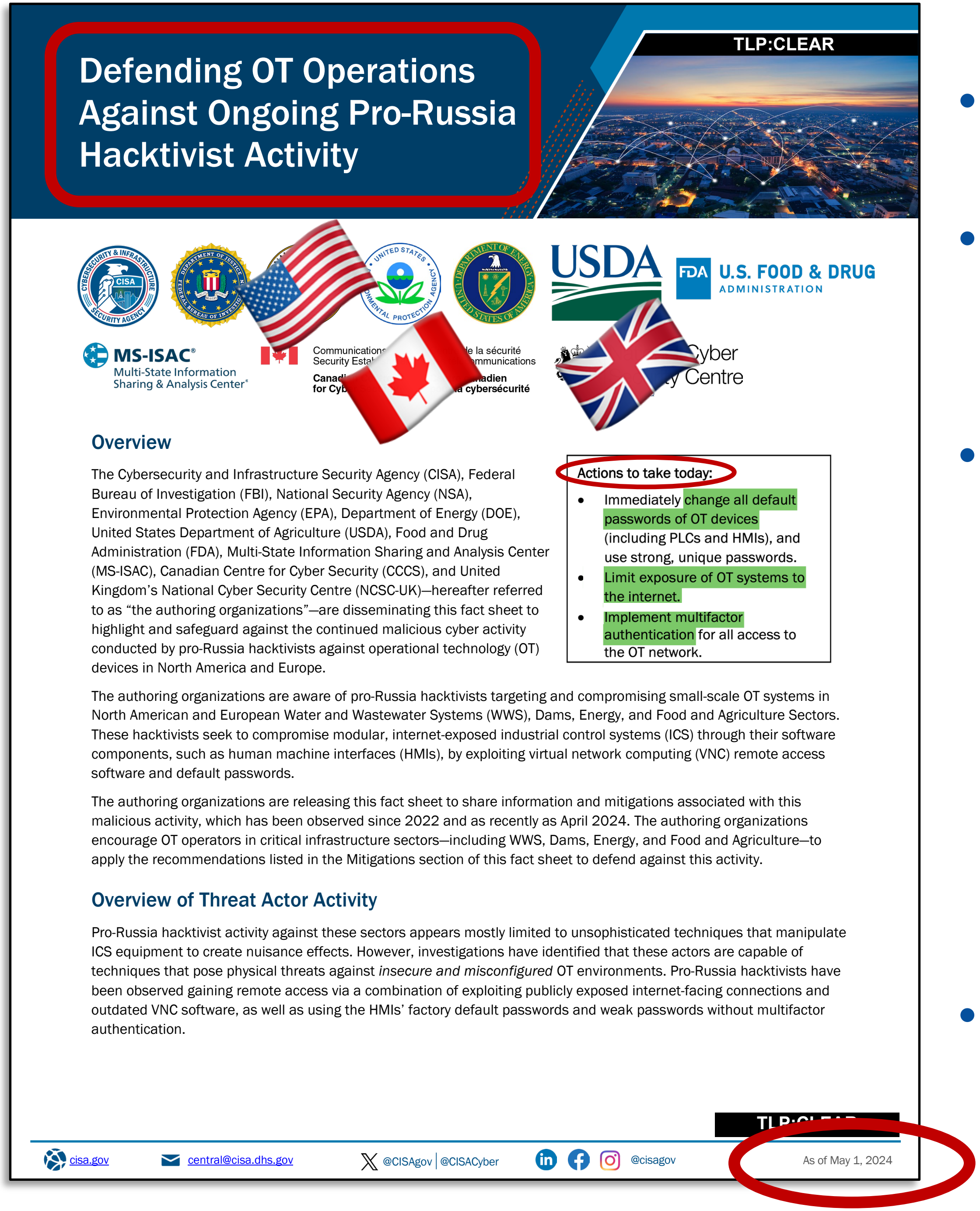
- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Enforce multifactor authentication.
- Secure and monitor remote desktop protocol and other risky services.
- Provide end-user awareness and training.

U.S. organizations*: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.* ***Australian organizations****: visit cyber.gov.au/acsc/report or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.* ***Canadian organizations****: report incidents by emailing CCCS at contact@cyber.gc.ca.* ***New Zealand organizations:*** *report cyber security incidents to ncscincidents@ncsc.govt.nz or call 04 498 7654.* ***United Kingdom organizations:*** *report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.*

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

TLP: WHITE

- April 20, 2022
- Russian attacks on critical infrastructure
- Multi-National Alert
  - United States
    - Cybersecurity Infrastructure Agency (CISA)
    - National Security Agency (NSA)
    - Justice Department
  - Australia, Canada, New Zealand, UK
- Recommendations



TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against *insecure and misconfigured* OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

TLP:CLEAR

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of May 1, 2024

- May 1, 2024
- Defending OT Operations Against Pro-Russia Hacktivist Activity
- Multi-National Alert
  - United States
    - Cybersecurity Infrastructure Agency (CISA)
    - Justice Department
    - National Security Agency (NSA)
    - Environmental Protections Agency
    - US Department of Agriculture
    - Food and Drug Administration
  - Canada, UK
- Recommendations

TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

USDA
U.S. FOOD & DRUG ADMINISTRATION
MS-ISAC
Multi-State Information Sharing & Analysis Center
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
a part of GCHQ

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs) by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against *insecure and misconfigured* OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

TLP:CLEAR

cisa.gov central@cisa.dhs.gov @CISAgov | @CISACyber @cisagov As of May 1, 2024

- May 1, 2024
- Defending OT Operations Against Pro-Russia Hacktivist Activity
- Multi-National Alert
  - United States
    - Cybersecurity Infrastructure Agency (CISA)
    - Justice Department
    - National Security Agency (NSA)
    - Environmental Protections Agency
    - US Department of Agriculture
    - Food and Drug Administration
  - Canada, UK
- Recommendations

What should we be doing **today** for **tomorrow**?

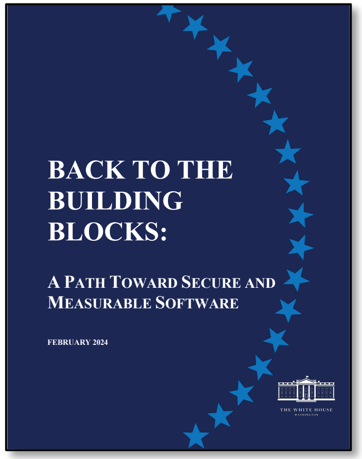
Idaho National Laboratory

High-level USG Policy

- 2013 Critical Infrastructure Security and Resilience (PPD-21)
  - Calls out
    - "enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario as well as cascading effect on other sectors"
- 2019 CISA Initiative on Securing ICSs
  - Calls out
    - "ICS performs within threshold under duress … despite malicious actions by adversaries in the control systems environment"
- 2023 White House's National Cyber Strategy
  - Calls out
    - "goal is defensible, resilient, ecosystems … where neither incidents nor errors cascade into catastrophic, systemic consequences"
    - "building a new generation of interconnected hardware and software systems that have the potential to strengthen the resiliency, safety, and efficiency of the U.S. electric grid."
- 2024 White House's Back to the Building Blocks: A Path Towards Secure and Measurable Software
  - Calls out
    - "focuses on the programming language as a primary building block, and explores hardware architecture and formal methods as complementary approaches to achieve similar outcomes."

THE WHITE HOUSE
Office of the Press Secretary
For Immediate Release
February 12, 2013
PRESIDENTIAL POLICY DIRECTIVE/PPD-21
NATIONAL CYBERSECURITY STRATEGY
BACK TO THE BUILDING BLOCKS:
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
SECURING INDUSTRIAL CONTROL SYSTEMS:
A UNIFIED INITIATIVE
FY 2019–2023

INL's High Assurance Industrial Systems



BACK TO THE BUILDING BLOCKS:

A PATH TOWARD SECURE AND MEASURABLE SOFTWARE

FEBRUARY 2024

THE WHITE HOUSE

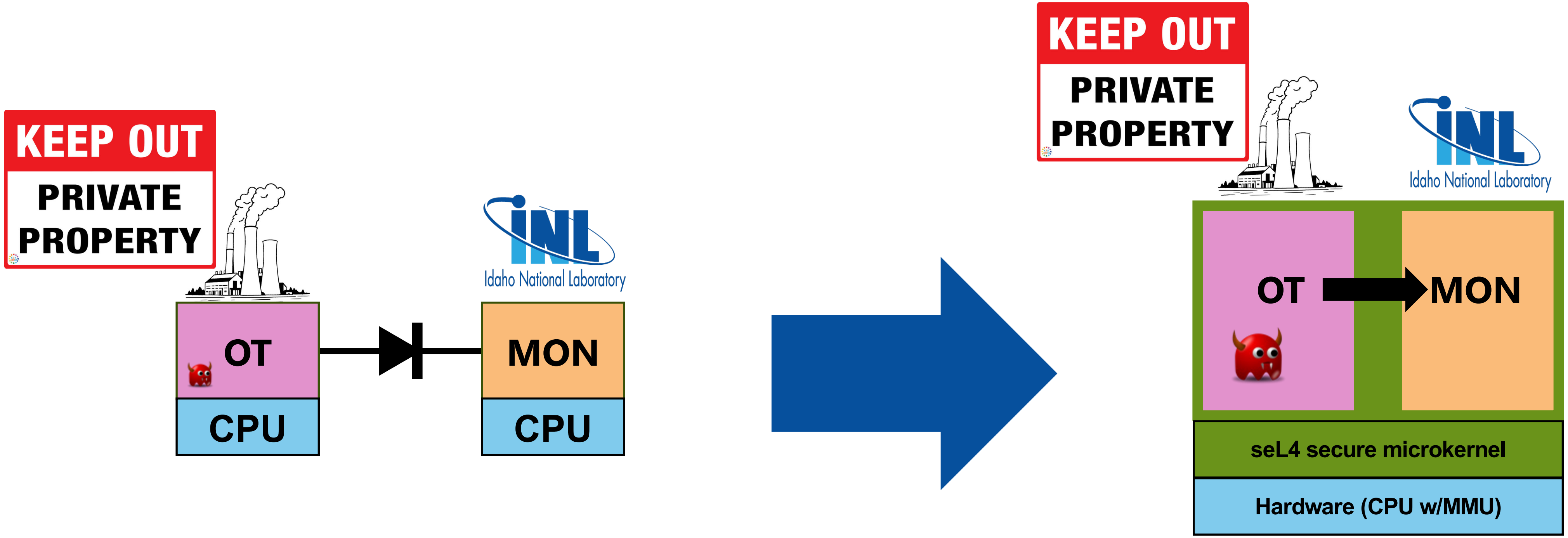
"The road toward this vision requires a recognition that the Nation is at its best when Americans work together. It is a path that requires the convergence of **government initiative**, **private sector innovation**, *and* **groundbreaking academic research**.*"*

INL

Idaho National Laboratory

KRY10

Motivation



KEEP OUT

PRIVATE PROPERTY

OT

CPU

Idaho National Laboratory

MON

CPU

KEEP OUT

PRIVATE PROPERTY

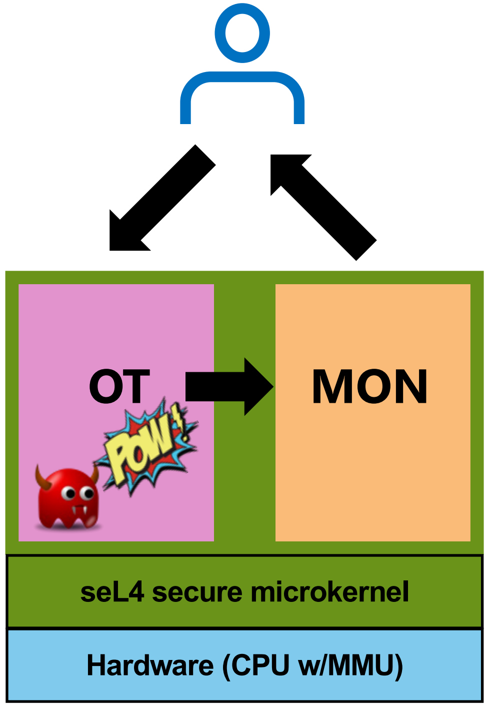
Idaho National Laboratory

OT

MON

seL4 secure microkernel

Hardware (CPU w/MMU)



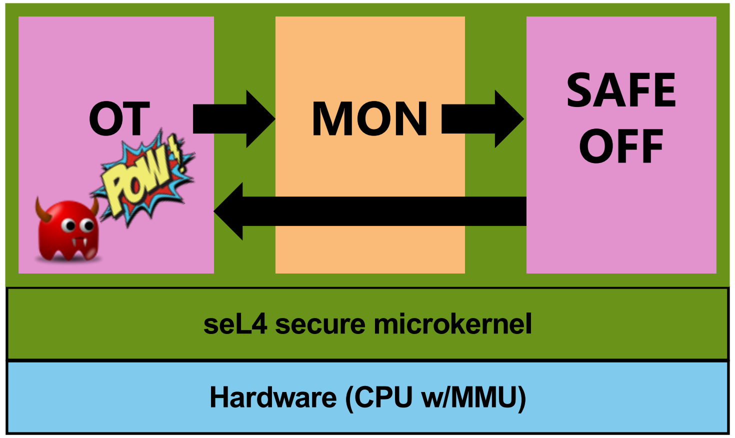
OT

MON

seL4 secure microkernel

Hardware (CPU w/MMU)

Monitor & Report System



OT

MON

SAFE OFF

seL4 secure microkernel

Hardware (CPU w/MMU)

Real-time Reactive System

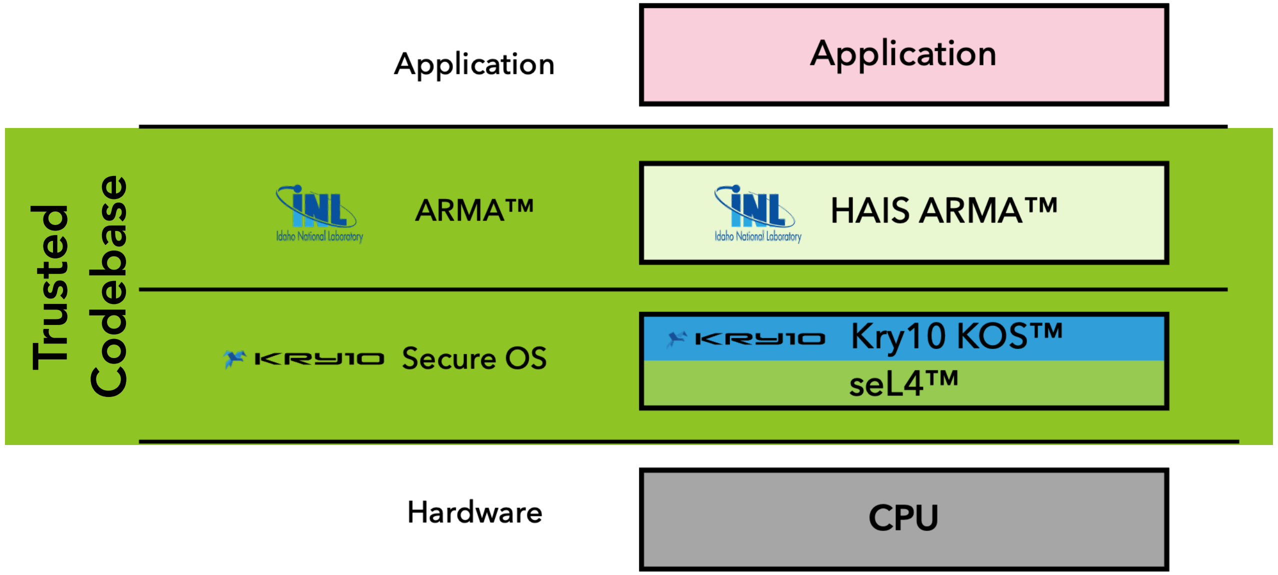
Assured Reserve Modes in Action

- Assured Reserve Mode Architecture (ARMA™)
- Fischertechnik Experimental Platform
- **Brownfields Problem** – Protecting existing critical infrastructure
  - ARMA Secure Gateway
- **Greenfields Opportunity** – Protecting new builds of critical infrastructure

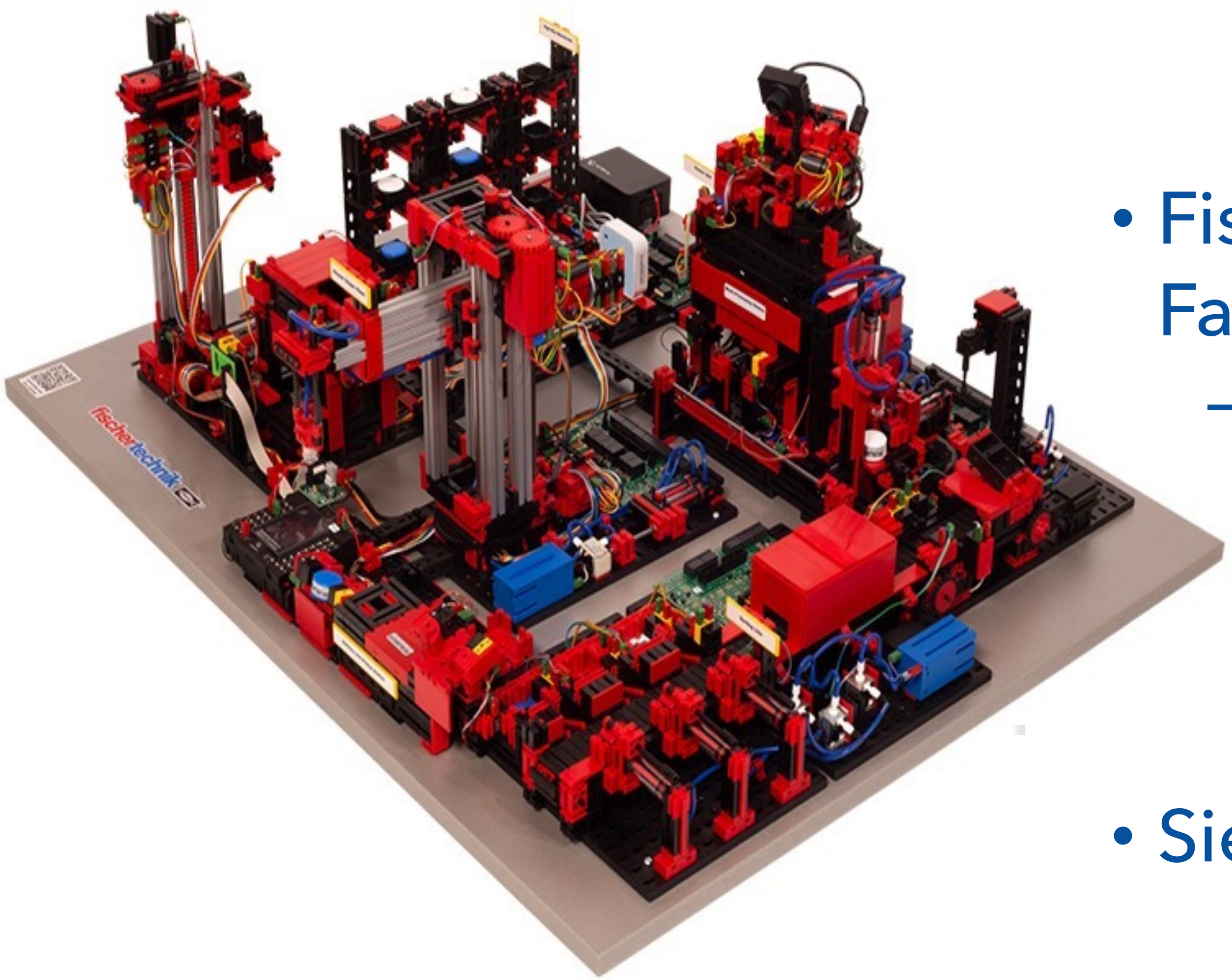
Assured Reserve Modes

- Reserve Modes
  - (Wartime) Reserve Modes – Military capabilities and configurations held in reserve for wartime or emergency use.
    - Wartime radio frequencies are different than peacetime frequencies
  - What would *cyber reserve modes* look like?

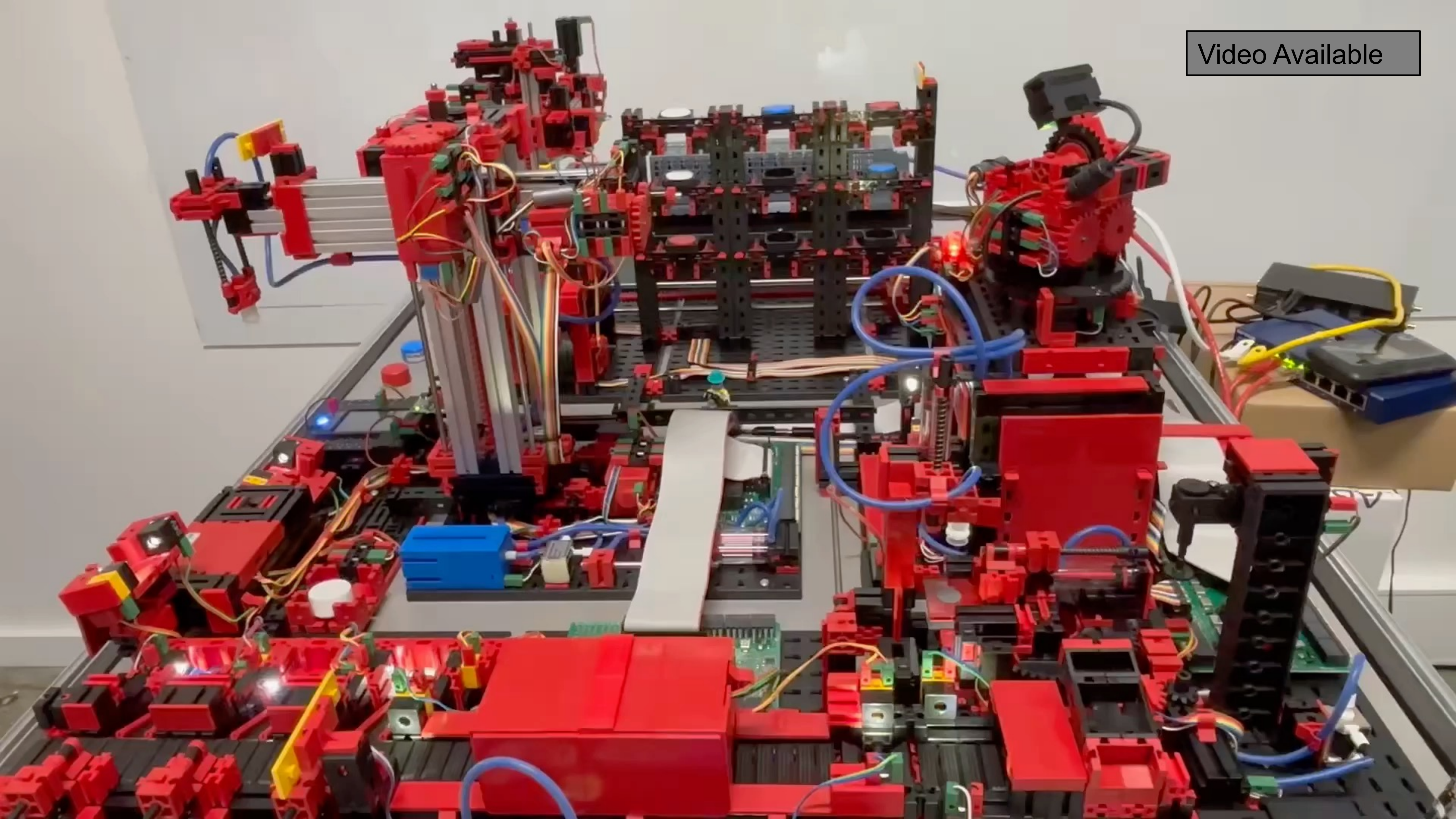
- **Assured** Reserve Modes
  - High-confidence that reserve modes can't be compromised
  - seL4-based system
  - Kry10's KOS™ implementation of seL4



Fischertechnik – Training Factory Industry

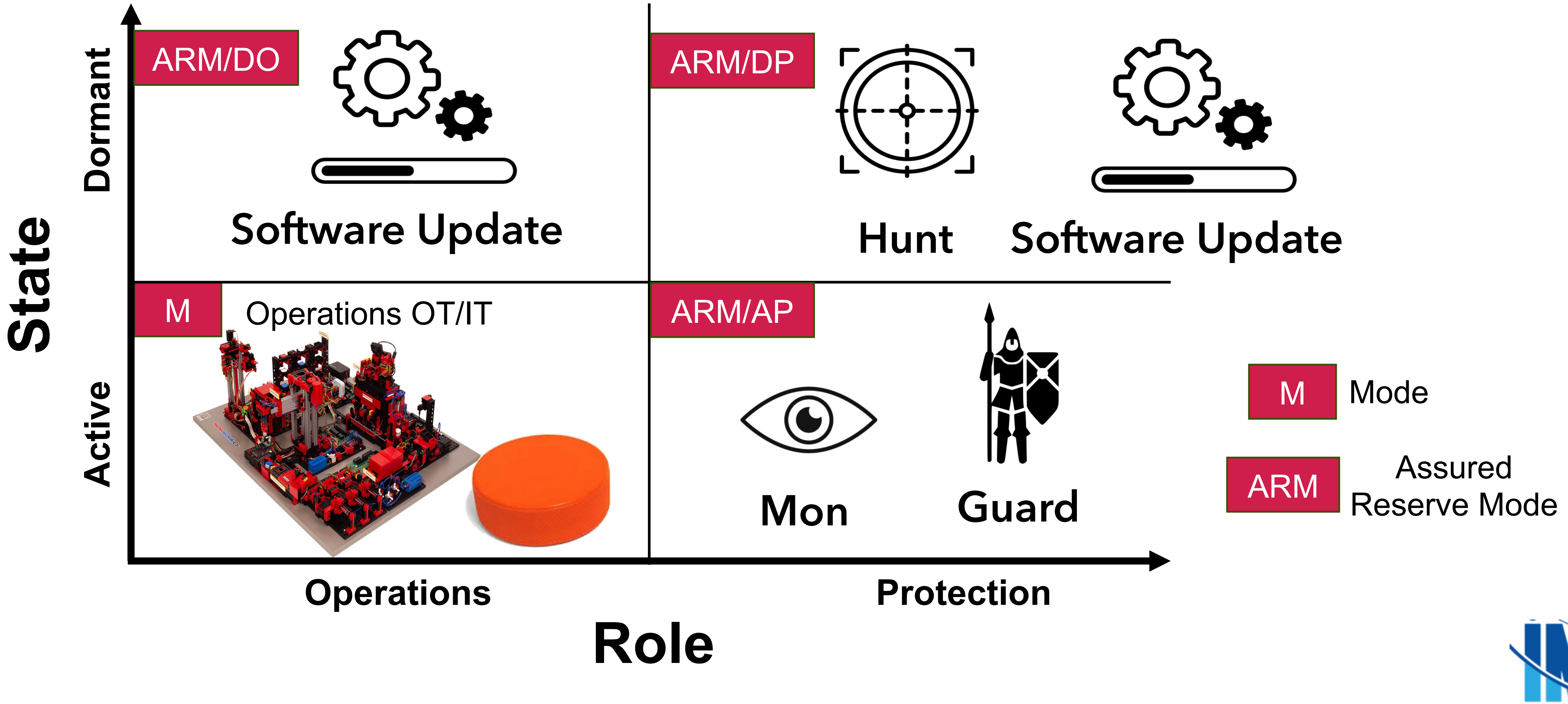


- Fischertechnik – Industrial Training Factory
  - 5 Stations
    - 28 digital inputs
    - 14 encoders
    - 2 analog
    - 43 actuators
- Siemens SIMATIC S7-1500 PLC



Video Available

Assured Reserve Mode Architecture (ARMA™) Modes & Assured Reserve Modes



State

Dormant

ARM/DO

Software Update

ARM/DP

Hunt

Software Update

Active

M

Operations OT/IT

ARM/AP

Mon

Guard

Operations

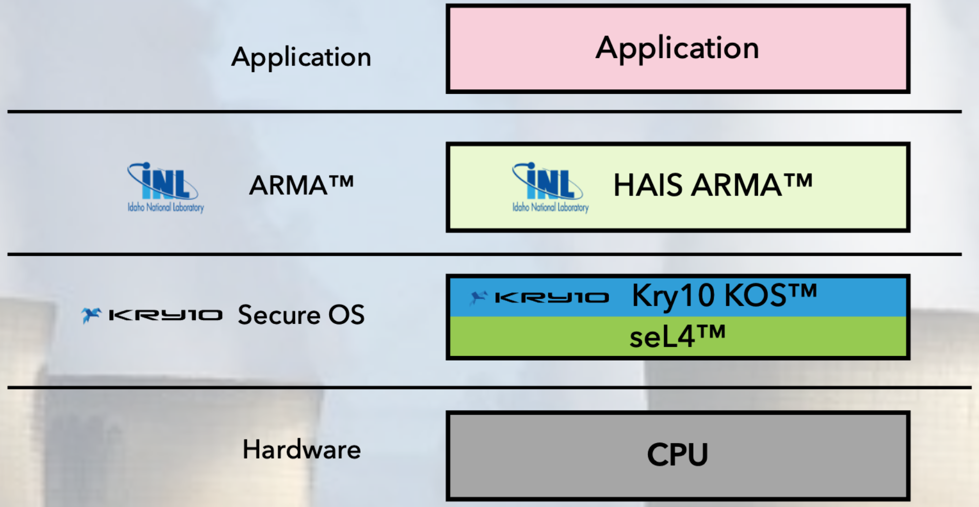
Protection

Role

M Mode

ARM Assured Reserve Mode

Protecting Critical Infrastructure – **Brownfields**



- Critical infrastructure (CI) lasts decades after being commissioned
- Limited opportunities for upgrades and technology refresh

- Increasingly CI is being connected to the Internet
- 👿 Prime target for cyber attack 👿

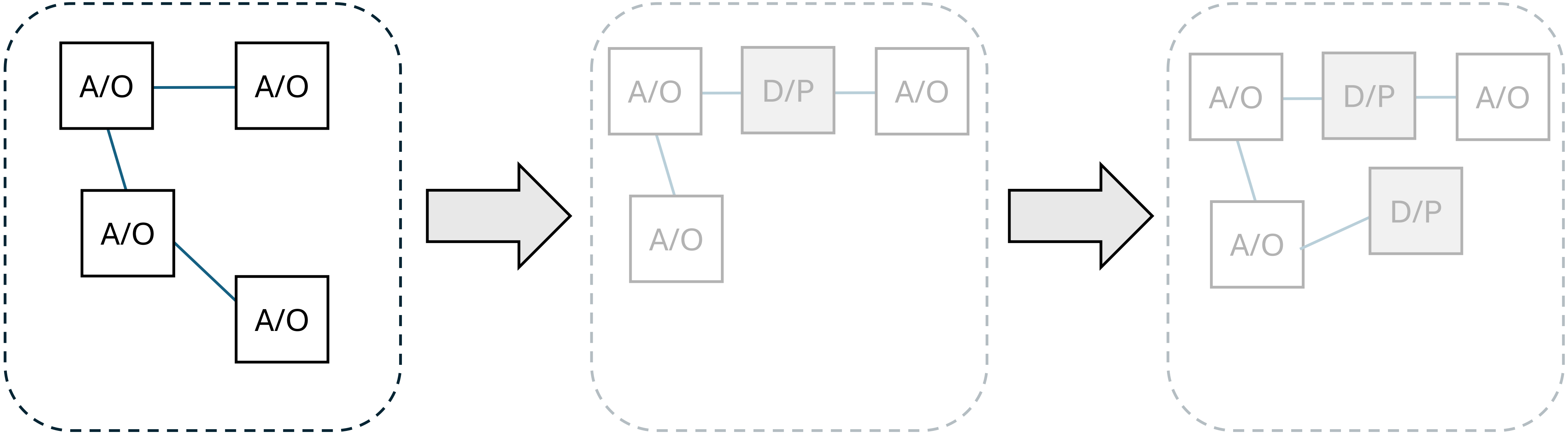
Protecting Brownfield Systems

1. System Configurations
2. Simple ARMA example
3. Implementing ARMA
   - Technical requirements
   - ARMA and seL4
   - ARMA and Kry10 OS
4. ARMA in Action: Factory example

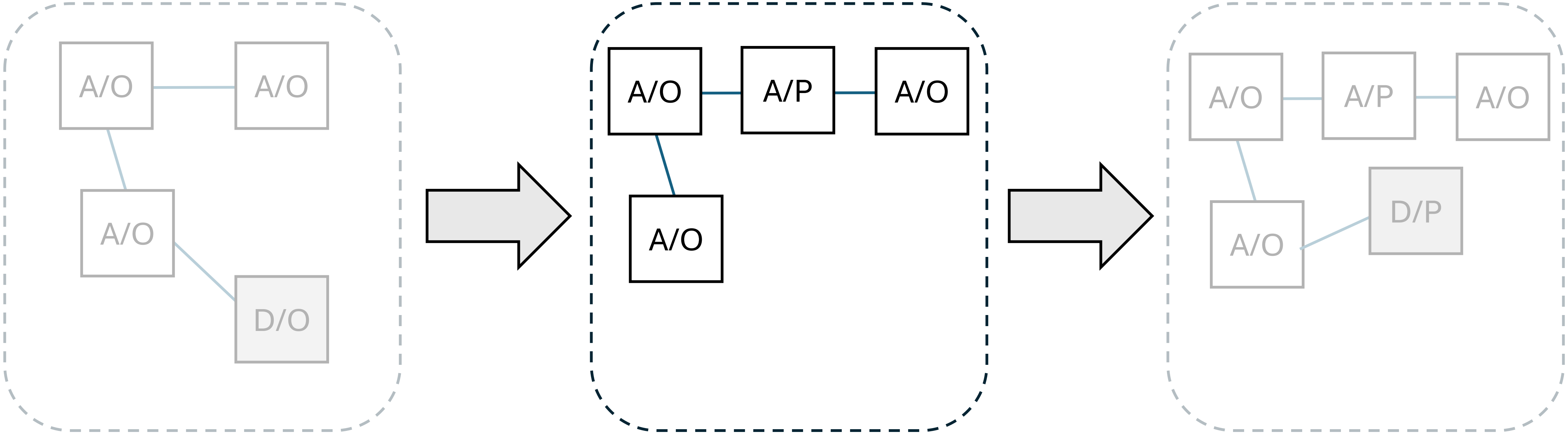
Reserve Mode System Configurations

- System configuration:
  - Specification of All running components and connections
  - Operation components, Protection components
  - "Reserve Mode"
- ARMA System lifecycle
  - Succession of system configurations
  - Switch between configurations to switch reserve modes
- ARMA System
  - All valid configurations and transitions between them
- Semi-dynamic system

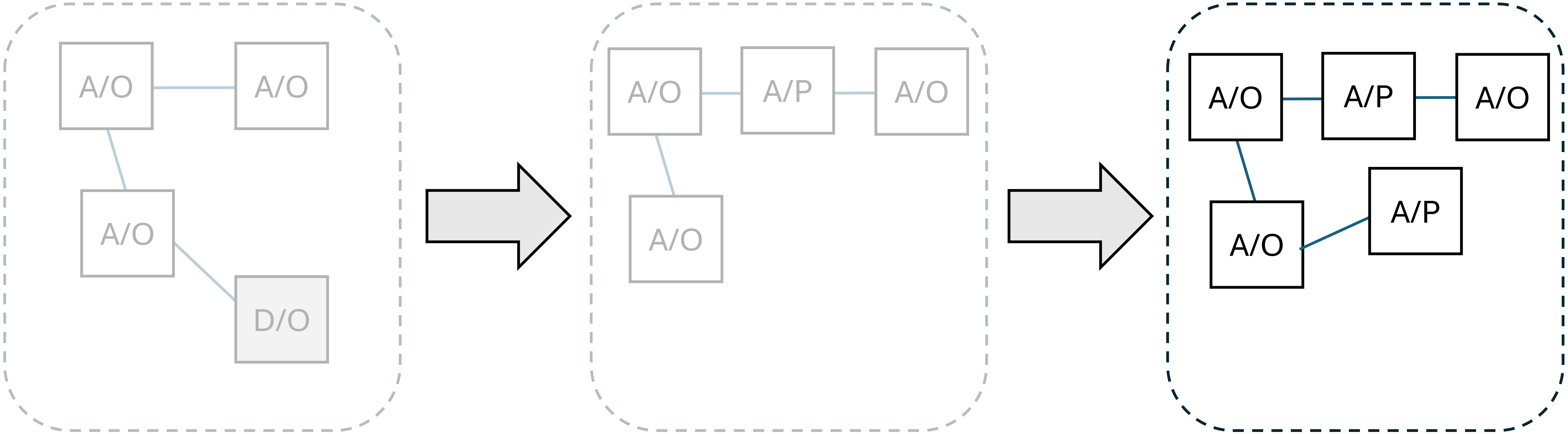
Reserve Mode System Configurations



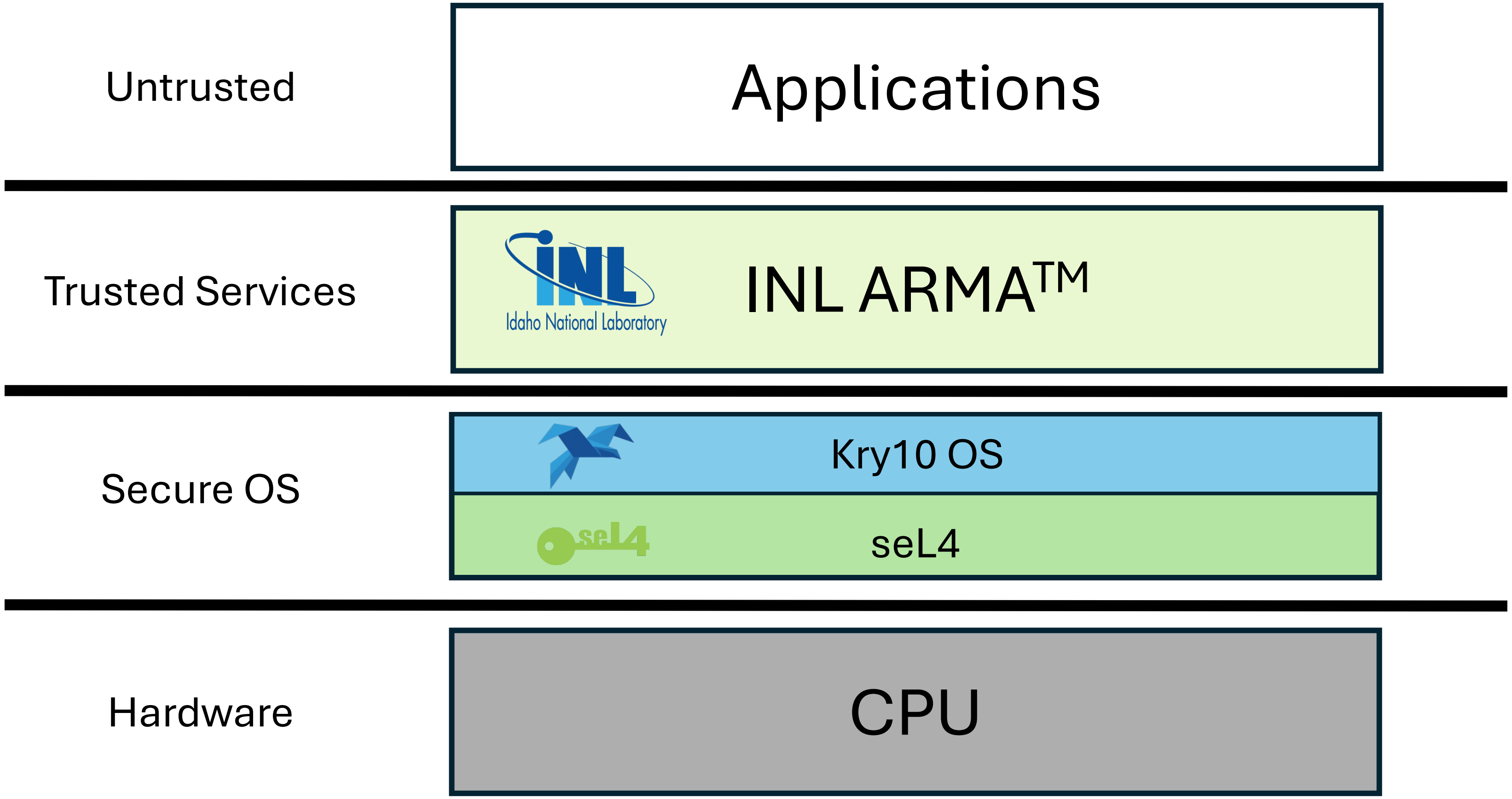
Reserve Mode Configurations



Reserve Mode Configurations



ARMA Example



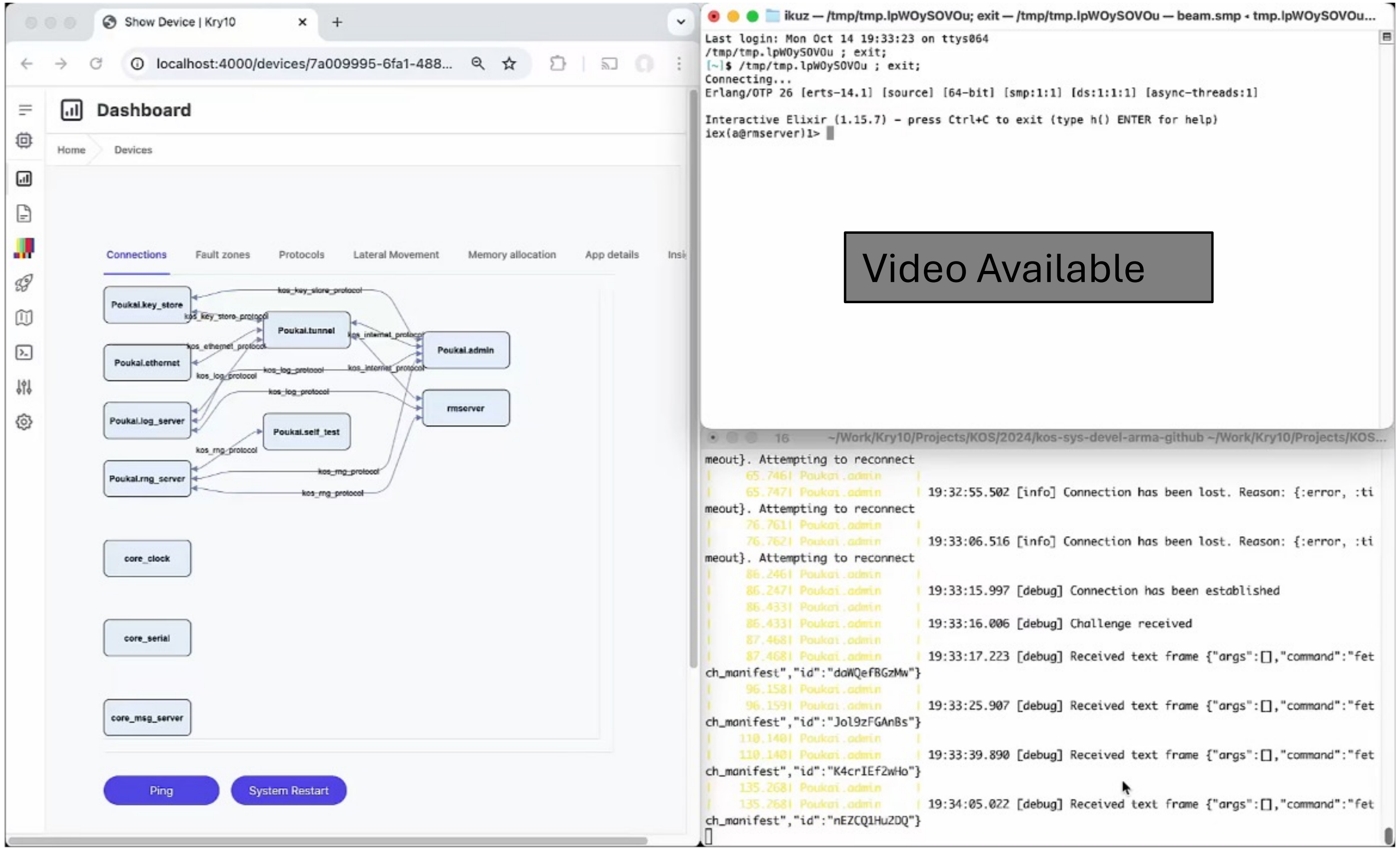
Untrusted | Applications

Trusted Services | INL ARMA^{TM}

Secure OS | Kry10 OS | seL4

Hardware | CPU

ARMA Example



```
Last login: Mon Oct 14 19:33:23 on ttys064
/tmp/tmp.lpWOySOVOu ; exit;
[~]$ /tmp/tmp.lpWOySOVOu ; exit;
Connecting...
Erlang/OTP 26 [erts-14.1] [source] [64-bit] [smp:1:1] [ds:1:1:1] [async-threads:1]

Interactive Elixir (1.15.7) - press Ctrl+C to exit (type h() ENTER for help)
iex(a@rmserver)1>
```

Video Available

```
meout}. Attempting to reconnect
|     65.746| Poukai.admin     |
|     65.747| Poukai.admin     | 19:32:55.502 [info] Connection has been lost. Reason: {:error, :ti
meout}. Attempting to reconnect
|     76.761| Poukai.admin     |
|     76.762| Poukai.admin     | 19:33:06.516 [info] Connection has been lost. Reason: {:error, :ti
meout}. Attempting to reconnect
|     86.246| Poukai.admin     |
|     86.247| Poukai.admin     | 19:33:15.997 [debug] Connection has been established
|     86.433| Poukai.admin     |
|     86.433| Poukai.admin     | 19:33:16.006 [debug] Challenge received
|     87.468| Poukai.admin     |
|     87.468| Poukai.admin     | 19:33:17.223 [debug] Received text frame {"args":[],"command":"fet
ch_manifest","id":"daWQefBGzMw"}
|     96.158| Poukai.admin     |
|     96.159| Poukai.admin     | 19:33:25.907 [debug] Received text frame {"args":[],"command":"fet
ch_manifest","id":"Jol9zFGAnBs"}
|    110.140| Poukai.admin     |
|    110.140| Poukai.admin     | 19:33:39.890 [debug] Received text frame {"args":[],"command":"fet
ch_manifest","id":"K4crIEf2wHo"}
|    135.268| Poukai.admin     |
|    135.268| Poukai.admin     | 19:34:05.022 [debug] Received text frame {"args":[],"command":"fet
ch_manifest","id":"nEZCQ1Hu2DQ"}
```

ARMA Technical Requirements

- System Configurations
  - Specify and instantiate system configurations
  - Reason about configurations (e.g. calculate deltas)
- Dynamics
  - Semi-dynamic (change between pre-configured systems)
  - Add/remove components, Allocate and deallocate resources
  - Set up and teardown connections
- Isolation
  - Protection between components (Operation vs Protection)
  - Protected access to resources (e.g. dormant components)
- Assurance
  - Assurance of operations

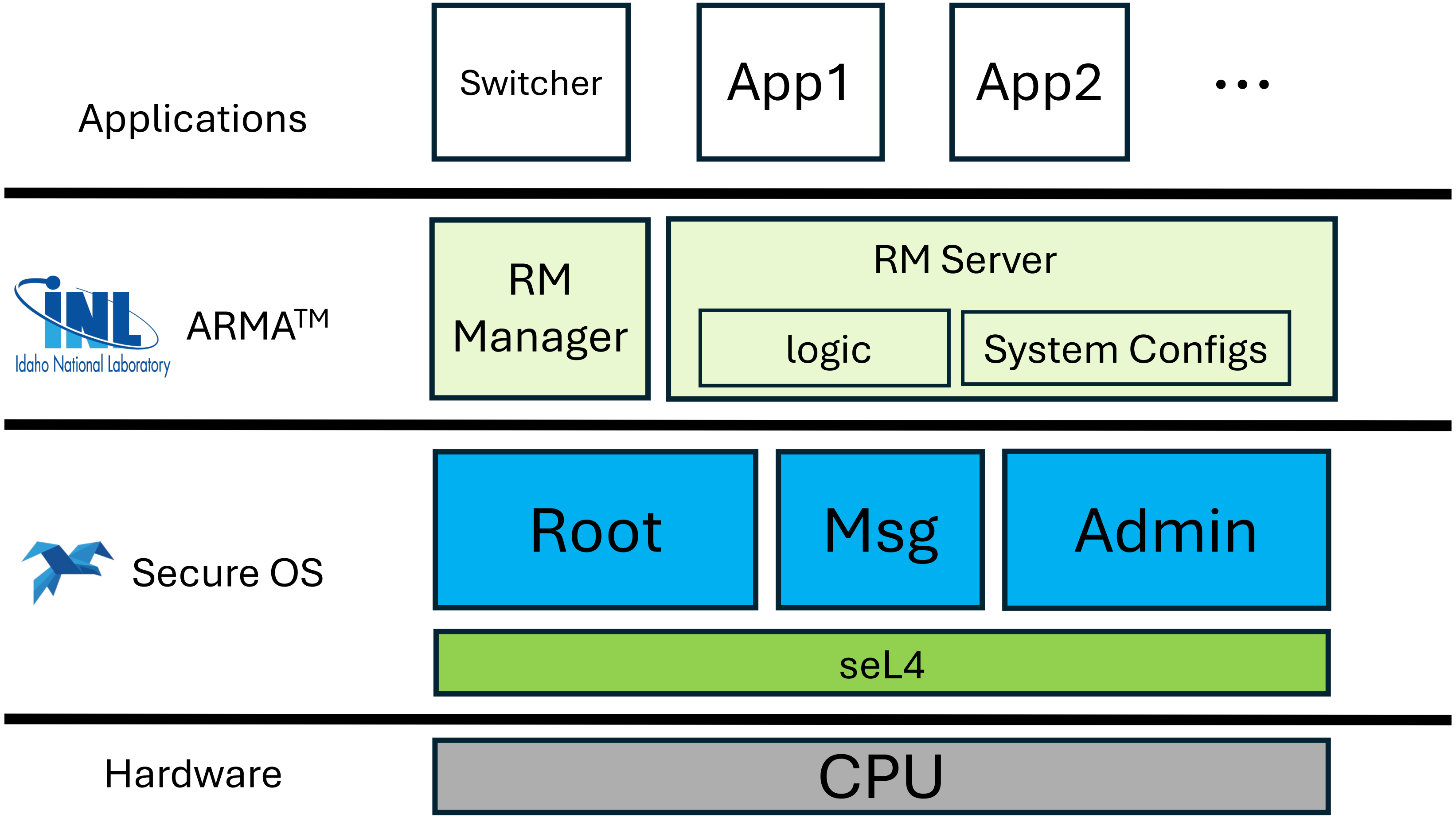
ARMA on seL4

- System Configurations
  - CapDL (also sel4 calls, CAmkES, microkit, etc.)
- Dynamics
  - Untyped retype
  - Cap transfer
  - Revocation and deletion of caps
- Isolation
  - Capabilities
  - Cspaces and vspaces
- Assurance
  - Verified kernel

Challenges

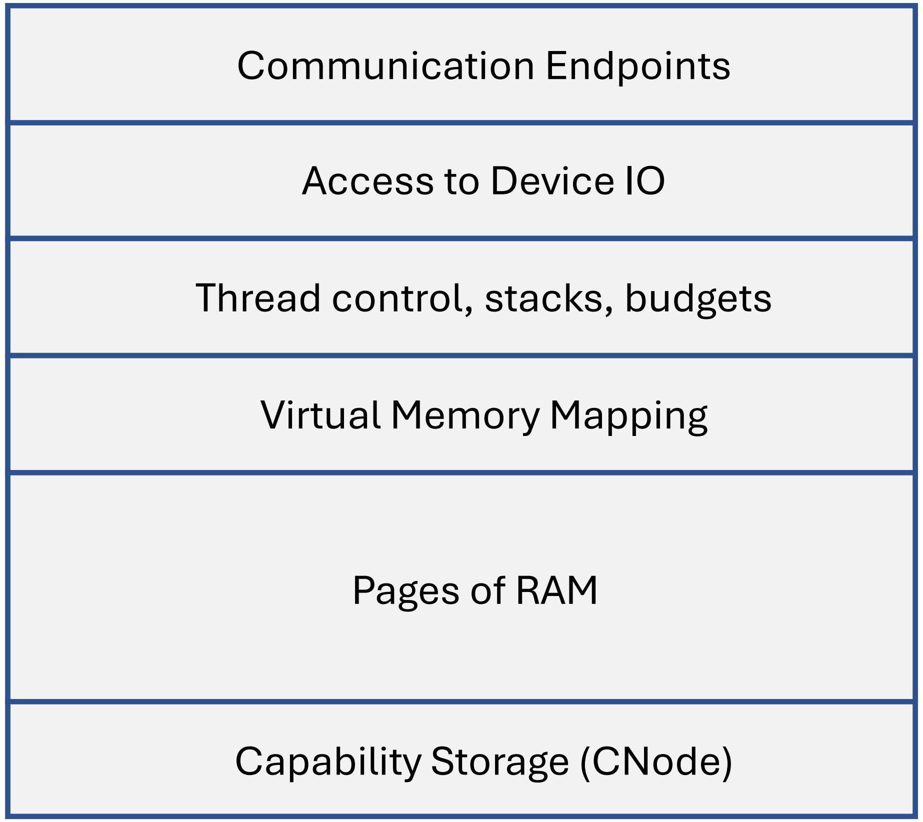
- System Configuration spec: CapDL
    - Too specific? Component internal details
    - Not specific enough? Backing UTs for resources?
- Dynamics
    - Set up Component resources for easy allocation and deallocation
        - Bookkeeping for deallocation
    - Flexibility for components to do what they want with their resources
        - Minimum policy, but enforce isolation
- Connections
    - Disconnect: remove endpoint, notification, shared memory from component.
    - Avoid accessing removed resources
    - Reconnect: add endpoint, notification, shared memory to component

Kry10 ARMA (K-ARMA): Overview



K-ARMA: Resource Management

- Problem
  - Bookkeeping componet's resources



Communication Endpoints

Access to Device IO

Thread control, stacks, budgets

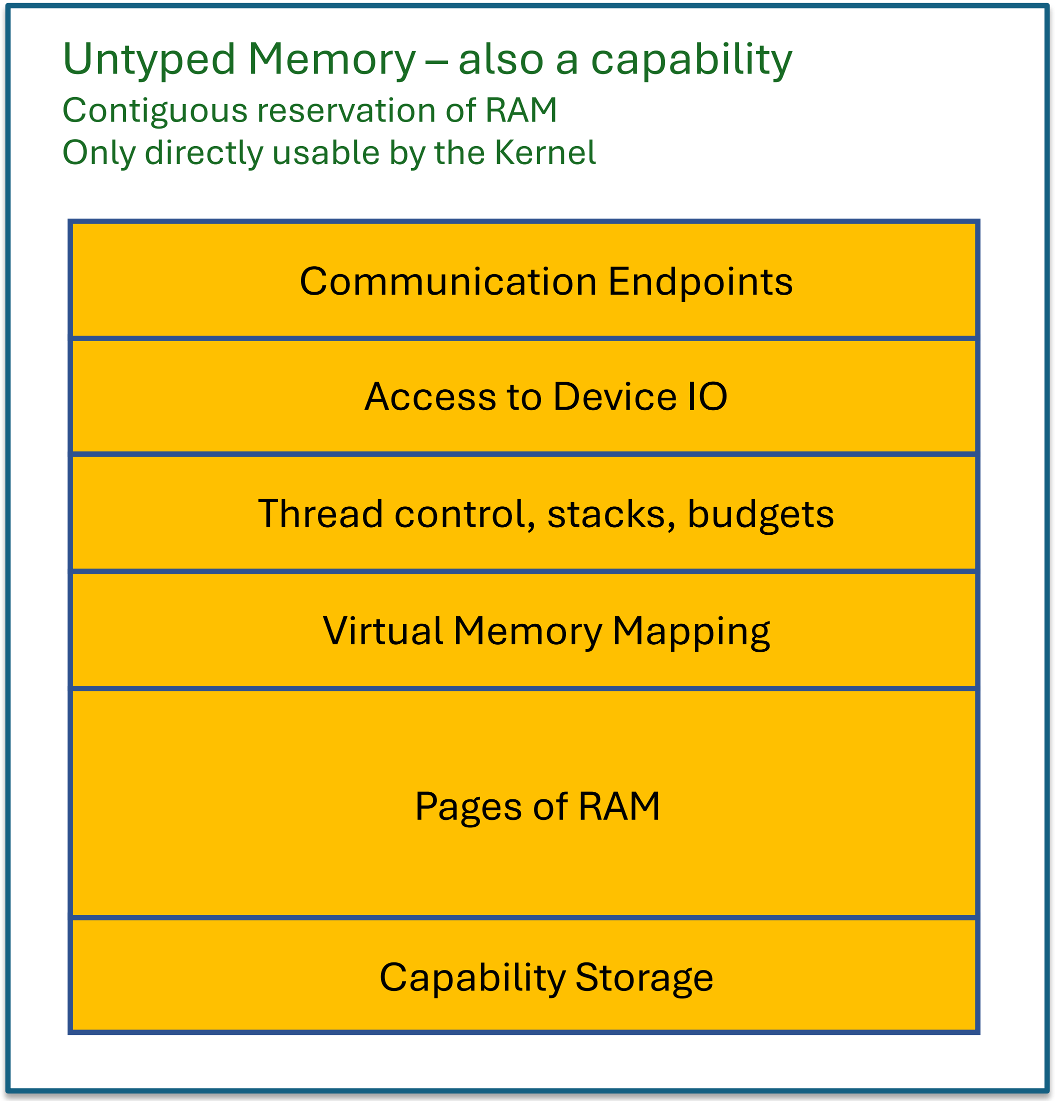
Virtual Memory Mapping

Pages of RAM

Capability Storage (CNode)

Kry10 ARMA Approach

- Problem
  - Bookkeeping componet's resources
- Build a sandbox
  - Define Untyped Memory
  - Allocate all other caps from it
  - Load code & run
- Reset a sandbox
  - Revoke the Untyped Memory
- Revocation is Verified
  - This is the only “garbage collector” needed



Untyped Memory – also a capability

Contiguous reservation of RAM
Only directly usable by the Kernel

Communication Endpoints

Access to Device IO

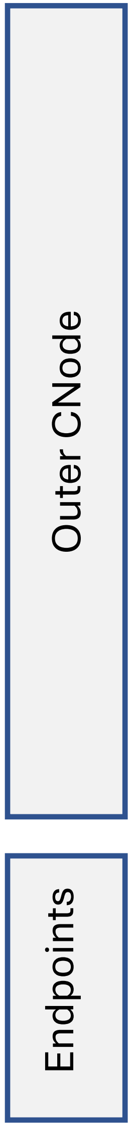
Thread control, stacks, budgets

Virtual Memory Mapping

Pages of RAM

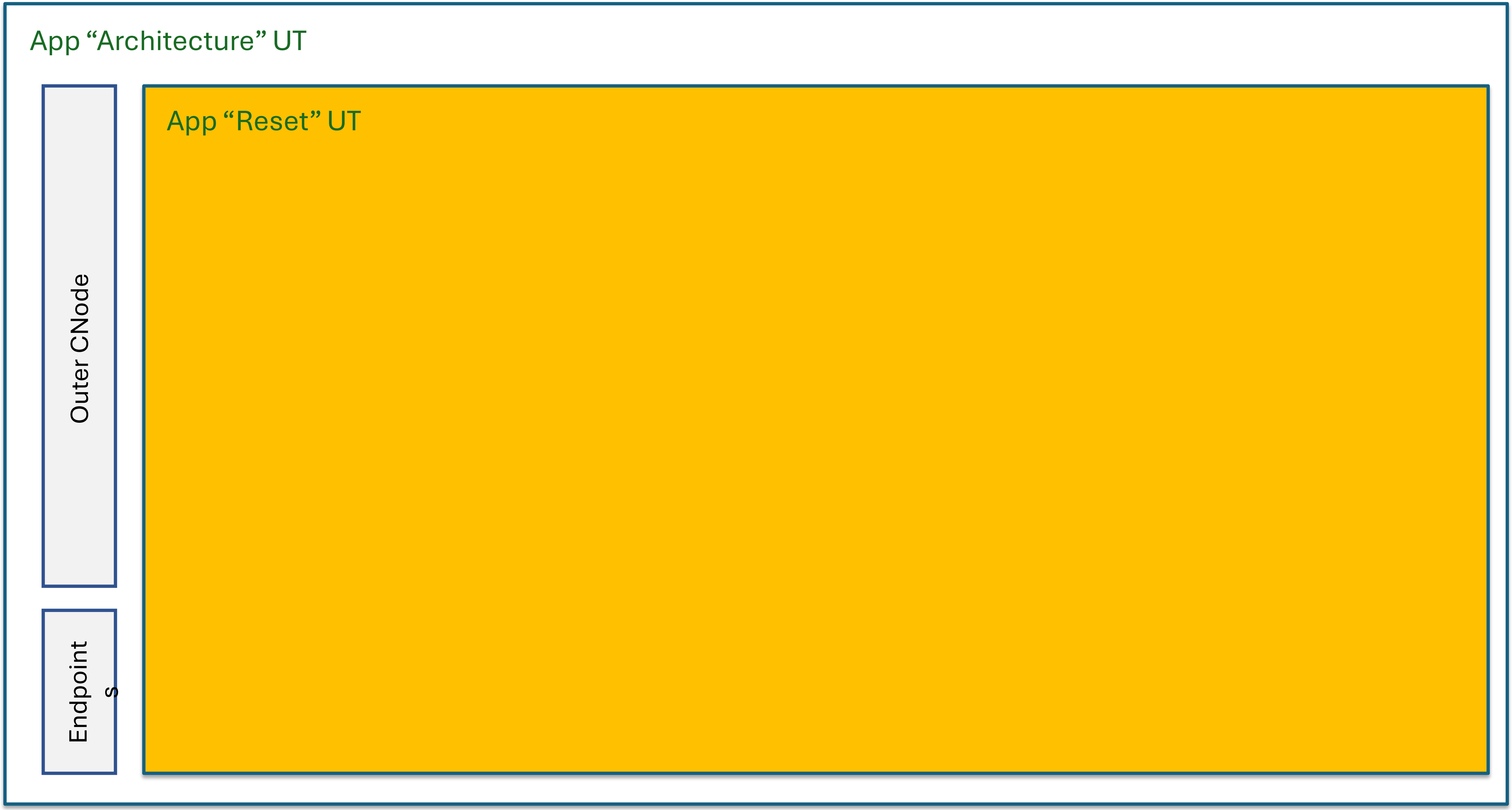
Capability Storage

App “Architecture” UT



Outer CNode

Endpoints

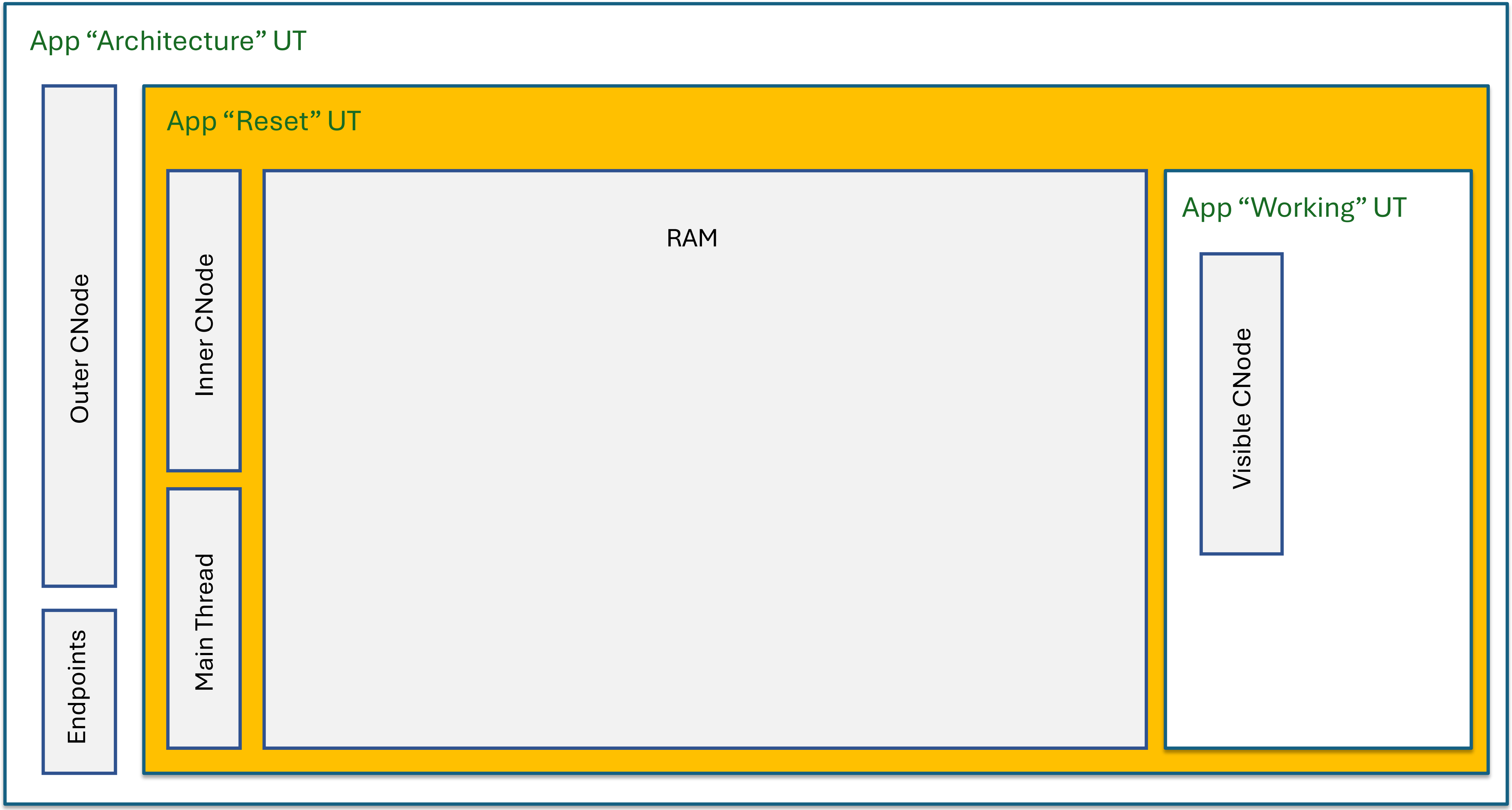


App “Architecture” UT

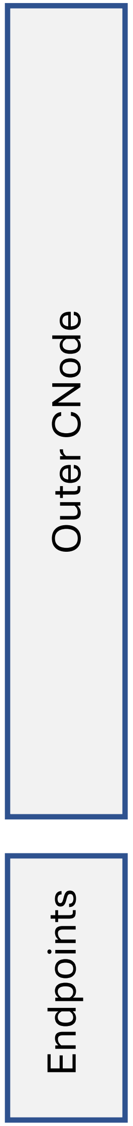
Outer CNode

Endpoints

App “Reset” UT

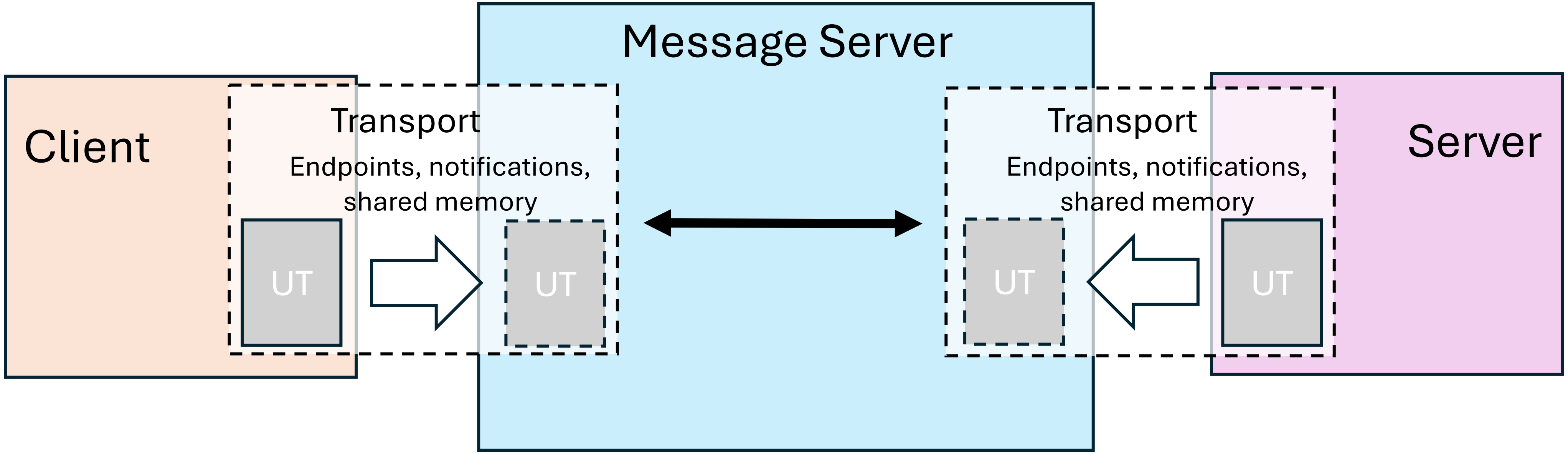

App “Architecture” UT
Outer CNode
Endpoints
App “Reset” UT
Inner CNode
Main Thread
RAM
App “Working” UT
Visible CNode

App “Architecture” UT



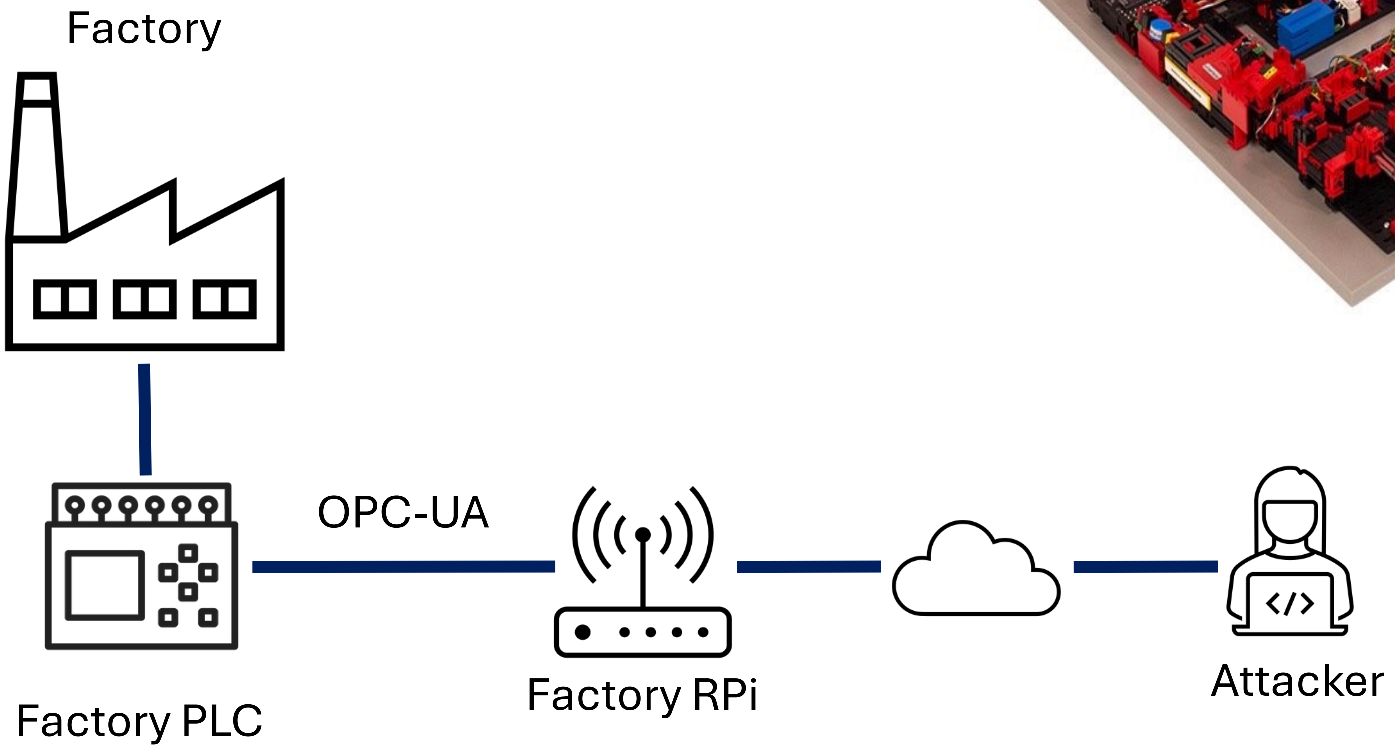
K-ARMA: Connections

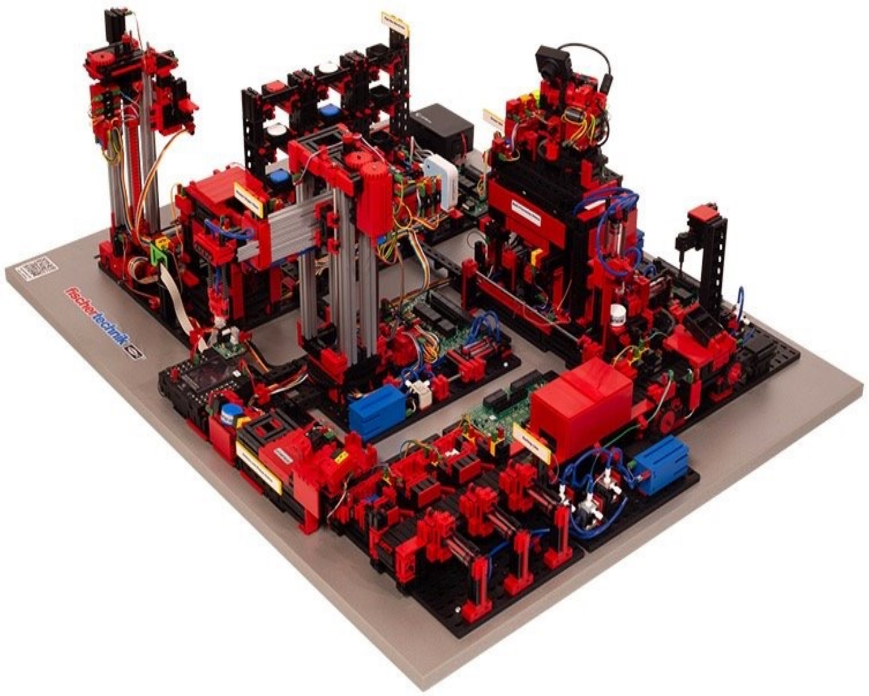
- Problem
  - Disconnecting and re-connecting
  - Without forcing structure and collaboration on components
- Message Server
  - Mediates creation of connections
  - Uses UTs from components for resources
  - New components re-connect explicitly


Message Server
Client
Transport
Endpoints, notifications, shared memory
UT
UT
Transport
Endpoints, notifications, shared memory
UT
UT
Server

Kry10 ARMA in Action

- ARMA for ***FT Factory Guard***

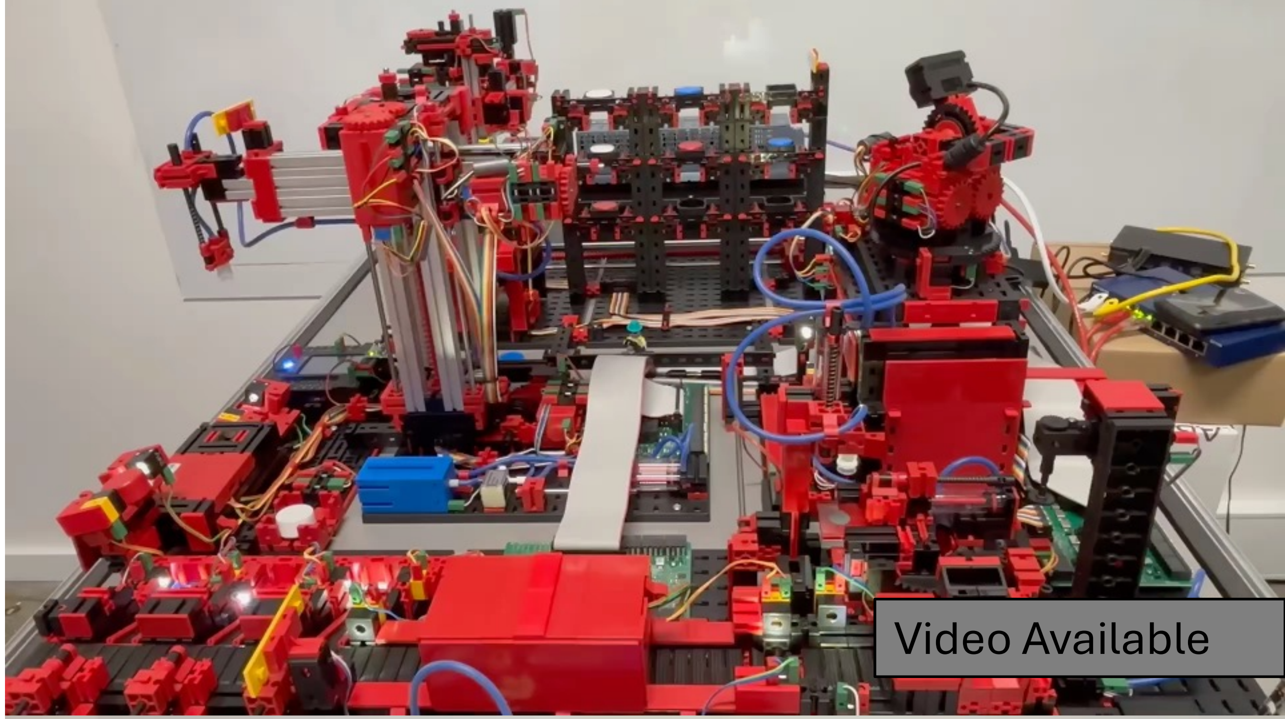




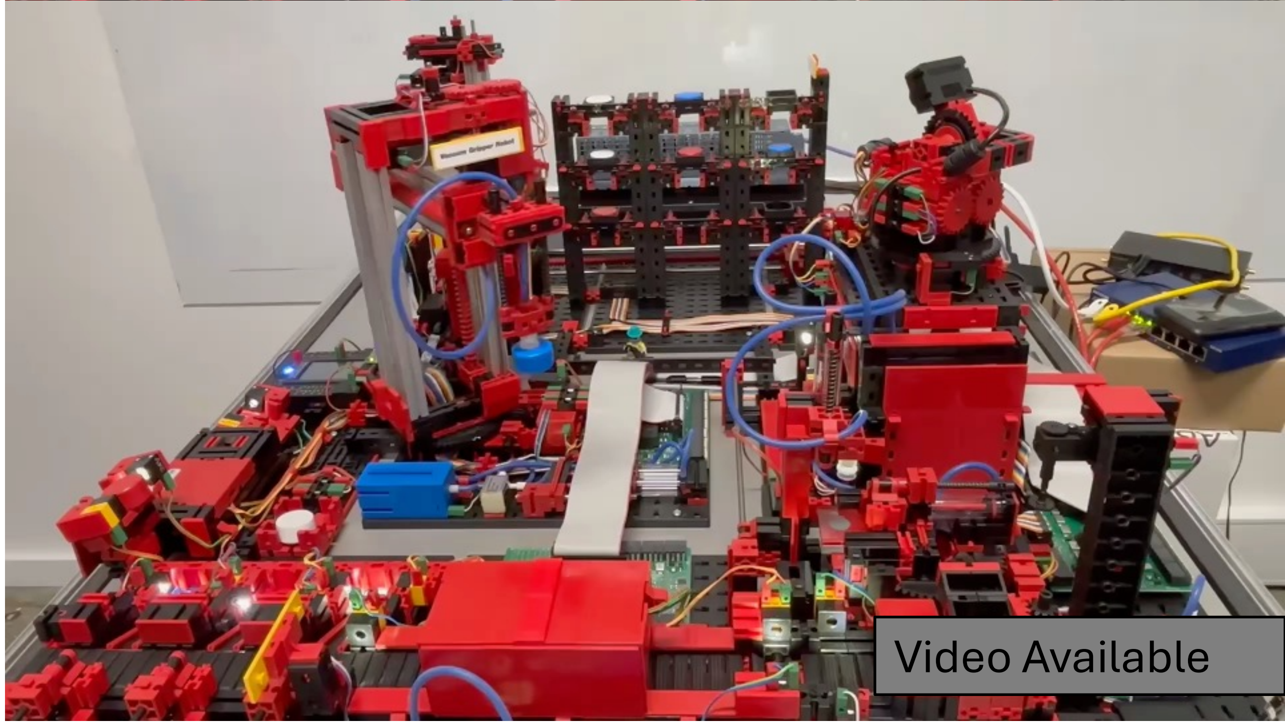
FT Factory: Attacks

Vulnerable to attacks

- OT connected to IT and Internet
- Commodity OS (Linux) on controllers
- Communication unencrypted
  - OPC-UA, MQTT



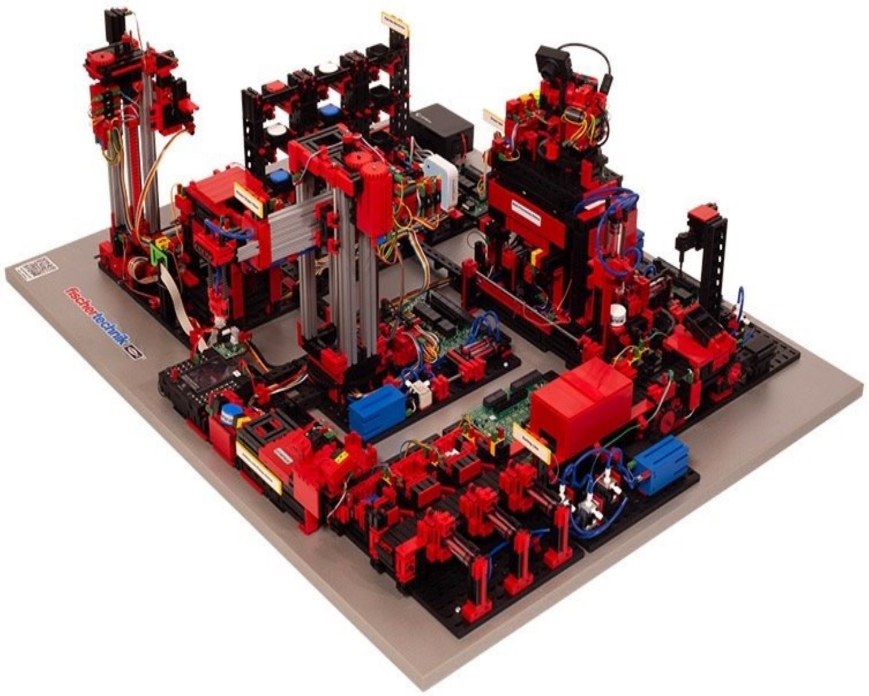
Video Available

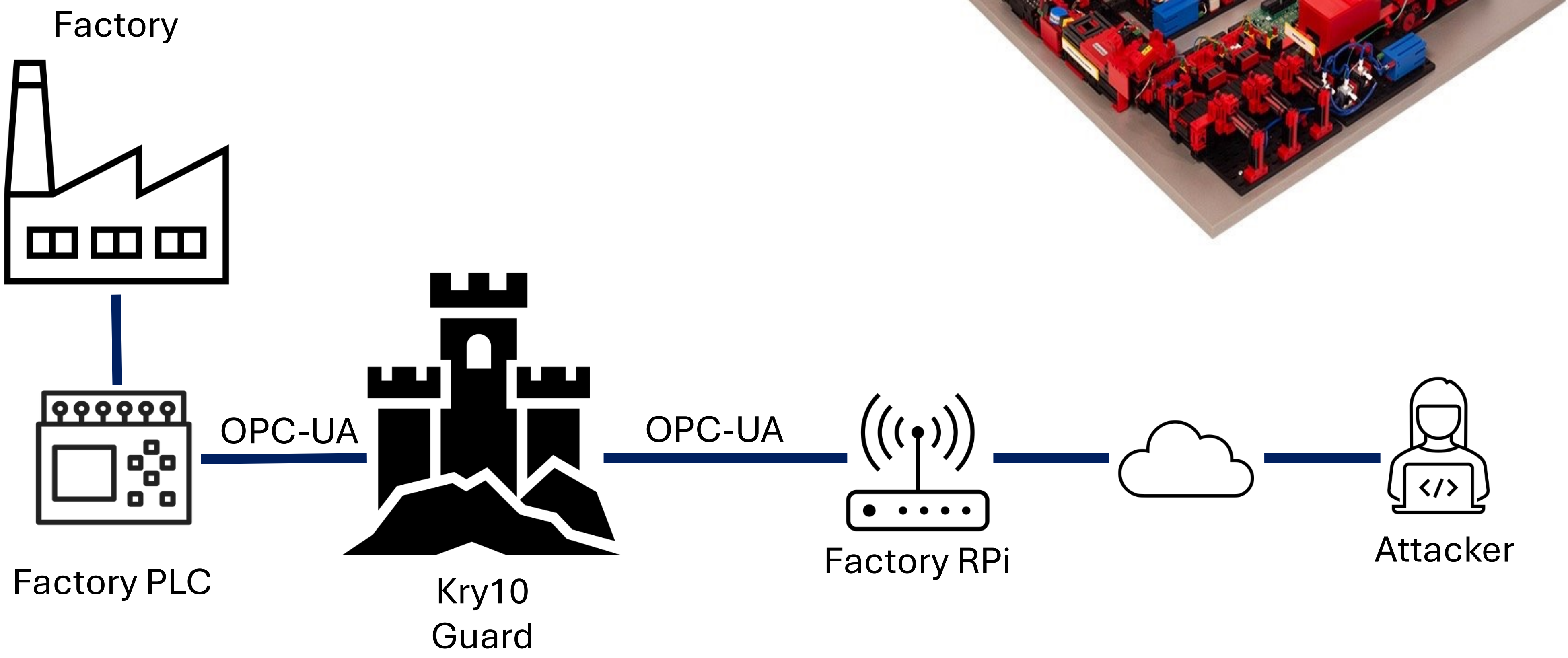


Video Available

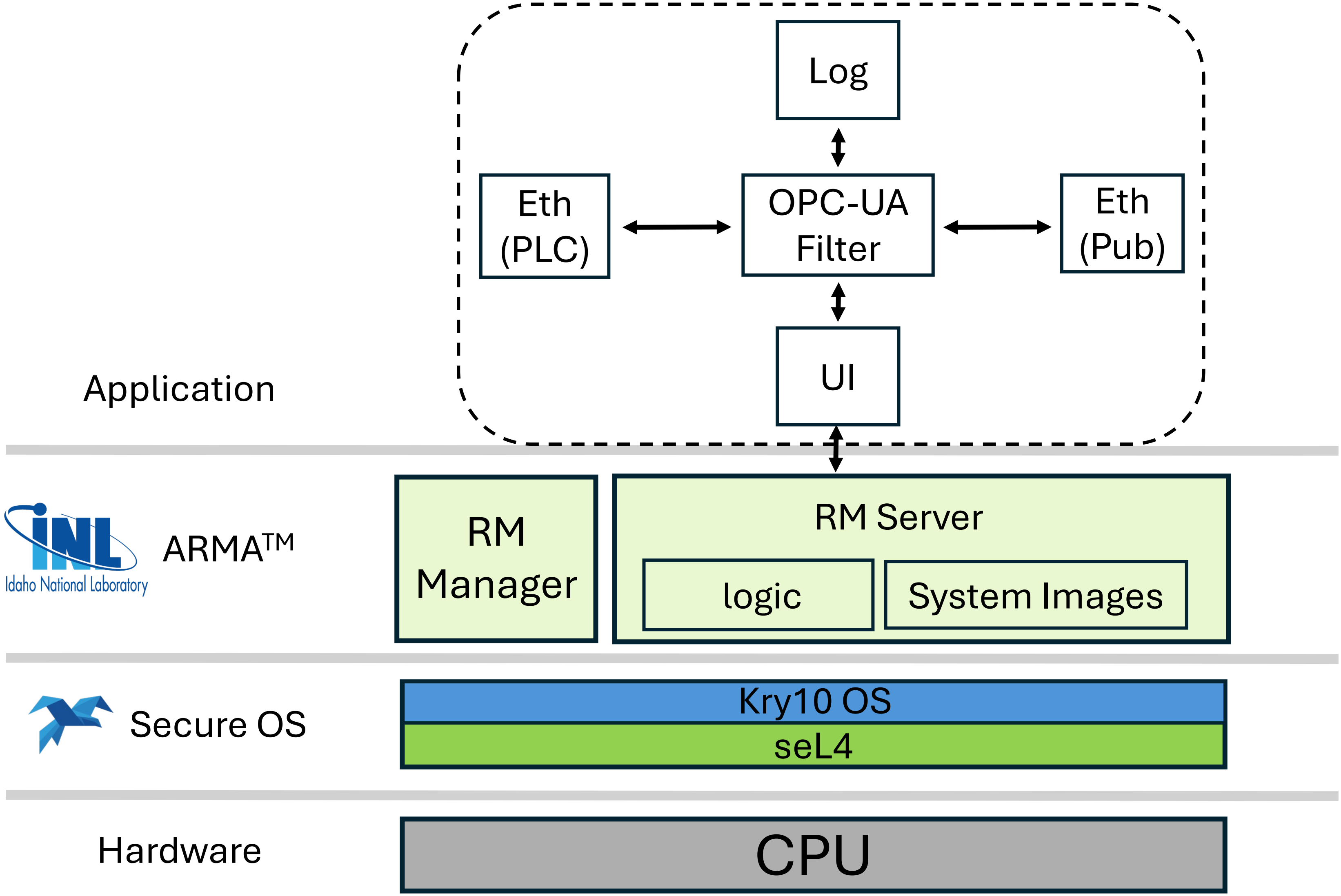
Kry10 ARMA in Action

- ARMA for ***FT Factory Guard***



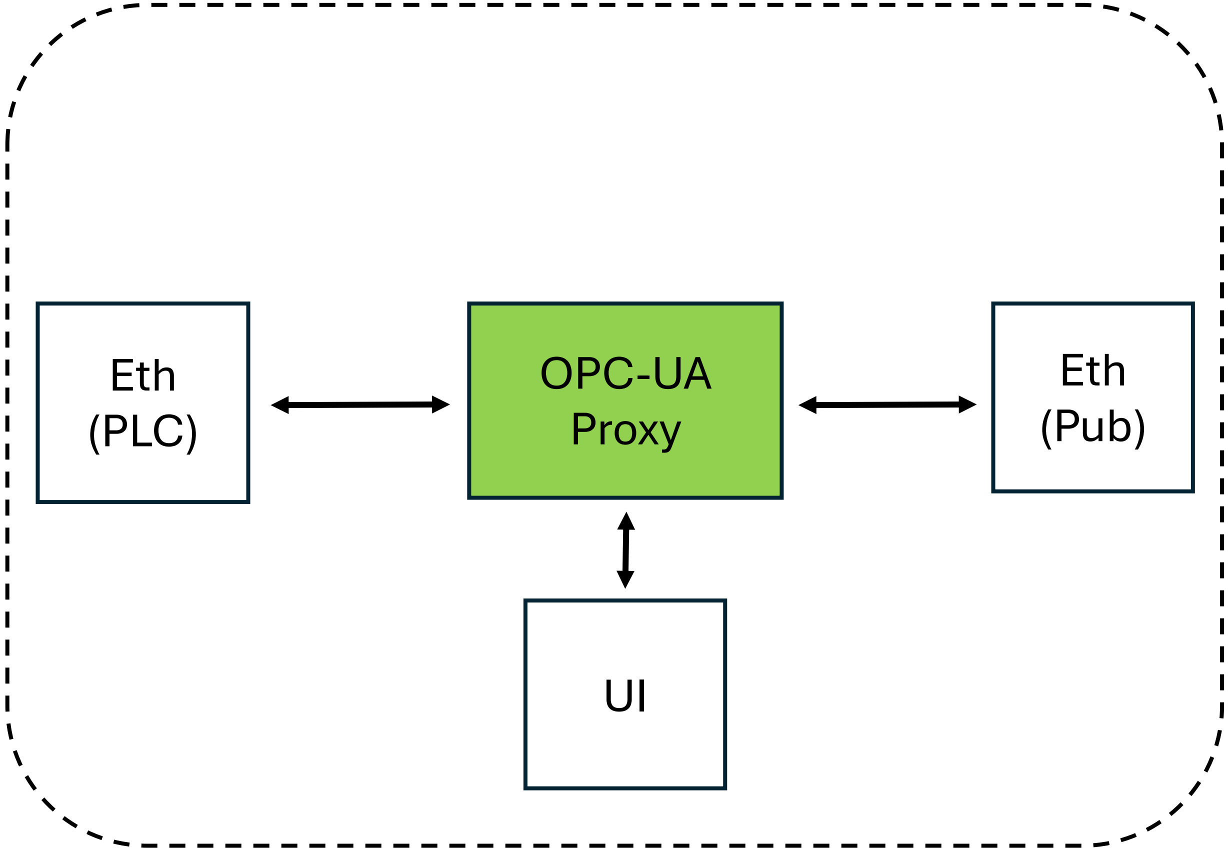


FT Factory Guard



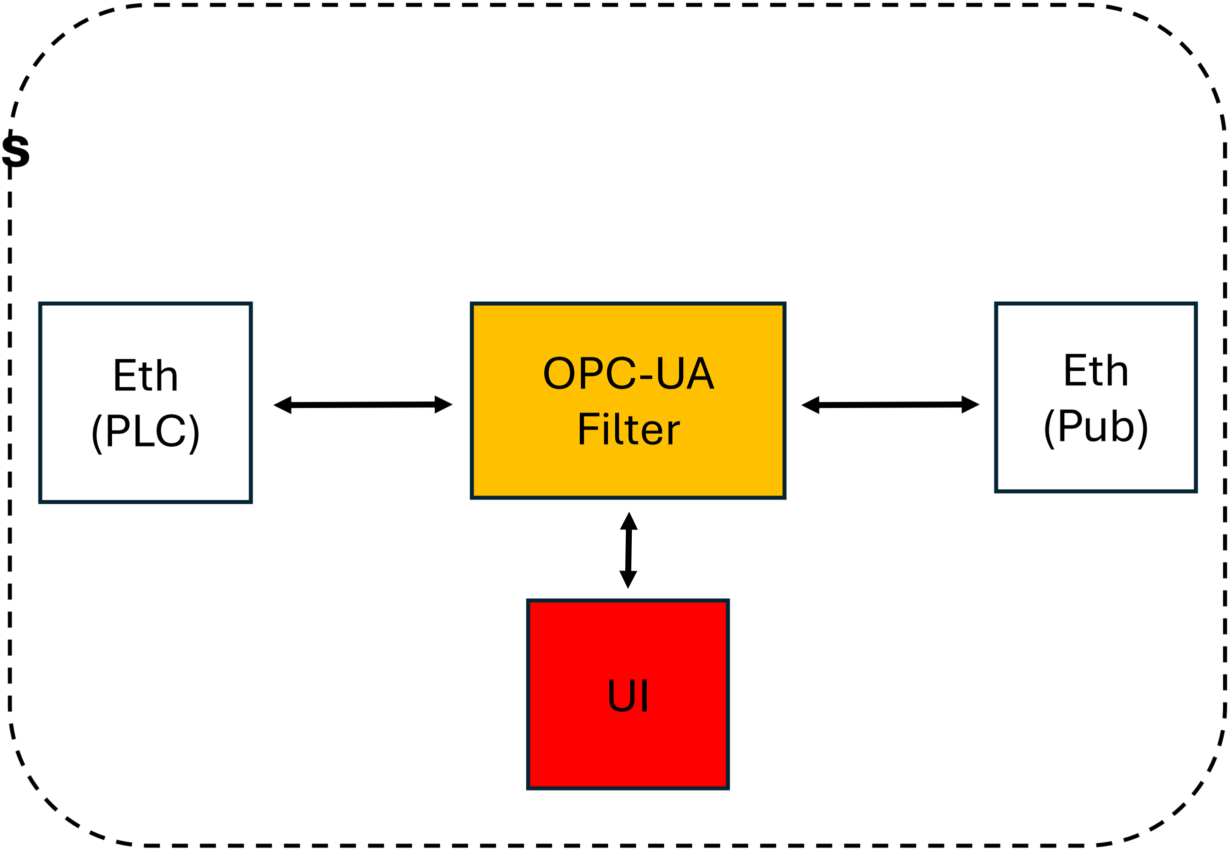
FT Factory Guard Reserve Modes

- Modes
  - **Normal: No Protection**
  - Filter: Filter out known attacks
  - Logging: Log all traffic
  - Disconnect: Disconnect PLC from Network
- Manual switch
- Automatic switch



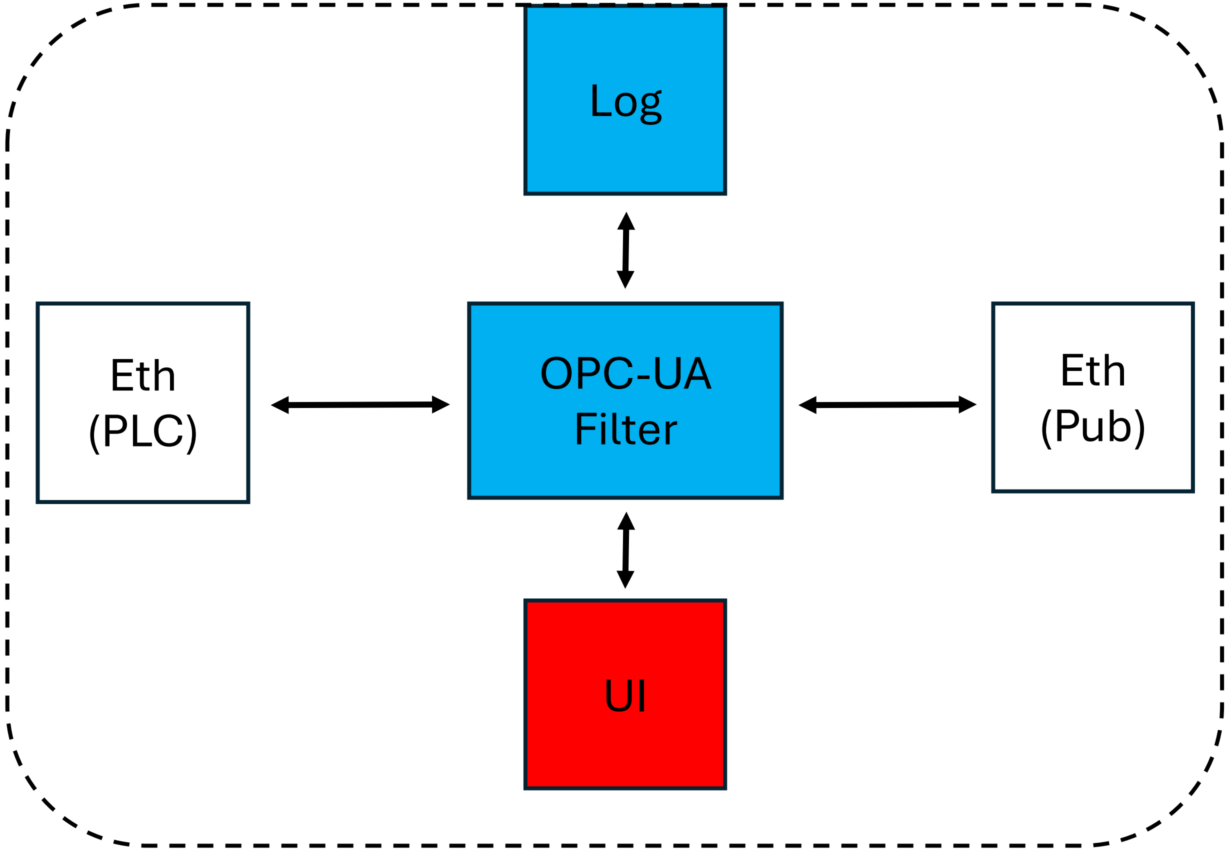
FT Factory Guard Reserve Modes

- Modes
  - Normal: No Protection
  - **Filter: Filter out known attacks**
  - Logging: Log all traffic
  - Disconnect: Disconnect PLC from Network
- Manual switch
- Automatic switch



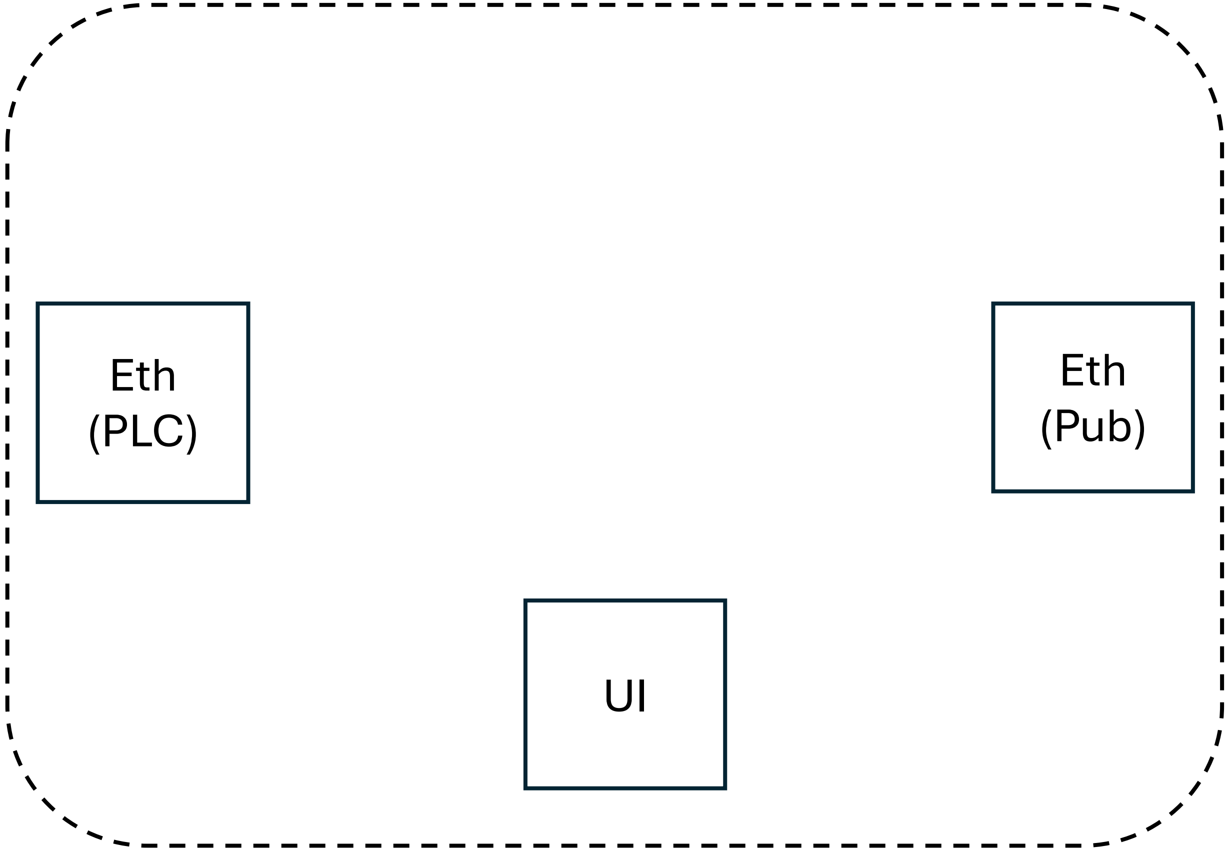
FT Factory Guard Reserve Modes

- Modes
    - Normal: No Protection
    - Filter: Filter out known attacks
    - **Logging: Log all traffic**
    - Disconnect: Disconnect PLC from Network
- Manual switch
- Automatic switch

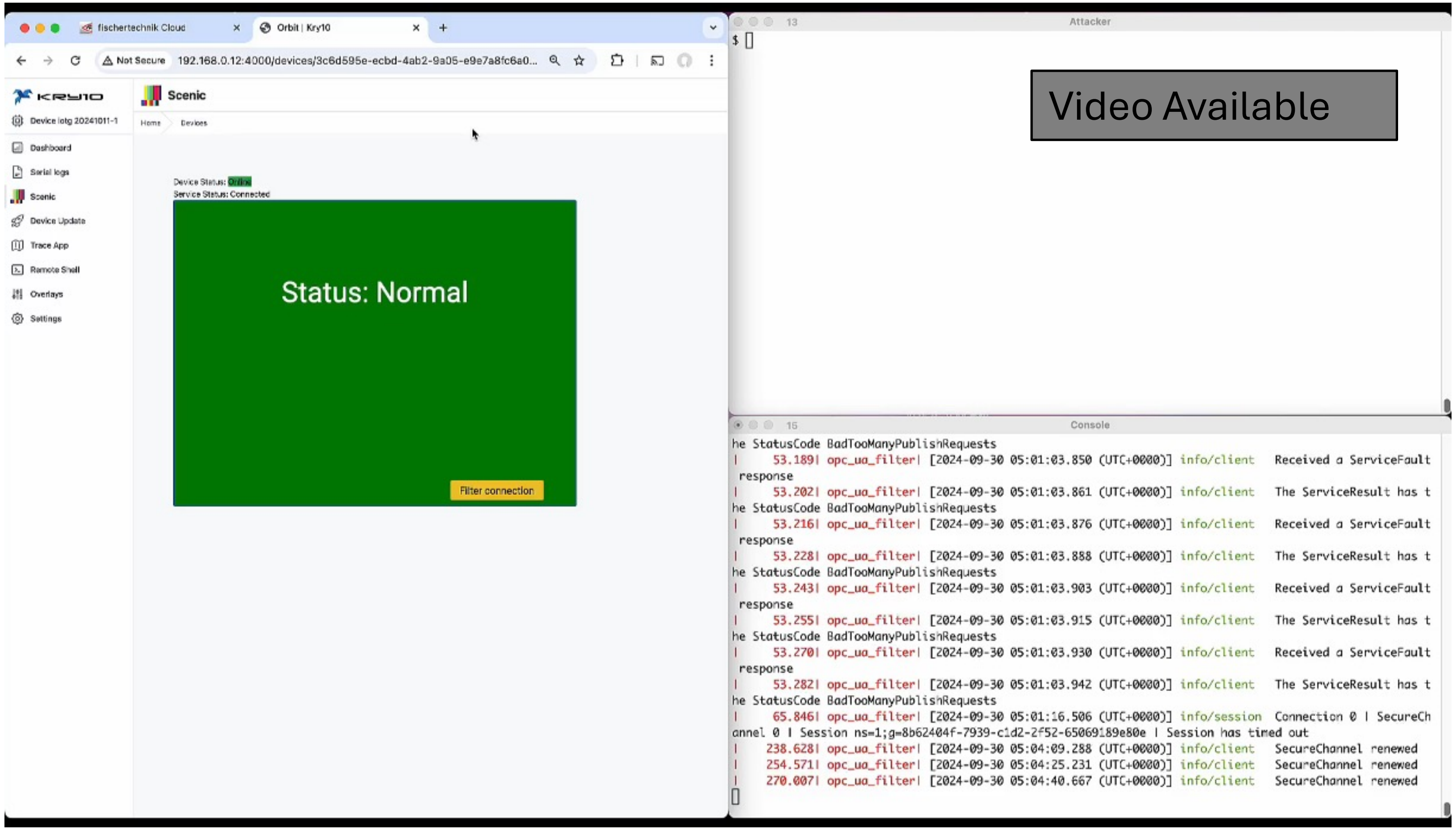


FT Factory Guard Reserve Modes

- Modes
  - **Normal: No Protection**
  - Filter: Filter out known attacks
  - Logging: Log all traffic
  - **Disconnect: Disconnect PLC from Network**
- Manual switch
- Automatic switch



FT Factory Guard ARMA in Action



Device Status: Online
Service Status: Connected

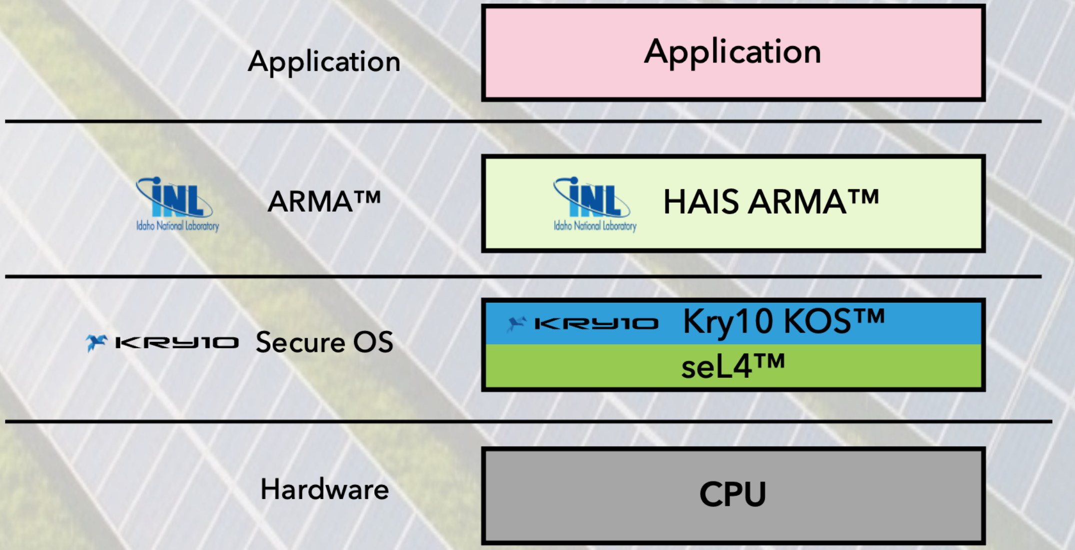
Status: Normal

```
$ 
```

```
he StatusCode BadTooManyPublishRequests
|     53.189| opc_ua_filter| [2024-09-30 05:01:03.850 (UTC+0000)] info/client   Received a ServiceFault
 response
|     53.202| opc_ua_filter| [2024-09-30 05:01:03.861 (UTC+0000)] info/client   The ServiceResult has t
he StatusCode BadTooManyPublishRequests
|     53.216| opc_ua_filter| [2024-09-30 05:01:03.876 (UTC+0000)] info/client   Received a ServiceFault
 response
|     53.228| opc_ua_filter| [2024-09-30 05:01:03.888 (UTC+0000)] info/client   The ServiceResult has t
he StatusCode BadTooManyPublishRequests
|     53.243| opc_ua_filter| [2024-09-30 05:01:03.903 (UTC+0000)] info/client   Received a ServiceFault
 response
|     53.255| opc_ua_filter| [2024-09-30 05:01:03.915 (UTC+0000)] info/client   The ServiceResult has t
he StatusCode BadTooManyPublishRequests
|     53.270| opc_ua_filter| [2024-09-30 05:01:03.930 (UTC+0000)] info/client   Received a ServiceFault
 response
|     53.282| opc_ua_filter| [2024-09-30 05:01:03.942 (UTC+0000)] info/client   The ServiceResult has t
he StatusCode BadTooManyPublishRequests
|     65.846| opc_ua_filter| [2024-09-30 05:01:16.506 (UTC+0000)] info/session  Connection 0 | SecureCh
annel 0 | Session ns=1;g=8b62404f-7939-c1d2-2f52-65069189e80e | Session has timed out
|    238.628| opc_ua_filter| [2024-09-30 05:04:09.288 (UTC+0000)] info/client   SecureChannel renewed
|    254.571| opc_ua_filter| [2024-09-30 05:04:25.231 (UTC+0000)] info/client   SecureChannel renewed
|    270.007| opc_ua_filter| [2024-09-30 05:04:40.667 (UTC+0000)] info/client   SecureChannel renewed
```

Video Available

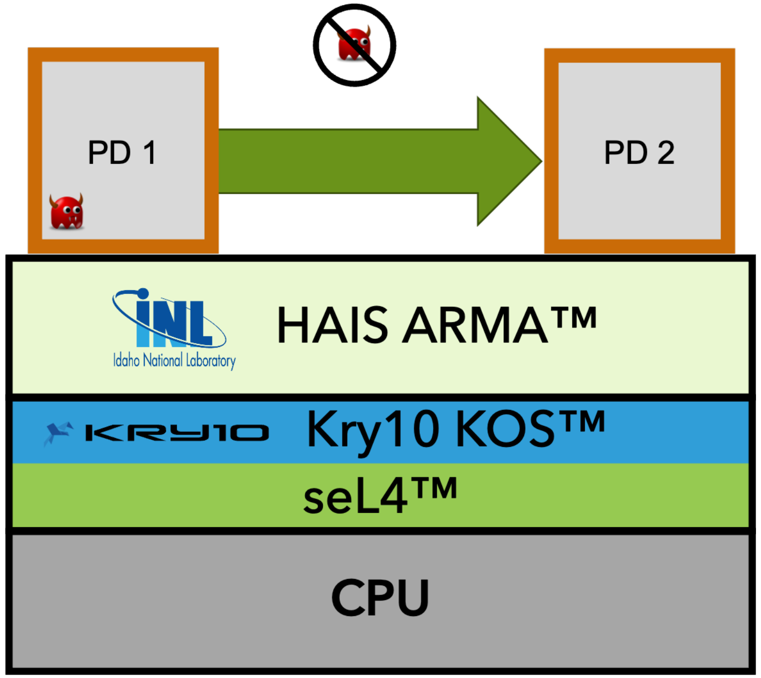
Protecting Critical Infrastructure – Greenfields



- New builds allows freedom of design

- **STOP COMPROMISE**: Assure critical infrastructure is not being held ***at risk***

- **ASSURED RESILIENCE**: Combat effects, (adversarial, natural faults, or developmental errors) before severe compromises occur



- seL4 makes it hard for and adversary to migrate to between PDs
- Serious attacks can still happen from a compromised PD
  - Functional manipulation
  - State manipulation
- Two ARMA Approaches
  - Distribution system functionality over PDs ➡
  - Finer granularity on communication for message passing systems ➡

➡

Classes of Attacks of the FT-ICS

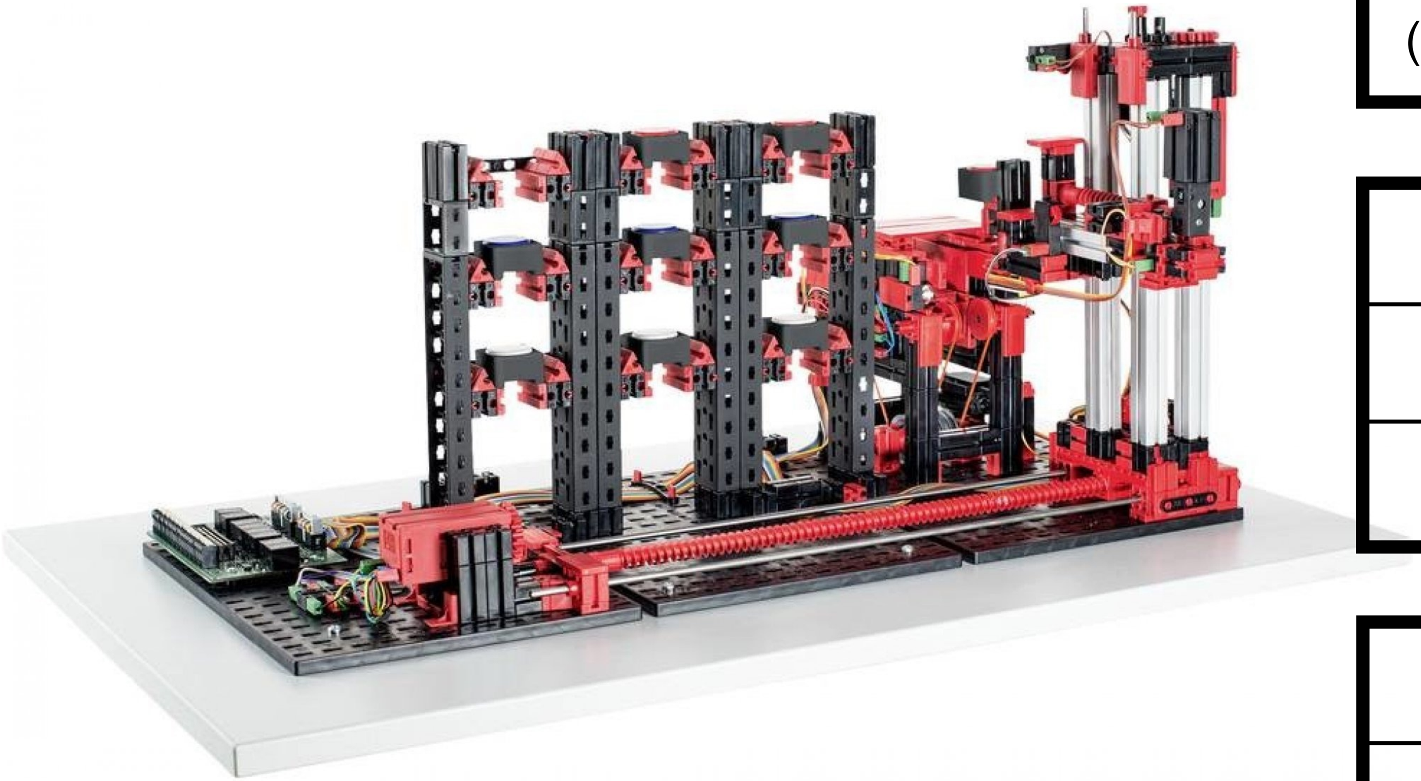
1. Information Leakage (Confidentiality)

2. Affect quality / quantity of manufactured product

3. Manipulation of Manufacturing Information State
   - Physical Damage

4. Forced Physical–Physical State Interaction
   - Physical Damage

High-Bay Warehouse



(1,1)	(1,2)	(1,3)
(2,1)	(2,2)	(2,3)
(3,1)	(3,2)	(3,3)

Bay Positions

E	E	E
E	E	E
E	E	E

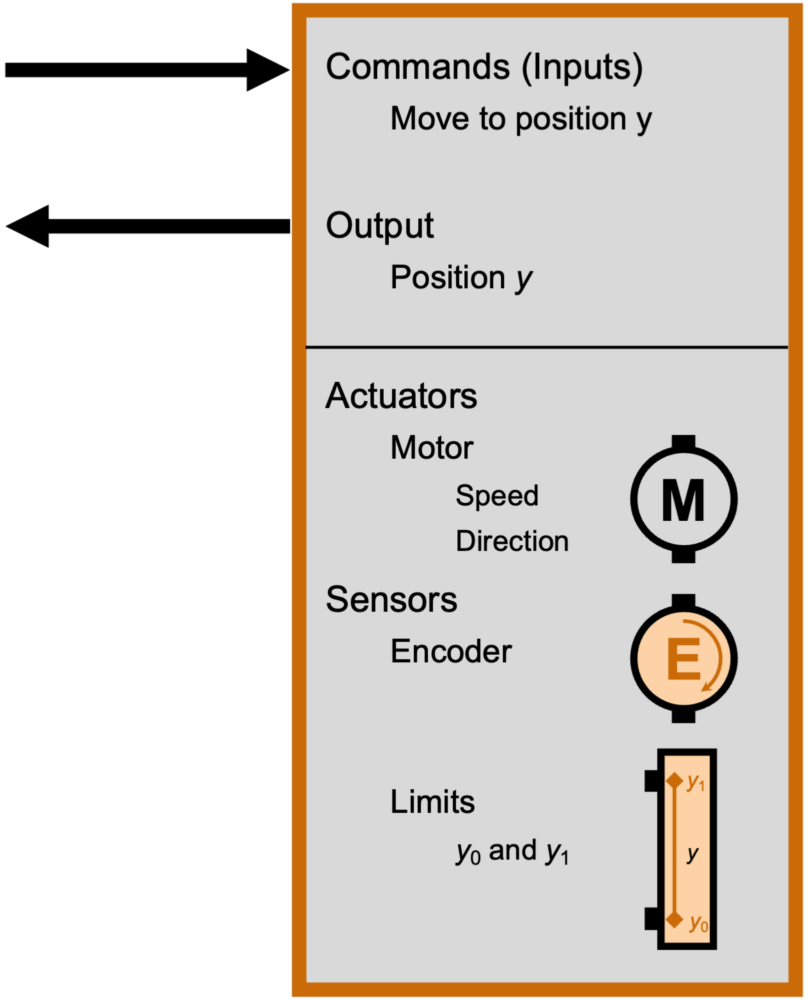
Initial State
(all empty)

E	E	🔵
E	🔴	E
E	🔵	E

Dynamic State

Protection Domain for 1D Linear Motion

- Physical Subsystem isolated in PD
  - Range-limited, limited motion in one dimension
- Restricted Commands
  - Move to position *y*
    - $y_0 < y < y_1$
- Reporting
  - At position y
- Easy to prove code is correct
  - Safety and Liveliness



Commands (Inputs)
Move to position y

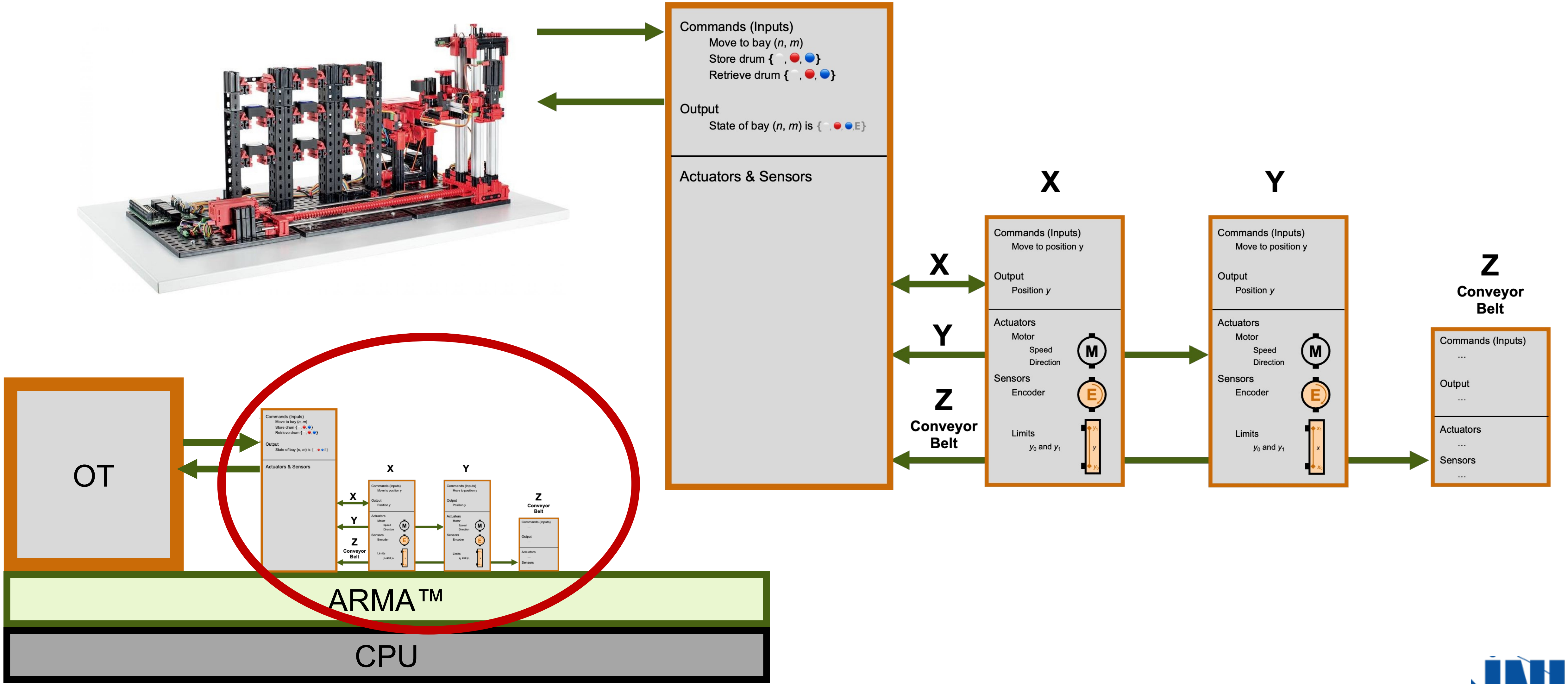
Output
Position *y*

Actuators
Motor
Speed
Direction

Sensors
Encoder

Limits
y_0 and y_1

ARM™ Architecture for High-Bay Warehouse



Commands (Inputs)

Move to bay (n, m)

Store drum { ⚪, 🔴, 🔵 }

Retrieve drum { ⚪, 🔴, 🔵 }

Output

State of bay (n, m) is { ⚪, 🔴, 🔵, E }

Actuators & Sensors

X

Commands (Inputs)

Move to position y

Output

Position y

Actuators

Motor

Speed

Direction

Sensors

Encoder

Limits

y_0 and y_1

Y

Commands (Inputs)

Move to position y

Output

Position y

Actuators

Motor

Speed

Direction

Sensors

Encoder

Limits

y_0 and y_1

Z Conveyor Belt

Commands (Inputs)

…

Output

…

Actuators

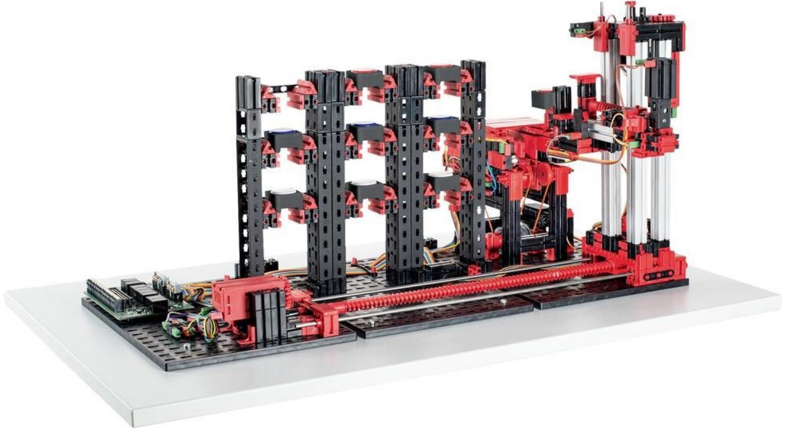
…

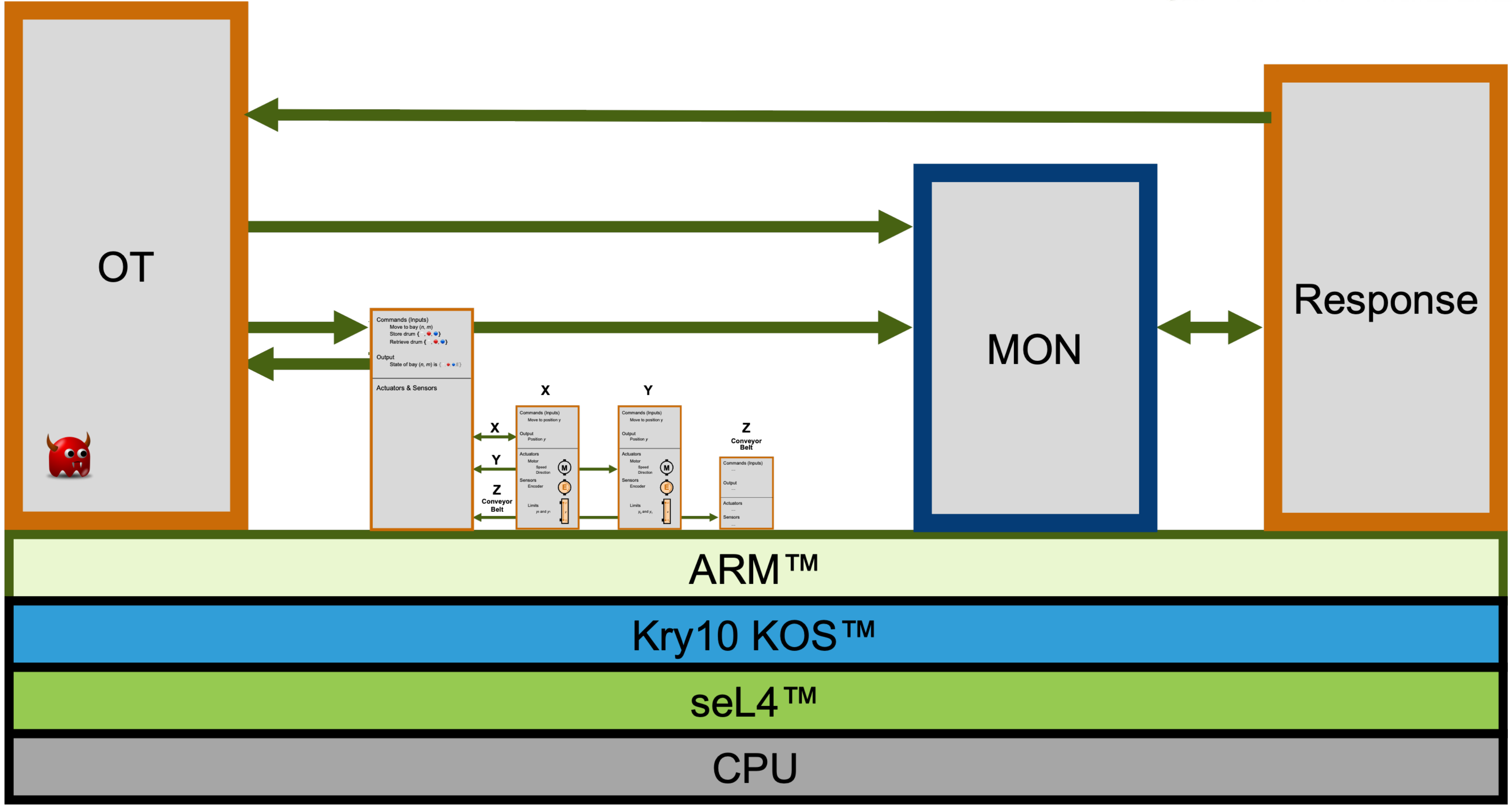
Sensors

…

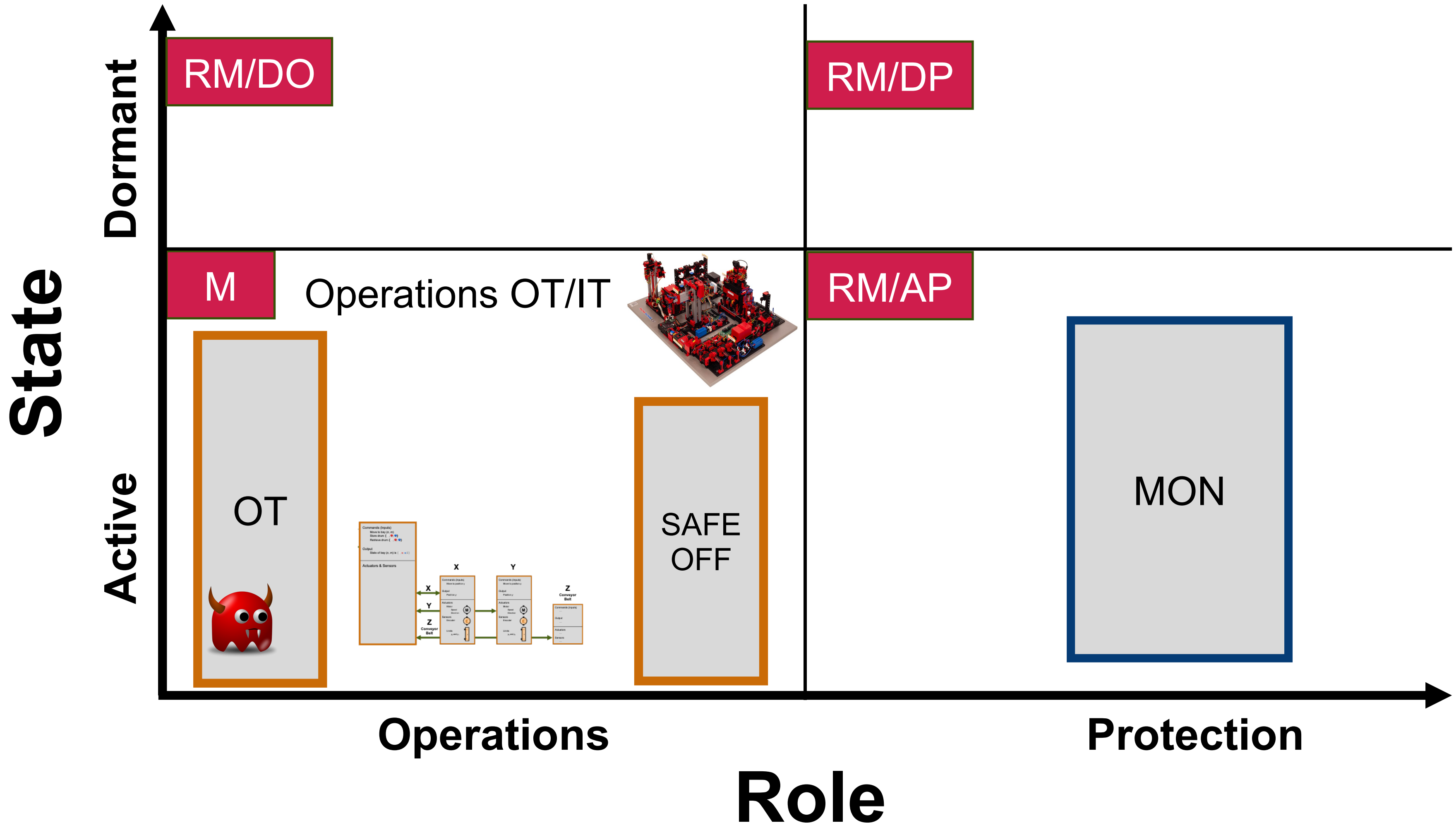
Commands (Inputs)
Move to bay (n, m)
Store drum { ⚪, 🔴, 🔵 }
Retrieve drum { ⚪, 🔴, 🔵 }
Output
State of bay (n, m) is { ⚪, 🔴, 🔵, E }
Actuators & Sensors
X
Y
Z Conveyor Belt

ARMA™ Example High-bay warehouse



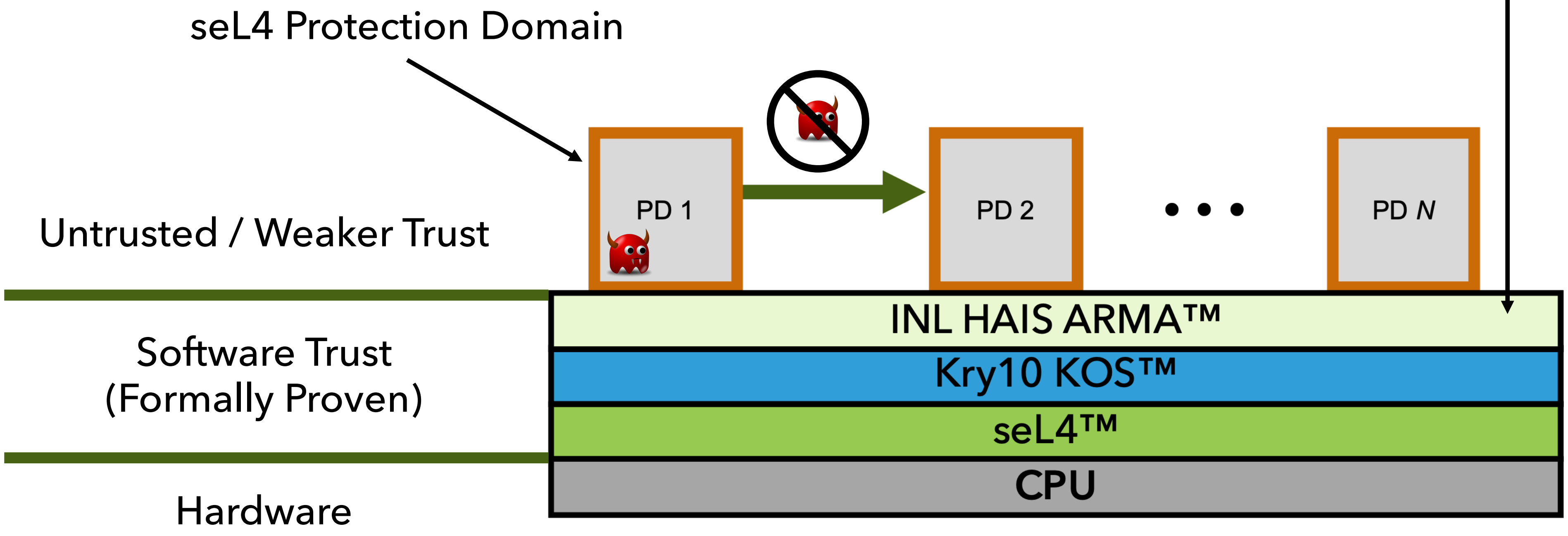


Modes, Reserve Modes, & Assured Reserve Modes

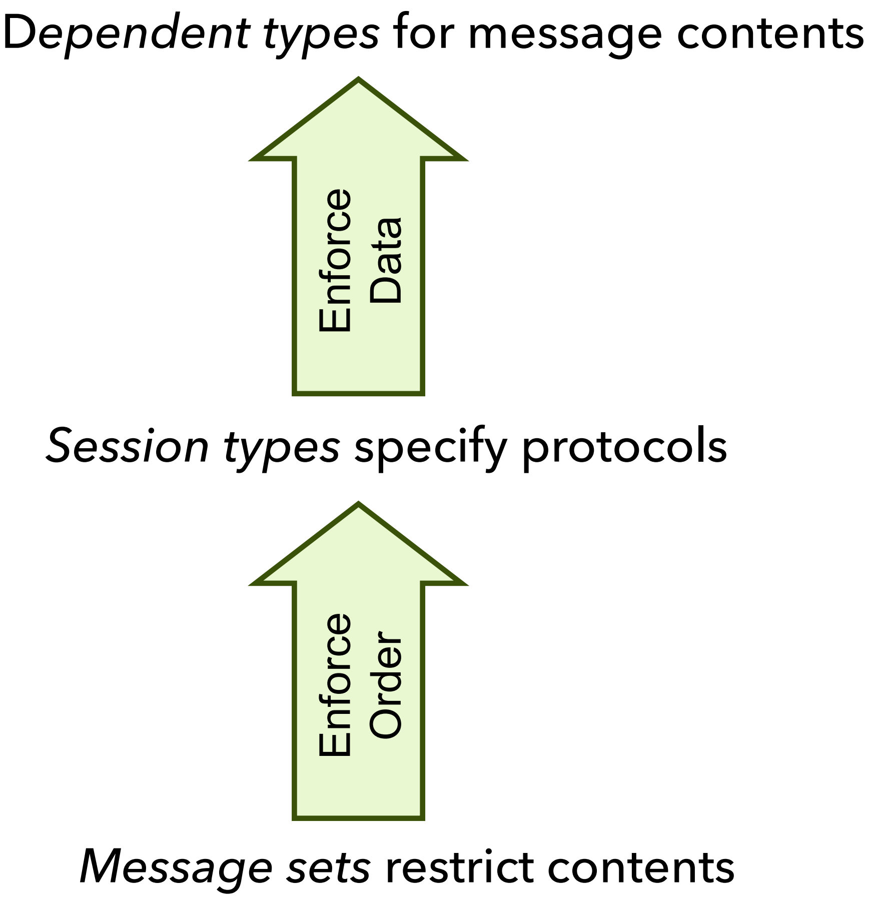


INL ARMA™ with DATUM

- Assured Reserve Mode Architecture (ARMA™)
  - Dynamically Assured Typed Universal Messages (DATUM)
    - Message sets restricts contents
    - Session Types restricts message ordering
    - Dependent message types restrict message data



DATUM



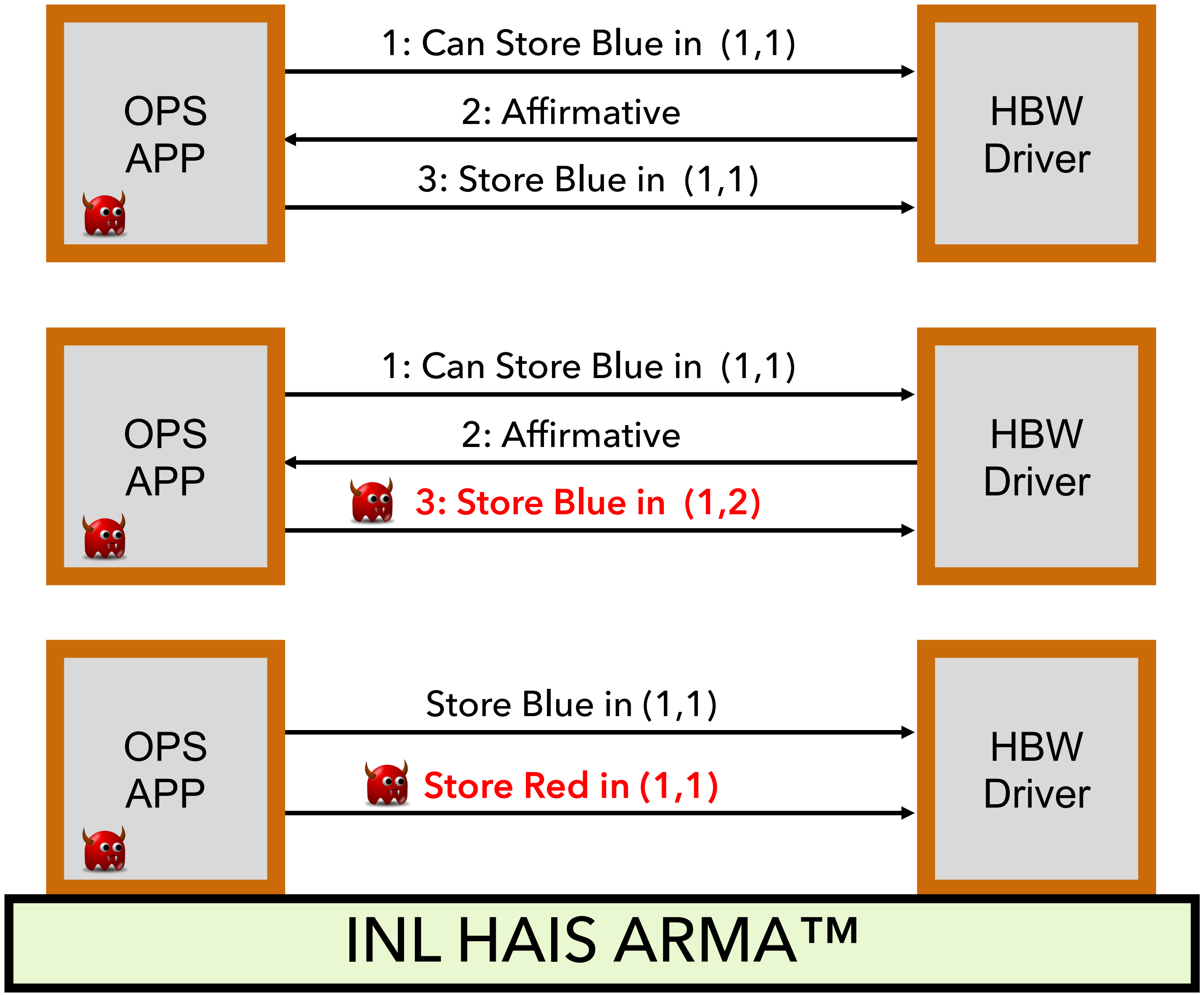
Dependent types for message contents

Enforce Data

Session types specify protocols

Enforce Order

Message sets restrict contents



OPS APP

1: Can Store Blue in (1,1)

2: Affirmative

3: Store Blue in (1,1)

HBW Driver

OPS APP

1: Can Store Blue in (1,1)

2: Affirmative

3: Store Blue in (1,2)

HBW Driver

OPS APP

Store Blue in (1,1)

Store Red in (1,1)

HBW Driver

INL HAIS ARMA™

Assured Reserve Modes in Action

- Urgent need active defenses for active defense to protect CI
- **Brownfields** and **Greenfields**
- INL's ARMA™ + Kry10's KOS™
- Assured Reserve Mode
  - **Assurance** is critical – They must work and work correctly when needed
  - Allows for presence and interaction between different authorities
  - Updating software is a critical function
  - When bad things happen –Time is of the essence

INL

Idaho National Laboratory

KRY10