RIC VIRTUAL 2022

U.S. Nuclear Regulatory Commission
34th ANNUAL REGULATORY
INFORMATION CONFERENCE

MARCH 8-10, 2022

PREPARING FOR TOMORROW

WWW.NRC.GOV #NRCRIC2022

A Zero Trust Paradigm for Cyber Security in New Reactors

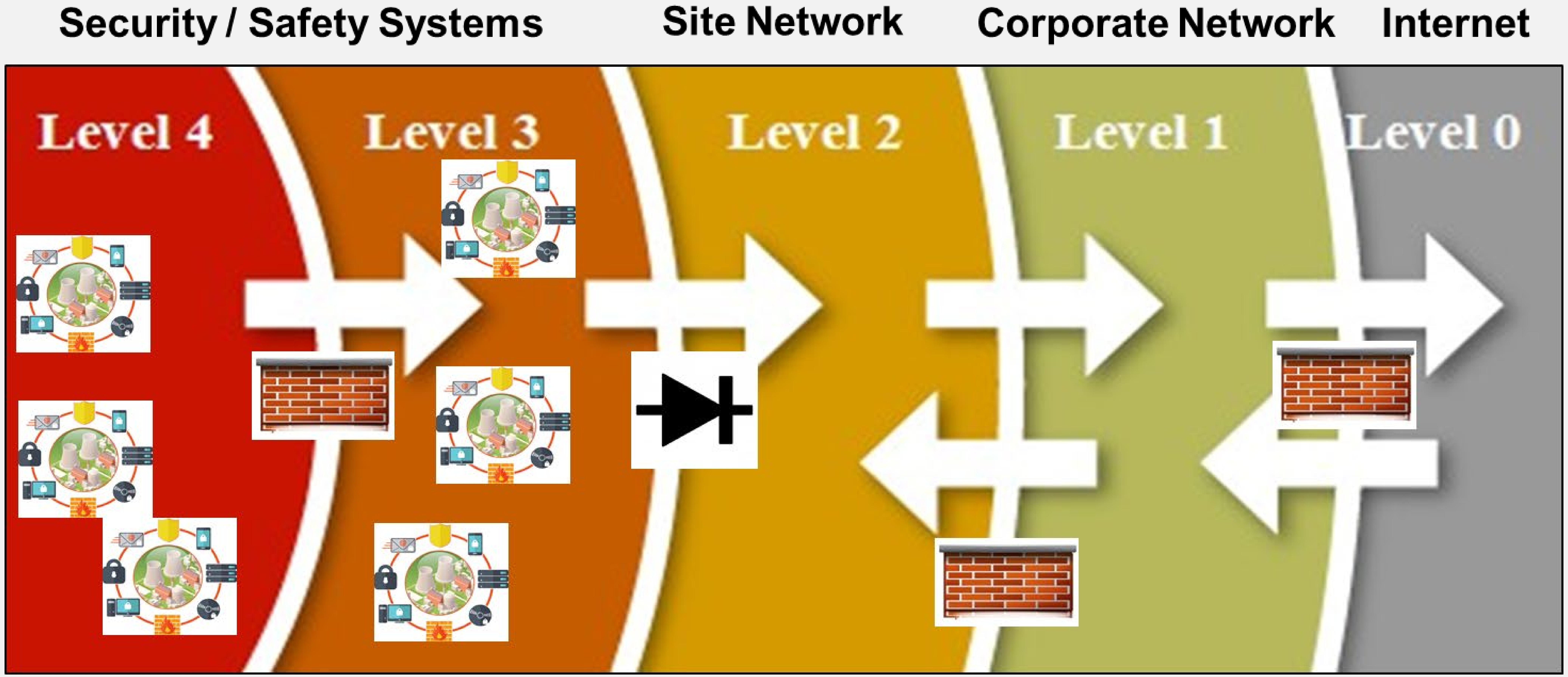
Anya Kim, NRC

Kim Lawson-Jenkins, NRC

Outline

- Why Zero Trust?
- What is Zero Trust, really?
- How do we plan to apply Zero Trust concepts to the nuclear industry?

Cyber security defensive architecture - current



Continuous Threats, New Technologies, Shifting Paradigms

Malware

Artificial intelligence

Drones

IoT Wireless

Remote operations and monitoring

Physical security

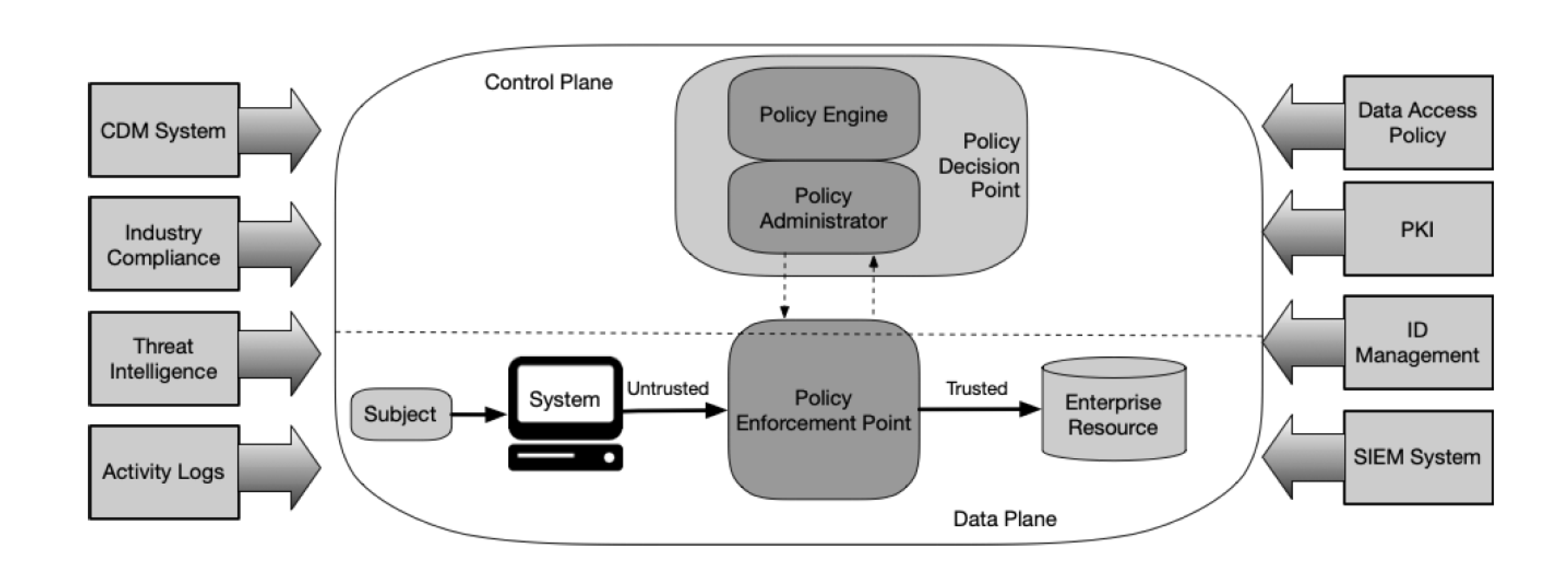
Regulatory compliance

Need a new way of thinking about security

What is Zero Trust?

- Here’s what it is not – not a product or solution, not one-size-fits-all
- It is a strategy – with set of guiding principles/assertions/tenets
    - Assume network is always hostile
    - Trust is explicit
    - Least privilege access (e.g., risk-based adaptive policies)
    - Every device, user, data flow should be authenticated and authorized

Core Components of a Zero Trust Architecture



From NIST SP 800-207 “Zero Trust Architecture”

Zero Trust Applied to the Nuclear Industry

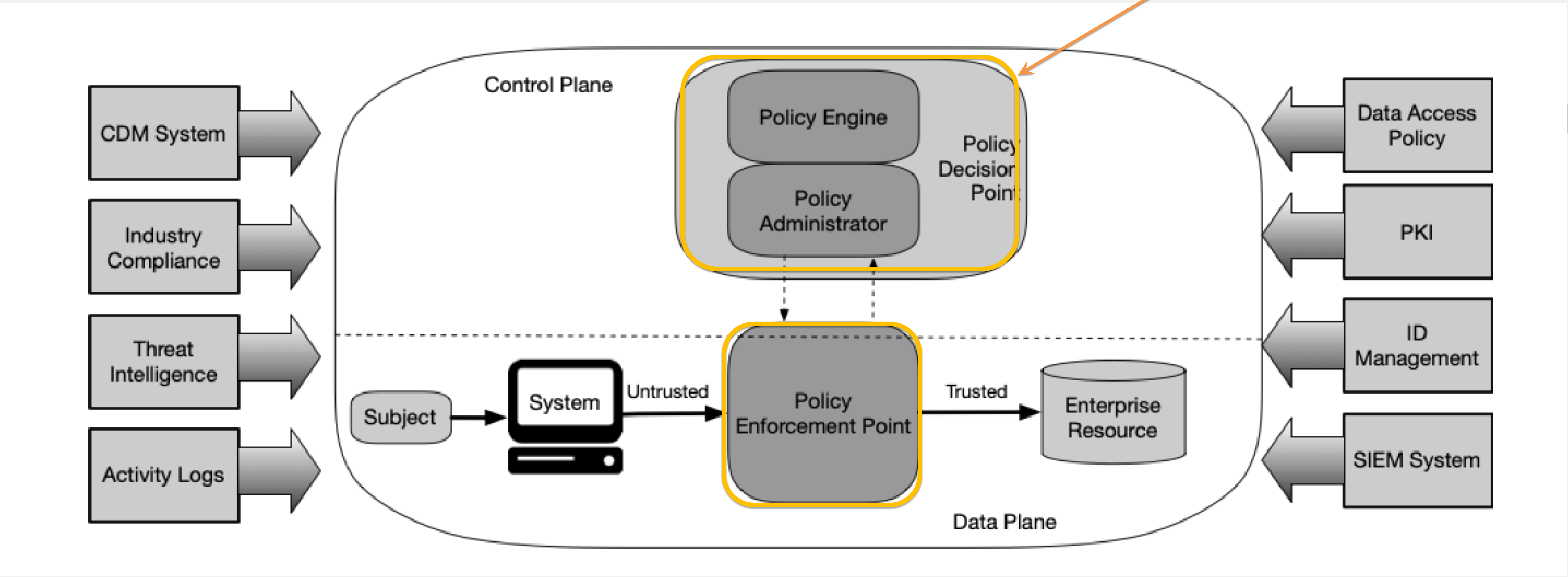
- Can a Zero Trust paradigm be applied as one way to protect new and advanced reactors?
  - Replace current defensive architecture
  - Satisfy safety requirements
  - Applicability of Zero Trust assertions and concepts in Industrial Control Systems
- How to provide guidance for licensees considering applying a Zero Trust architecture?

Our Approach

- Survey the Zero Trust landscape
- Develop Zero Trust Framework suitable for nuclear security
  - Scope and define Zero Trust principle(s) suitable for use in nuclear industry
  - Identify the technical challenges
    - Examine the interface between cyber security and safety for a Zero Trust architecture
  - Develop Implementation strategies
- Develop guidance on adoption of Zero Trust strategies for new and advanced reactors
- Develop performance criteria for the trust algorithm/policy engine

Zero Trust Architecture Revisited

Trust Algorithm



From NIST SP 800-207 “Zero Trust Architecture”

Expected Results and Benefits

- Provide the basis for future regulatory guidance documents
  - Zero Trust architectures may provide alternatives to current defensive architectures when applied to new reactors
- Educate applicants, licensees, vendors, and inspectors regarding not only the Zero Trust paradigm, but the potential usefulness of various (Zero Trust) implementation strategies

Thank you!

Anya Kim
Anya.Kim@nrc.gov
Computer Scientist
Instrumentation, Controls, and Electrical Eng. Branch
Division of Engineering
Office of Research

Kim Lawson-Jenkins
Kim.Lawson-Jenkins@nrc.gov
Cyber Security Specialist
Cyber Security Branch
Division of Physical and Cybersecurity Policy
Office of Nuclear Security and Incident Response