ADVANCED REACTOR SAFEGUARDS & SECURITY

Secure Elements

May Program Review

PRESENTED BY

Benjamin Karch

May 15, 2024

SAND2024-06154PE

Motivation and Background

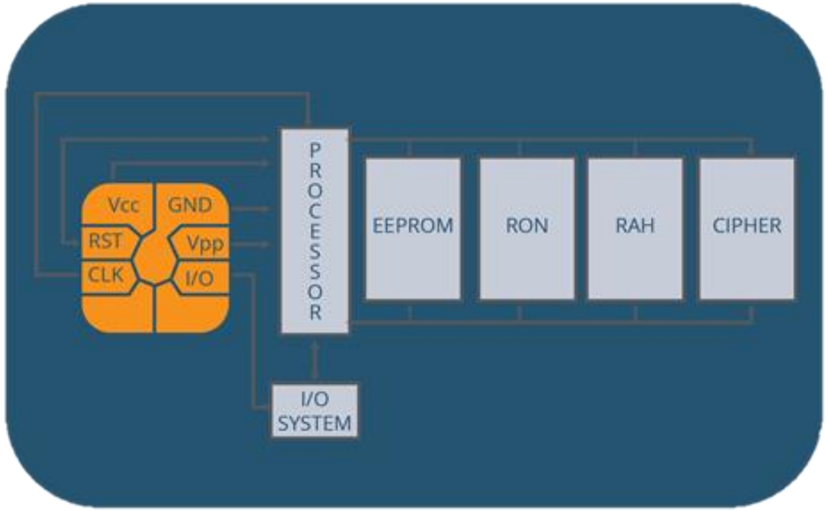
- Existing fleet cybersecurity approach is wrap-around
  - "guns, gates, and guards"
- Current cybersecurity guidelines provide economic burden to operator
  - Large numbers of Critical Digital Assets (CDAs)
  - Site Acceptance Testing
  - Supply Chain management is difficult
- Advanced Reactor industry changing nuclear business case
  - Reduction of on-site security
  - Distributed / remote monitoring and possibly control

Project History and Overview

- Work began in FY22 as a supply chain threat mitigation study
  - Secure Element leveraged as potential for system fingerprinting
  - Provide "digital identity to physical device mapping" via digital signature and 1:1 relationship between public key and device
- FY23
  - Work to extend protection to runtime operations of Programmable Logic Controllers (PLCs)
  - PLC state monitoring tied closely with a Secure Element for trusted operational reporting
- Current FY24 Scope
  - Considering Field Programmable Gate Array (FPGA) based safety systems for architectures including Secure Elements

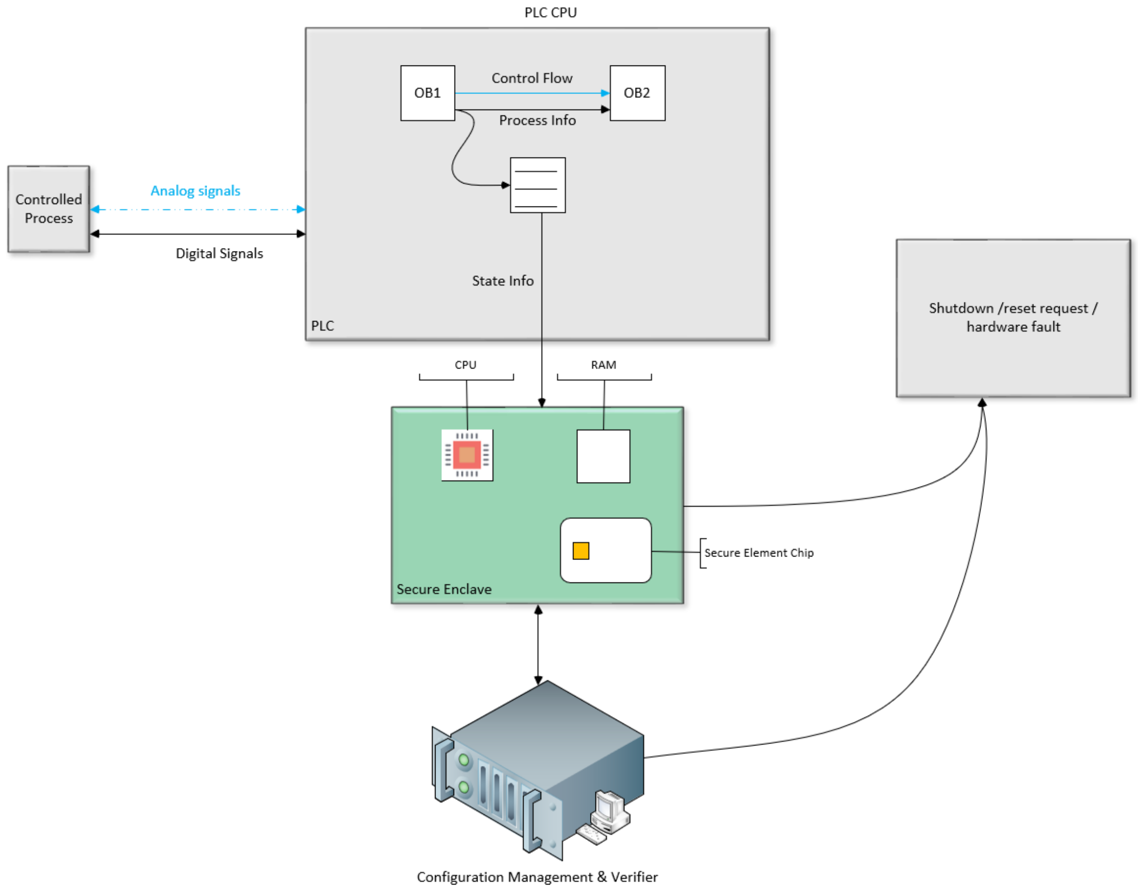
Secure Element – What is it?

- Integrated circuit providing:
  - Tamper resistance
  - Cryptographic security
  - Secure offline storage
  - Assurance through Common Criteria
  - Economy of scale
- Common use cases:
  - Telecommunications
  - Device security (e.g. Trusted Platform Module)
  - Finance (e.g. credit cards)



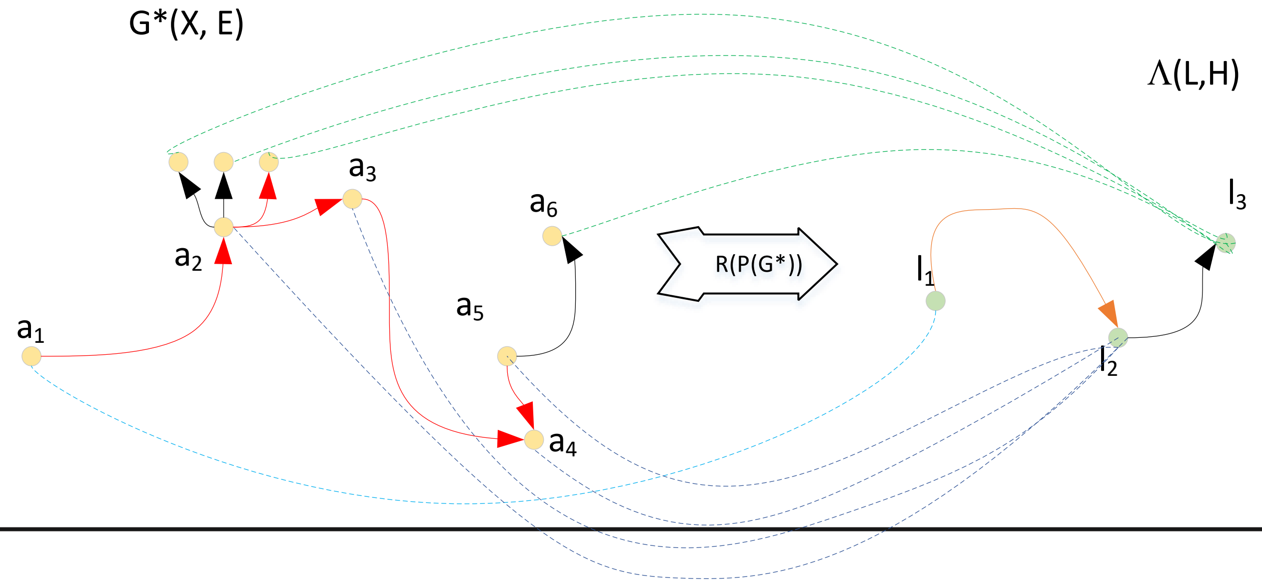
Secure Element - Application

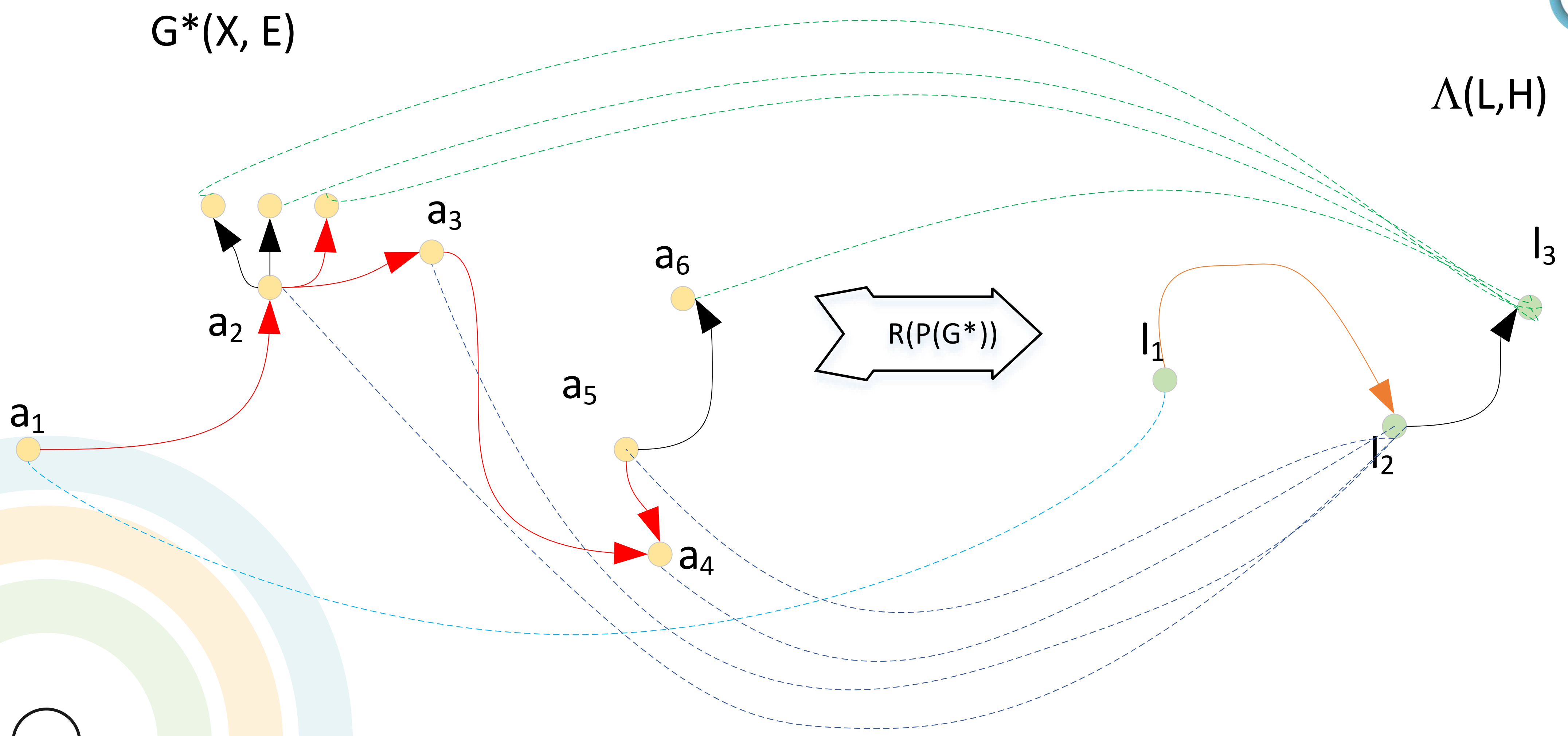
- Leveraged as **Hardware Root of Trust**
- Cryptographic assurance of origins and data confidentiality

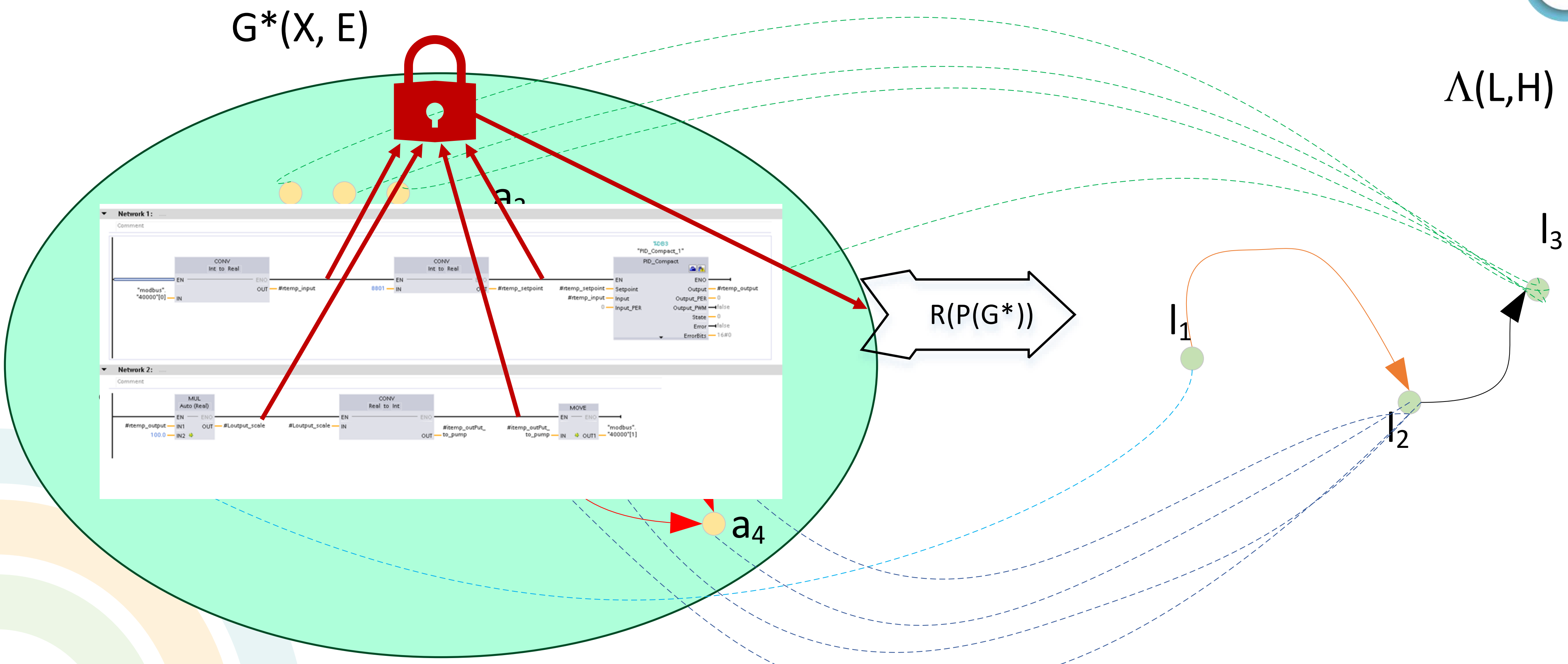


Secure Element – Application

- Integrated SE-rooted cryptography into Commercial Off The Shelf (COTS) PLC
  - Siemens S7 1518
  - AES-GCM 256-bit encryption and MAC
- Trustworthy and secure reporting of asset-centric state information
  - Left side of figure

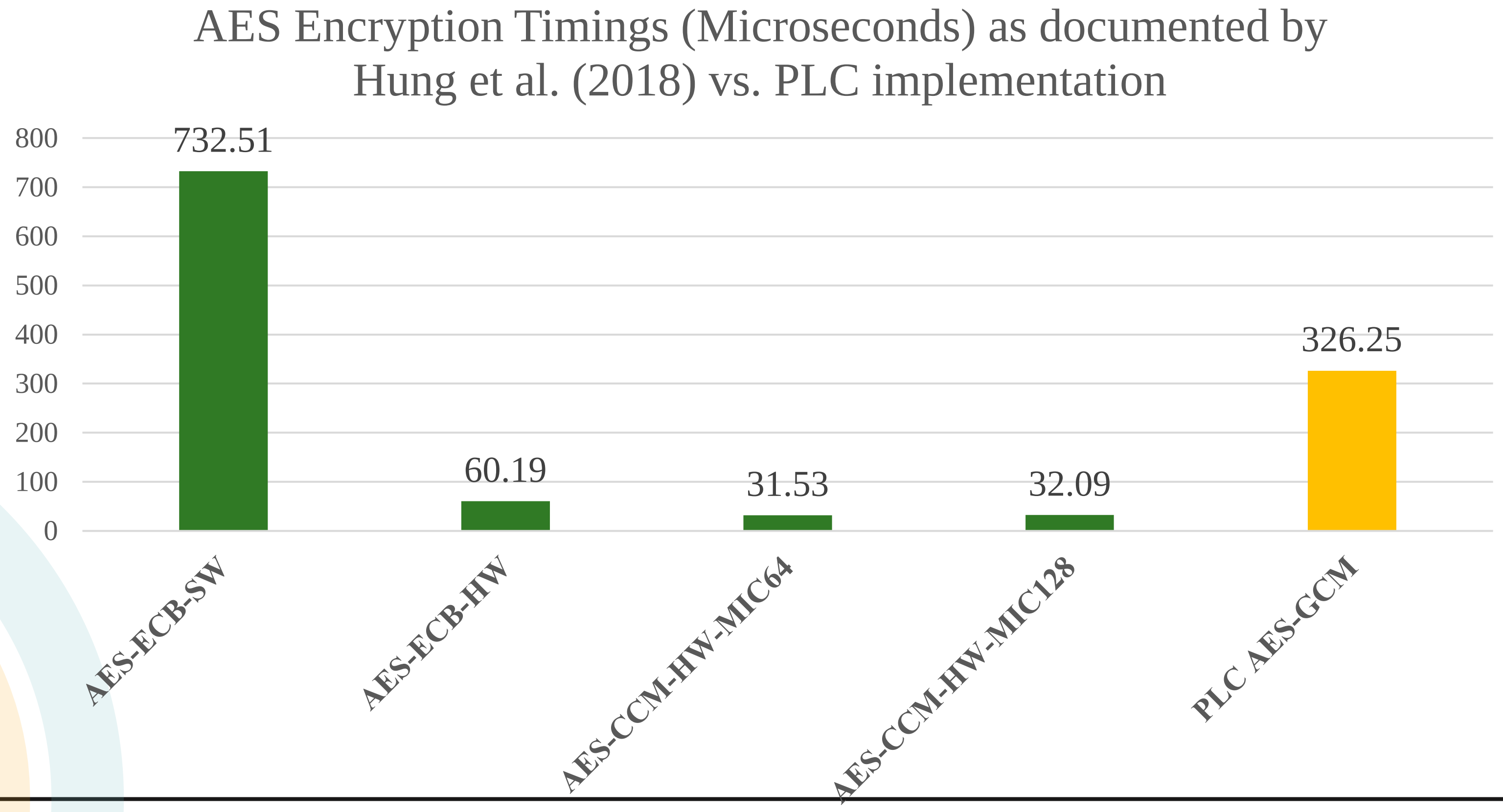



G*(X, E)
a1
a2
a3
a4
a5
a6
R(P(G*))
Λ(L,H)
l1
l2
l3


G*(X, E)
Λ(L,H)
Network 1:
Network 2:
R(P(G*))
l_1
l_2
l_3
a_4

FY23 Results

- Cryptographic performance acceptable for per-cycle state reporting in most demanding (1 ms cycle time) scenarios



FY24

- Focus on Field Programmable Gate Array (FPGA) based security systems
- FPGAs planned for use in safety systems for Advanced Reactors

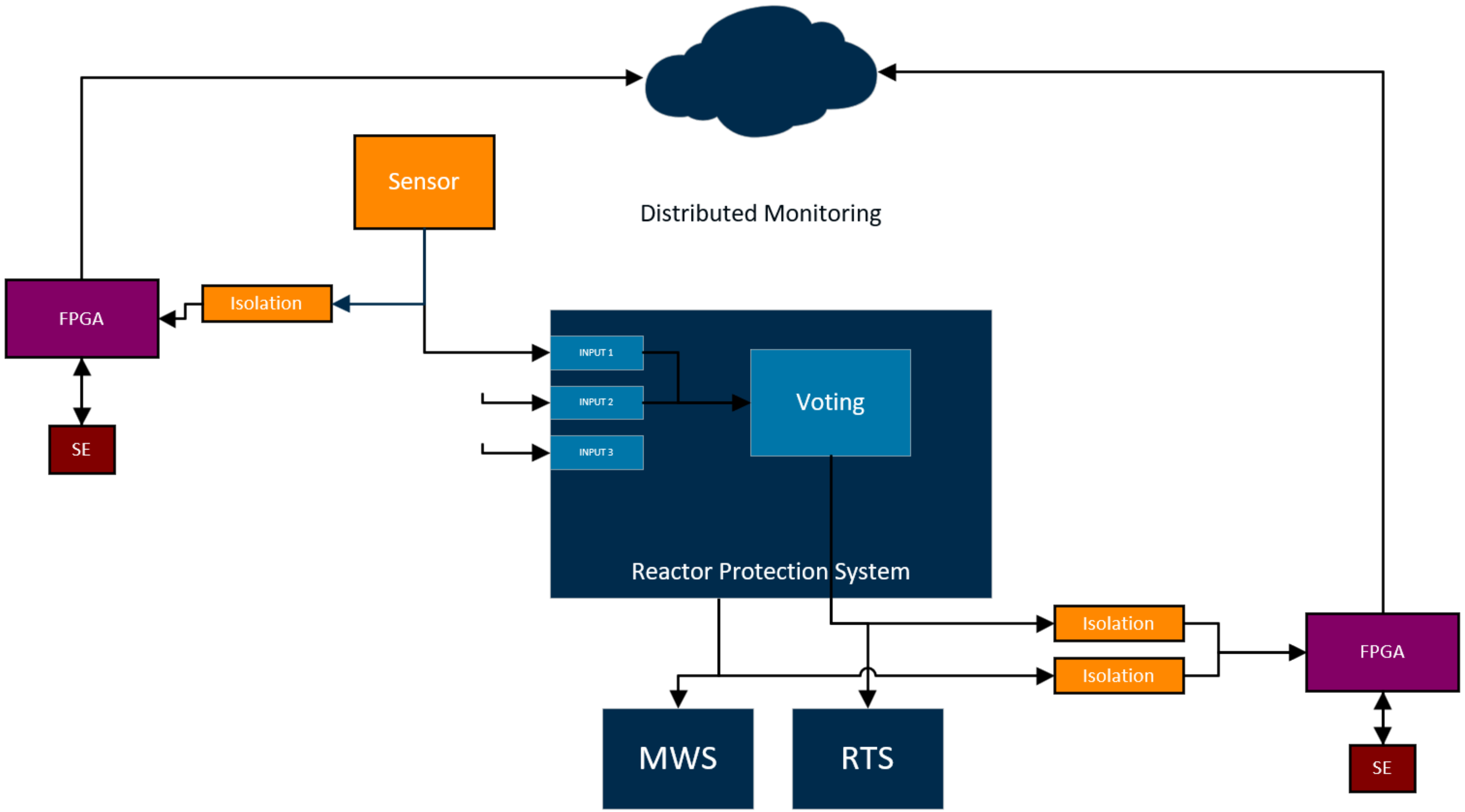
FPGA Platforms

Platform	Safety Evaluation Report Approval	Country of Origin
Westinghouse ALS	2013	USA
Paragon / Rock Creek Innovations HIPS	2017	USA
Radiy RadICS	2019	Ukraine
Doosan HFC FPGA	2021	South Korea

FPGA Implications

- Treated as “Software”
- Lack Operating System, Central Processing Unit, traditional boot operations
    - Secure Element integration becomes trickier due to client/server paradigm
- Relatively large number of distinct FPGAs in safety system design aiding in diversity and redundancy

Licensing Friendly(er)* Design Candidate



*maybe

Project Status and Future

- Development and initial testing underway with FPGA and Secure Element development board communication over inter-integrated circuit (i2c) protocol
- Testing performed on sample FPGA safety system
- ANS Annual Meeting panel session
- On schedule for final report

Thank You!