Secure Element Review

Advanced Reactor Safeguards and Security Program Review Nov. ‘23

Benjamin Karch

November 1, 2023

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525.

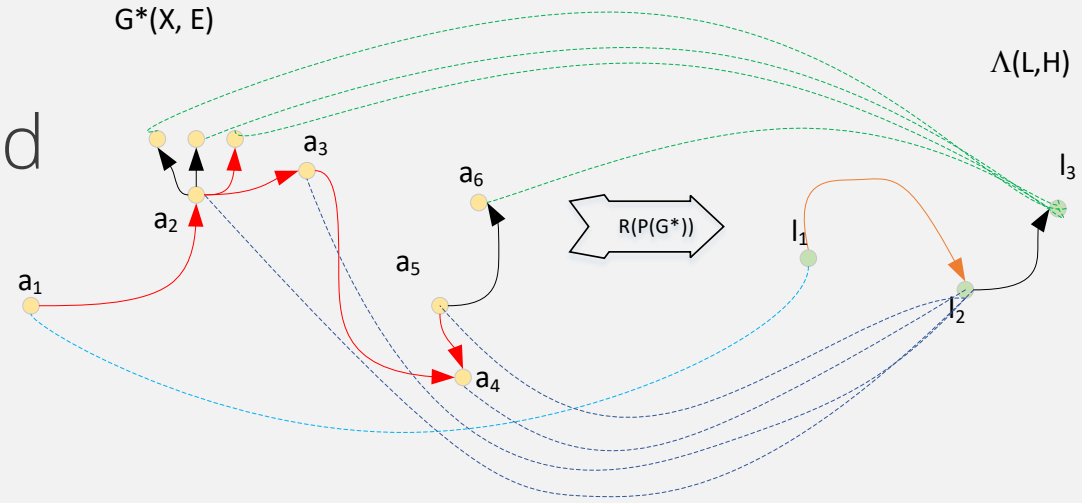
SAND2024-15029PE

Introduction

- Current defensive strategies based on restricting access to attack pathways:
  - Physical Access
  - Wired Network Connectivity
  - Wireless Network Connectivity
  - Portable Media and Mobile Devices (PMMD)
  - Supply Chain
- "Wrap-around" defensive strategy
- Goal: leverage Secure Elements (SEs) to enable "core-to-perimeter" security

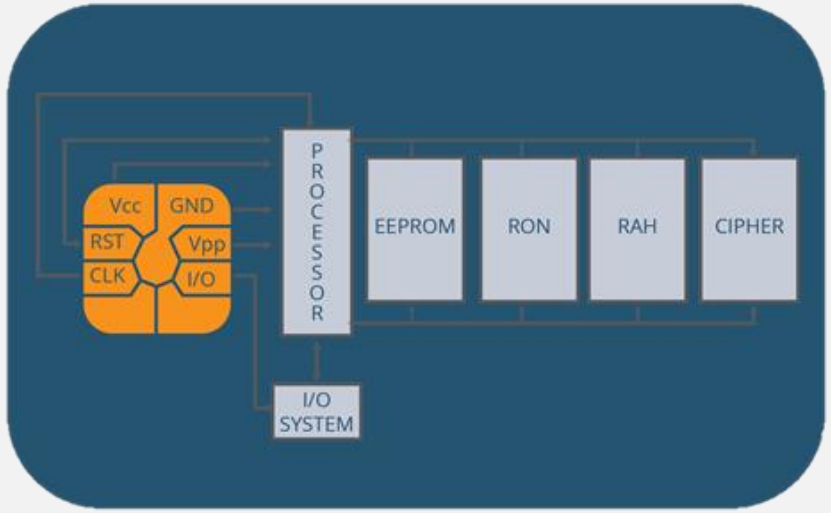
Formal Security Models

- Generally two categories:
  - Integrity
  - Confidentiality
- Terminology differs from popular data-oriented definitions and are system-oriented
- This work focused on Integrity focused security models like Clark-Wilson



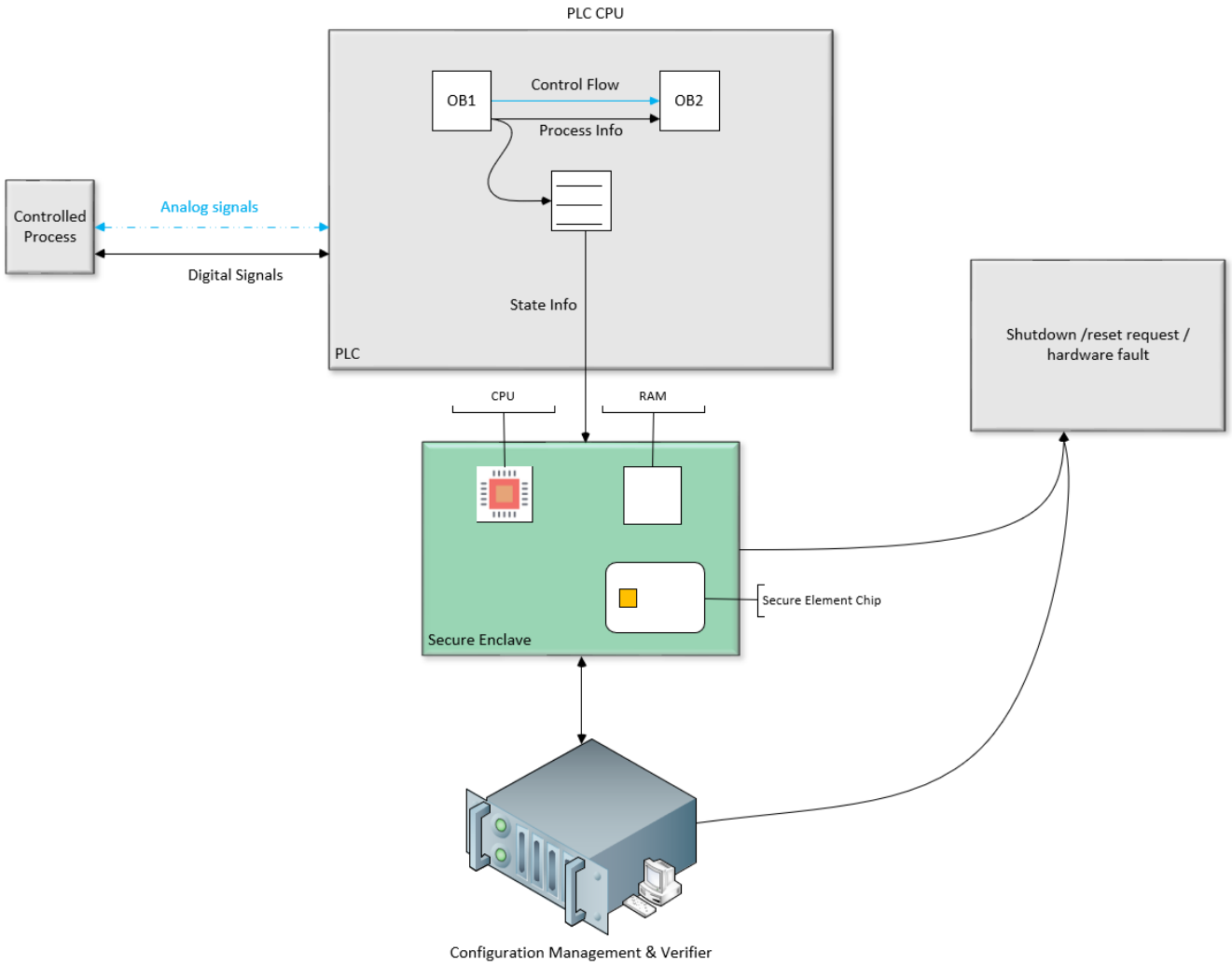
Secure Element – What is it?

- 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)



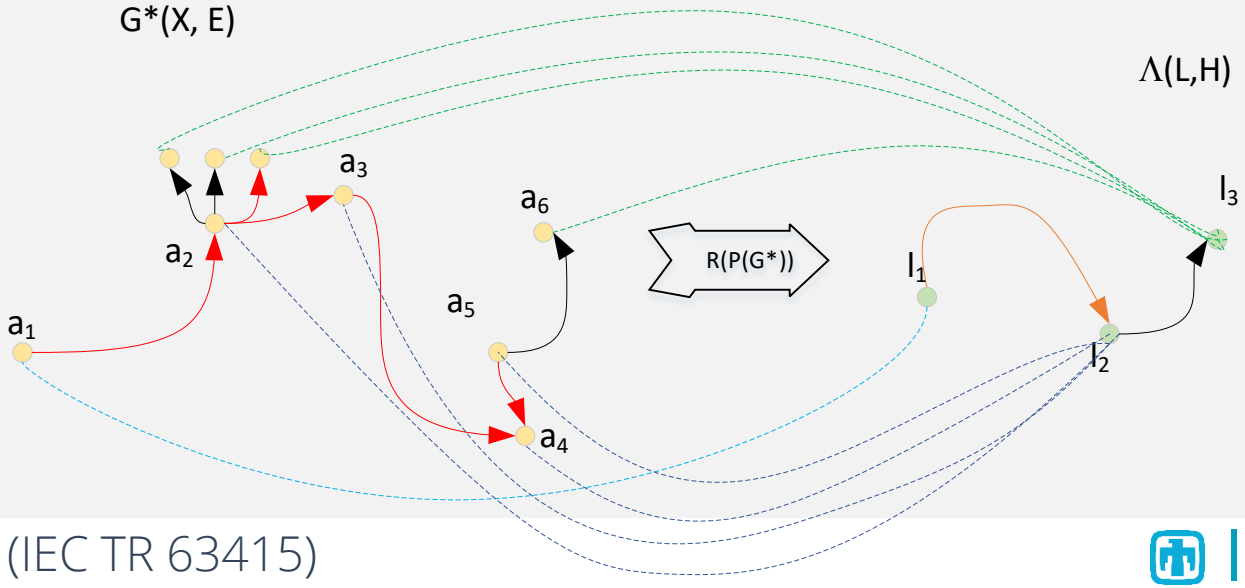
Secure Element - Application

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



FY23 Results

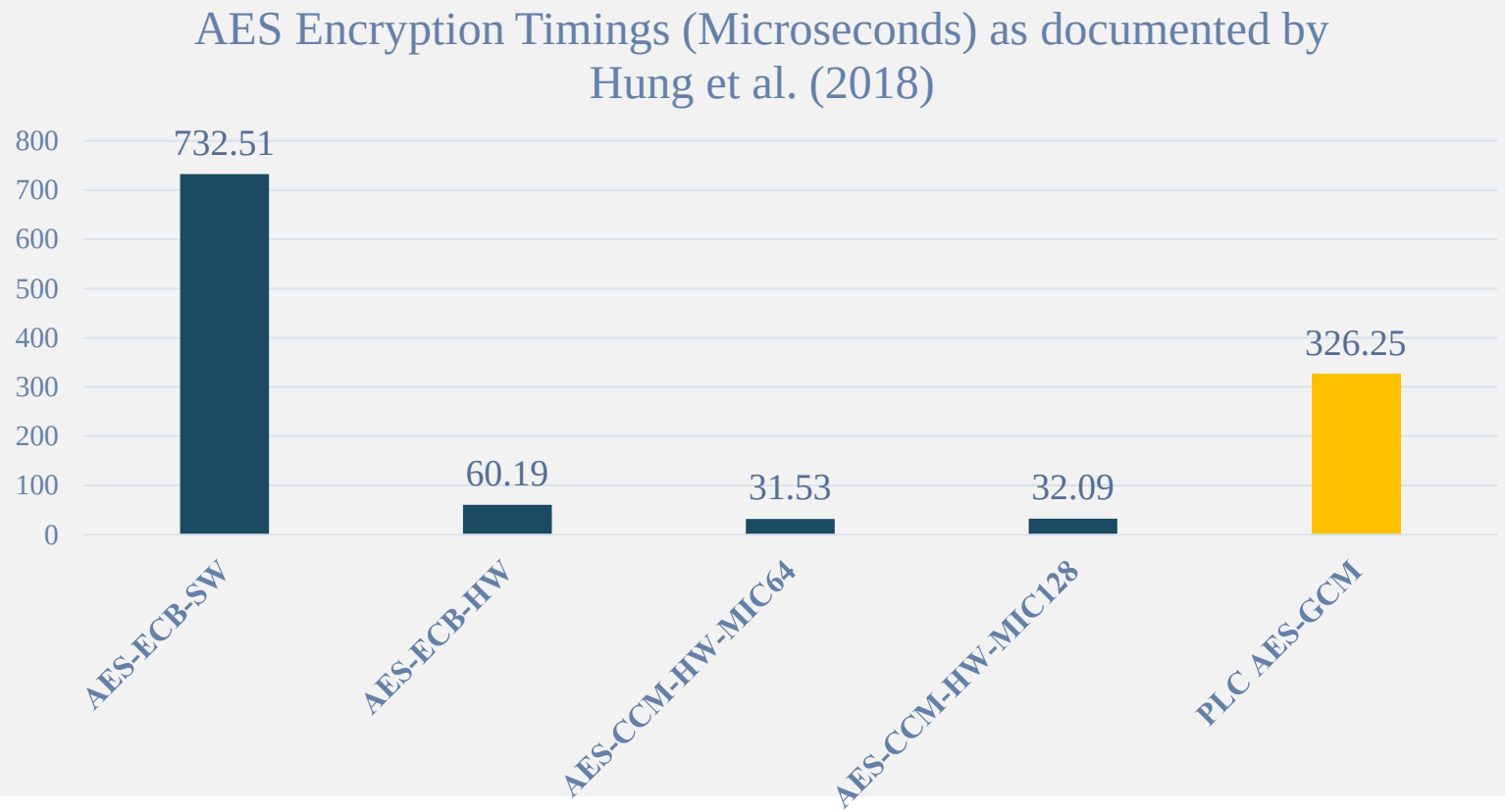
- Integrated SE-rooted cryptography into Commercial Off The Shelf (COTS) PLC
  - Siemens S7 1518
  - AES-GCM 256-bit encryption and MAC
- Trustworthy and secure reporting of asset-centric state information
  - Left side of figure



(IEC TR 63415)

FY23 Results

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



Advanced Reactor Asset Authentication

Advanced Reactor Control Systems Authentication Methods and Recommendations

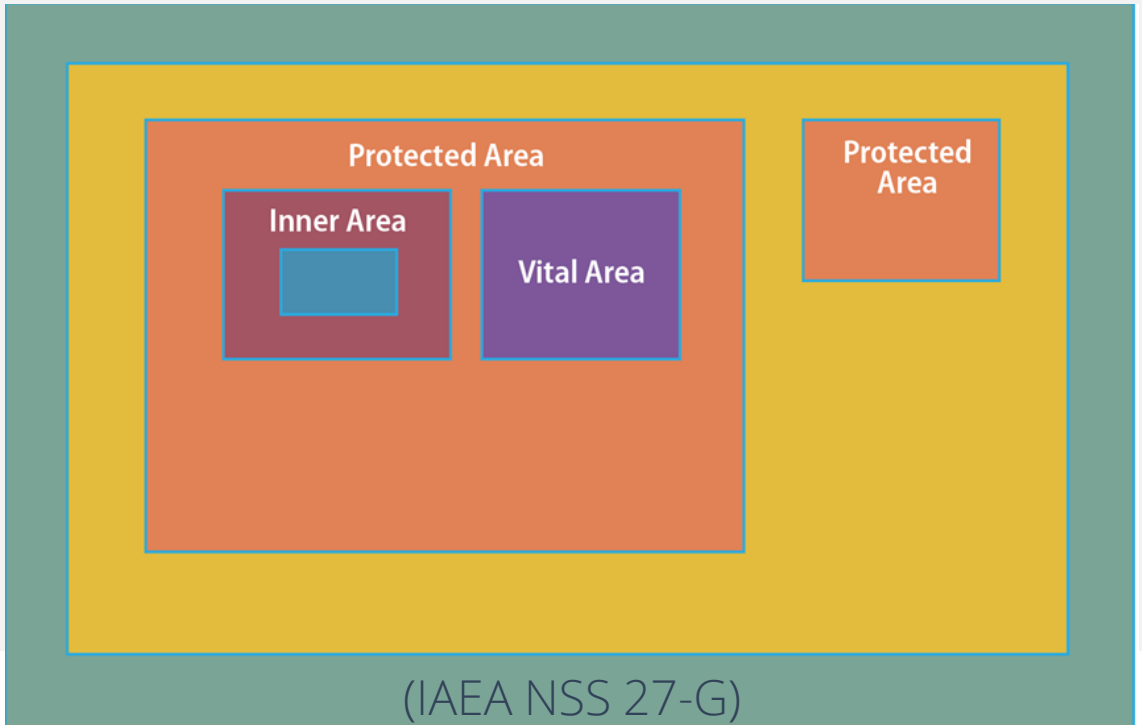
Benjamin Karch

January 2, 2024

November 1, 2023

Introduction

- "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system"
  - NIST 800-39
- Current practice implicitly trusts devices and communications based on strict security boundaries



(IAEA NSS 27-G)

Existing Approaches – Information Technology

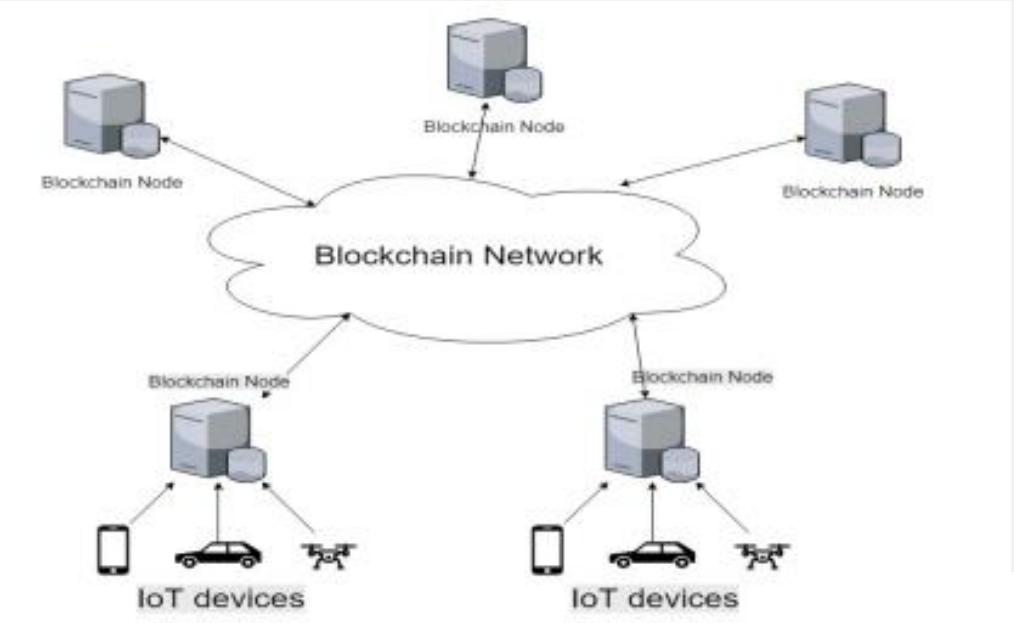
- Enterprise and telecommunication have a long standing need for authentication based on financial and security needs
- Authentication mechanisms in commonplace protocols:
  - Kerberos
  - LTE / 5G
  - Amazon Cognito
- Typically based on central authentication server, pre-shared keys / passwords, user-focused

Existing Approaches – Operational Technology

- Landscape lacking standardization
- Proposed protocols lack full descriptions
  - E.g. assume existing secure communication channel for key agreement
- Scattered use cases
  - Literature specifically for intra-domain machine-to-machine authentication is missing

Blockchain Application

- Distributed ledger solves redundancy problems present in central authentication server approaches
- Blockchain ensures agreement between nodes
- Operators able to utilize both identities leveraging Certificate Authorities or added on-site



(Singla, Bertino 2018)

Discussion