MIRION Connect 25

Annual Users' Conference

INNOVATION AT WORK

Connecting Visionaries in Radiation Safety, Science and Industry

Conrad Orlando Resort, FL –July 28th – August 1st

MIRION TECHNOLOGIES

Nuclear Cyber Security

A brief walk through 10 CFR 73.54 and application to RMS

Ben Ranayhossaini P.E.

Director of Project Engineering – Mirion SIS

Mirion Connect | Annual Users' Conference 2025

Orlando, Florida

MIRION Connect 25
Annual Users' Conference

Innovation at Work

Agenda

Nuclear Cyber Security

- Introduction
- 10 CFR 53 – What does it mean?
- Discuss Mirion approach to Cyber Security
- Cyber Security for RMS
- An intro to Plant Cyber Systems
- How can Mirion SIS help you with your Cyber Security goals

Introduction

About your instructor

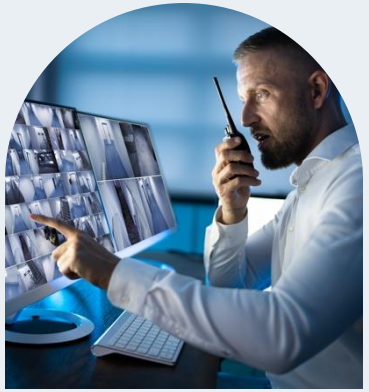
Ben Ranayhossaini P.E.

Director of Project Engineering

Mirion Technologies, Secure Integrated Solutions

- Nuclear power industry +17 years
  - Nuclear Non-Safety I&C Systems
  - Nuclear Security Systems
  - Nuclear Cyber Security
- B.S. & M.S. Electrical Engineering
- P.E. – Electrical Power

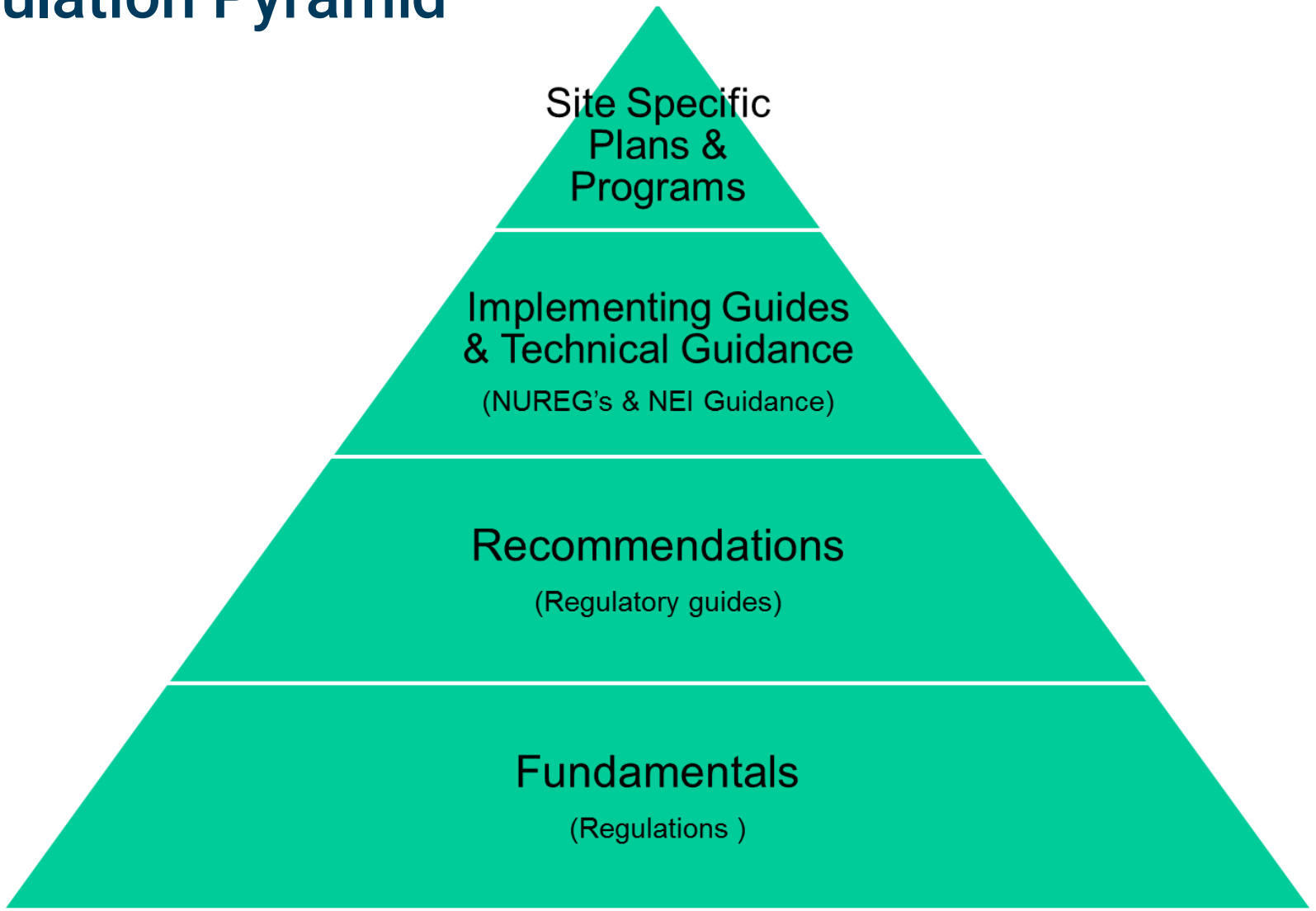
About Mirion Technologies SIS



- **Secure** – Valued and trusted by our customers for the protection of critical assets and personnel safety
- **Integrated** – For real-time performance meeting mission requirements
- **Solutions** – That meet our customer's expectations for operational capability and sustained performance

10 CFR 73 – What does it mean?

NRC Regulation Pyramid



➢ **Fundamentals: U.S. NRC Regulations –** *Law; Requirements binding on all persons and organizations who receive a license from NRC to use nuclear materials or operate nuclear facilities*

- **10CFR Part 73 - PHYSICAL PROTECTION OF PLANTS AND MATERIALS**
  - Subpart F
    - 10CFR 73.55 - Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage.
    - 10CFR 73.54 - Protection of digital computer and communication systems and networks

➢ **Recommendations: U.S. NRC Regulatory Guide -** *Regulatory guides' (R.G.s) present methods acceptable to NRC for implementing specific parts of NRC regulations, delineate techniques used by the staff in evaluating specific problems, and provide guidance to applicants, licensees, or certificate holders.*

- Reg Guide 5.71 - Cyber Security Programs for Nuclear Facilities

➢ **Implementing Guides: U.S. NRC NUREG's & NEI Guidance -** *Technical Information for Licensees; NRC or NEI may suggest a course of action, these suggestions are not legally binding and the regulated community may use other approaches to satisfy regulatory requirements.*

- NEI 13-10 - Cyber Security Control Assessments
- NEI 08-09 - Cyber Security Plan for Nuclear Power Reactors

➢ **Licensee Plans & Programs: Site Specific Plans are submitted for review and acceptance**

- Cyber Security Plan

Overview / Disclaimer

- NRC regulations provide high-level requirements for security (10 CFR Part 73 – Protection of digital computer and communication systems and networks)
- NRC does not “certify” or “approve” security designs or implementations – they only audit and provide findings.
- Each site is responsible for developing their own security plans (physical security, cyber security, etc.)

- The end results is…EVERY SITE DOES CYBER SECURITY DIFFERENTLY

What's the worst that could happen?

- Release of radioactivity through sabotage on nuclear reactors or specifically containment buildings.
  - The impact of such an attack could involve hundreds or even thousands of **immediate fatalities**, tens of thousands of **delayed deaths from radiation**-induced cancers, and **immense economic damage** from the contamination of territory.

- Fissile material may be stolen from nuclear plants

- Destruction of an important piece of energy-supply infrastructure
  - 1 MW/day = 34 homes
  - Smallest plant – OPPD – 479 MW/day
  - Largest plant – APS – 3,937 MW/day

Mirion Approach to 10 CFR 73.54 Cyber

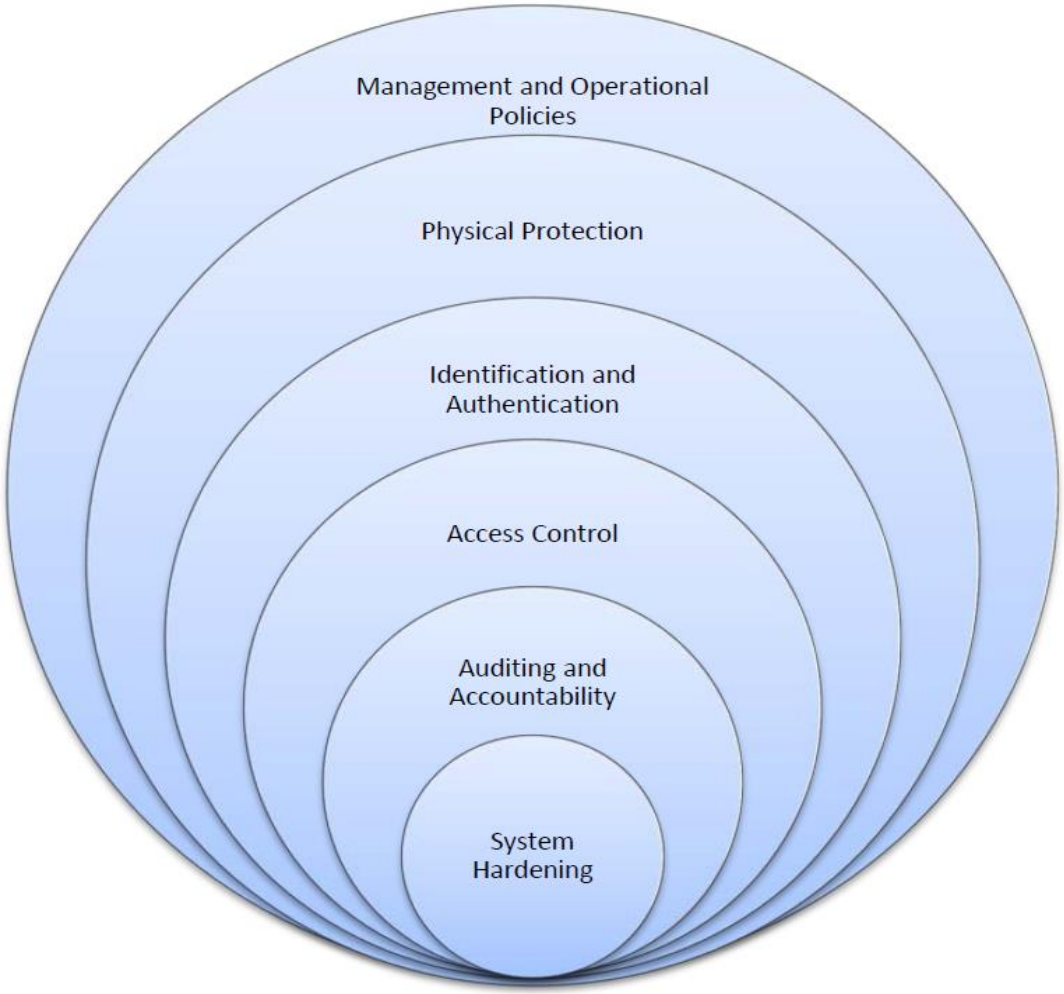
NEI 08-09, NEI 13-10, and CDAs

- NEI 08-09 - Cyber Security Plan for Nuclear Power Reactors
  - This document provides guidance for licensees to develop their Cyber Security Plans, and to also apply cyber security controls to the CDAs throughout the plant.
  - Apply controls to protect CDAs up to the Design Basis Threat (DBT).
- CDA – What is a CDA?
  - Critical Digital Asset
    - Key here is ‘Digital’
    - Analog devices are typically not considered CDAs (Although some site still treat them as CDAs as defined by their CSP).
- NEI 13-10 - Cyber Security Control Assessments
  - Guideline to help licensees perform assessments on their CDAs to determine how to apply controls defined in NEI 08-09

Mirion Cyber Security Approach

Defense-in-depth

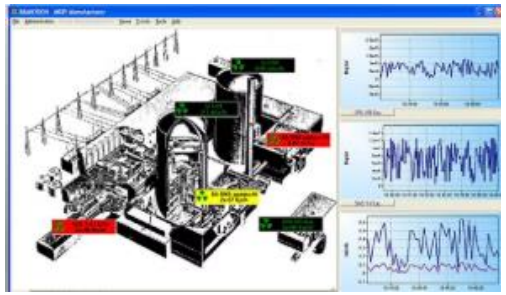
- Strategy based on risk and impact to create multiple barriers for threat agents:
  - Prohibitively costly
  - Time consuming
- Establishes multiple barriers to achieve a robust cyber security poster
  - Physical
  - Administrative
  - Technical
- Based on:
  - NEI 08-09, Rev. 6



Cyber Security for RMS Systems

Cyber Security for RMS Systems - Where do we start?

- Assessing the system and CDAs
  - Mirion RMS Systems/Sub-Systems
    - DRMS, ERMS, PRMS, ARMS
      - CDAs = RMS Application (Vital Supervision / Ramvision), DRMS Server, DRMS Network Switch, Ramsys Monitors, LDU, LPU, etc.



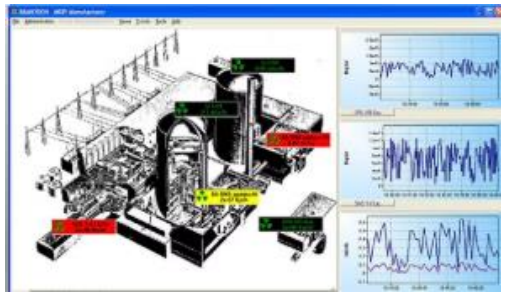
MIRION Connect 25
Annual Users' Conference

Innovation at Work

Cyber Security for RMS Systems

Assessment Walk through

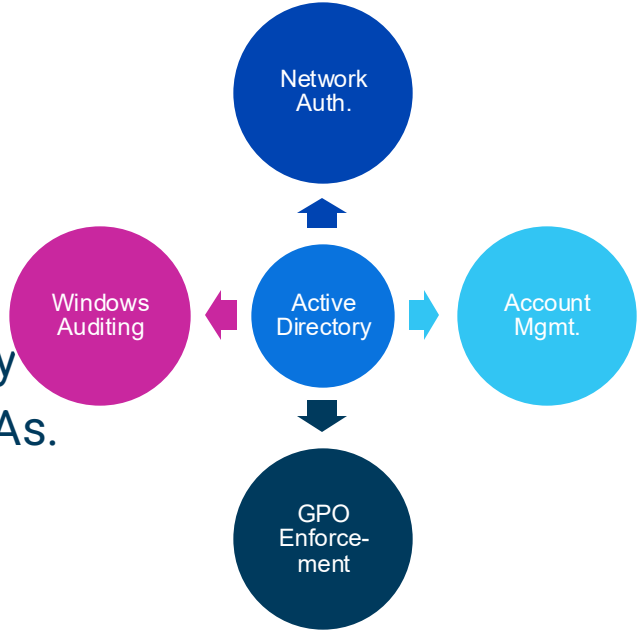
Scope – Vital Supervision, DRMS Server / Rack, LDU/LPU



MIRION Connect 25
Annual Users' Conference

Innovation at Work

IDENTIFICATION and AUTHENTICATION



Control to implement identification and authentication technology to uniquely identify authenticate individuals and processes acting on behalf of users interacting with CDAs.

- DRMS Applications (Vital Supervision)
  - Assessment - Application supports role-based authentication.
- DRMS Chassis
  - Assessment - The DRMS Chassis is a Windows based machine and can support role-based authentication.
- Local Processing & Display Unit (LPDU), Local Display Unit (LDU), Local Processing Unit (LPU)
  - Assessment – Have simple HMI with user input limited to a predefined list of commands entered by a keypad.

Access Control

Control to ensure that only authorized individuals can access CDAs, thereby protecting their confidentiality, integrity, and availability while maintaining accountability and compliance.

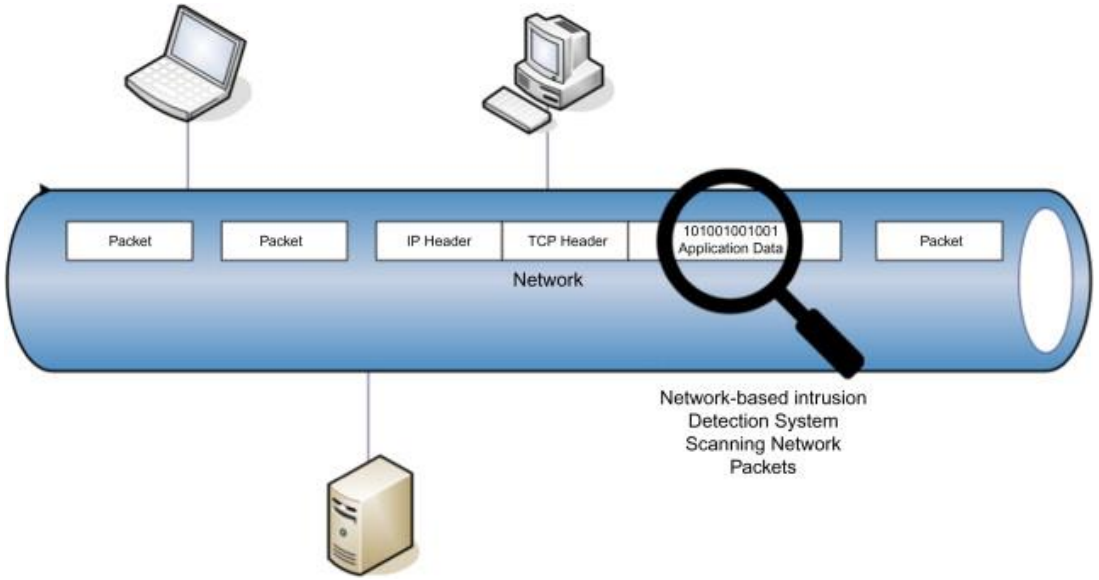
Categories under this control are Account Management, Access Enforcement, Information Flow Enforcement, Separation of Functions, Least Privilege, etc.

Access Control

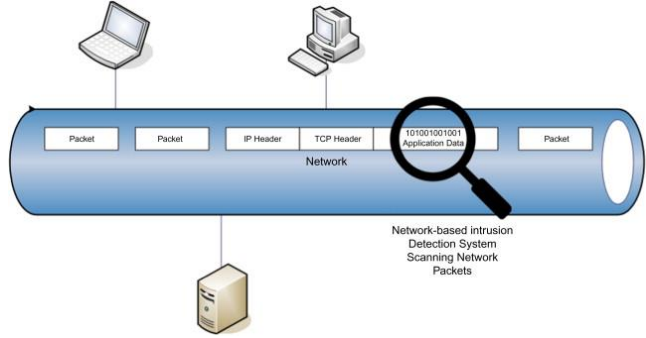
- DRMS Applications (Vital Supervision)
  - Assessment - Application supports role-based authentication, Application does not require any communication to lower security levels, service accounts are only assigned the permissions required to carry out the service's function, etc.
- DRMS Chassis
  - Assessment - Can support role-based authentication, Does not require communication to lower security levels, can integrate with existing Active Directory policies to apply user based privilege.
- Local Processing & Display Unit (LPDU), Local Display Unit (LDU), Local Processing Unit (LPU)
  - Assessment – Have simple HMI with user input limited to a predefined list of commands entered by a keypad, not able to communicate between boundaries.

Auditing and Accountability

The intent of the Auditing and Accountability control is to ensure that actions affecting critical digital assets are recorded, monitored, and traceable to individuals, enabling the detection of unauthorized activity, supporting incident response, and maintaining regulatory compliance.



Auditing and Accountability



- DRMS Applications (Vital Supervision)
  - Assessment - Application will provide means to send event logs to a centrally managed SIEM.
- DRMS Chassis
  - Assessment - In addition to the SIEM forwarding, audit events are stored locally on the DRMS Chassis in a password protected databases.
- Local Processing & Display Unit (LPDU), Local Display Unit (LDU), Local Processing Unit (LPU)
  - Assessment –Devices maintain local logs; however, these logs are primarily used for functional events rather than audit events. Device does not communicate using TCP/IP, so the logs cannot be forwarded to a SIEM.

System hardening

The intent of the System Hardening control is to reduce the attack surface of critical digital assets by disabling unnecessary functions, services, and ports, thereby minimizing vulnerabilities.

System hardening

- DRMS Applications (Vital Supervision)
  - Assessment - Application allows for services/features to be turned on/off.
- DRMS Chassis
  - Assessment - Hardening of DRMS server would consist of including the required services/features to run Vital Supervision application and any other required 3rd party applications. Further hardening can occur through the DRMS Server BIOS.
- Local Processing & Display Unit (LPDU), Local Display Unit (LDU), Local Processing Unit (LPU)
  - Assessment – These devices only communicate using serial links and thus do not allow for the disablement of services/features.

An Intro into Nuclear OT Cyber Systems

An Intro into Nuclear OT Cyber Systems

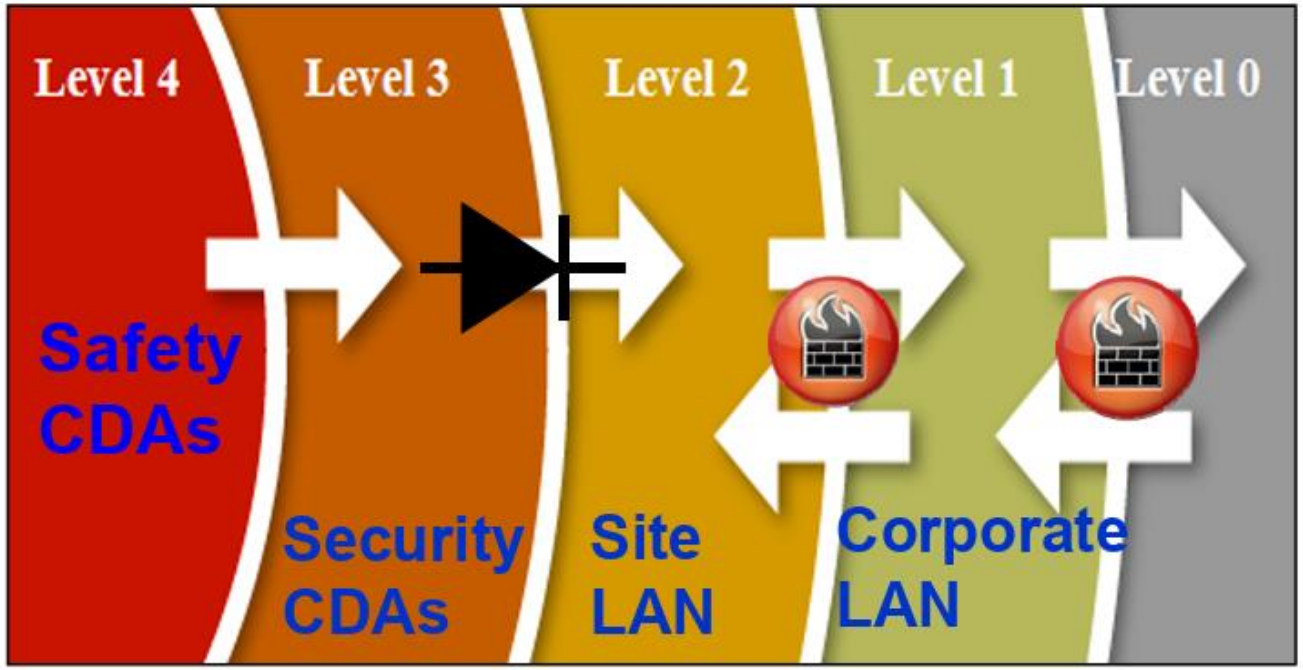
As nuclear plant systems advance and the integration increases, the need for an integrated cyber security solution that can be utilized across a plant has.

Modern plants are moving to a centralized cyber security solution to apply cyber to all plant (Operational Technology) systems.

Reverse Purdue Model of Cyber Security Layers

Defense Model Architecture

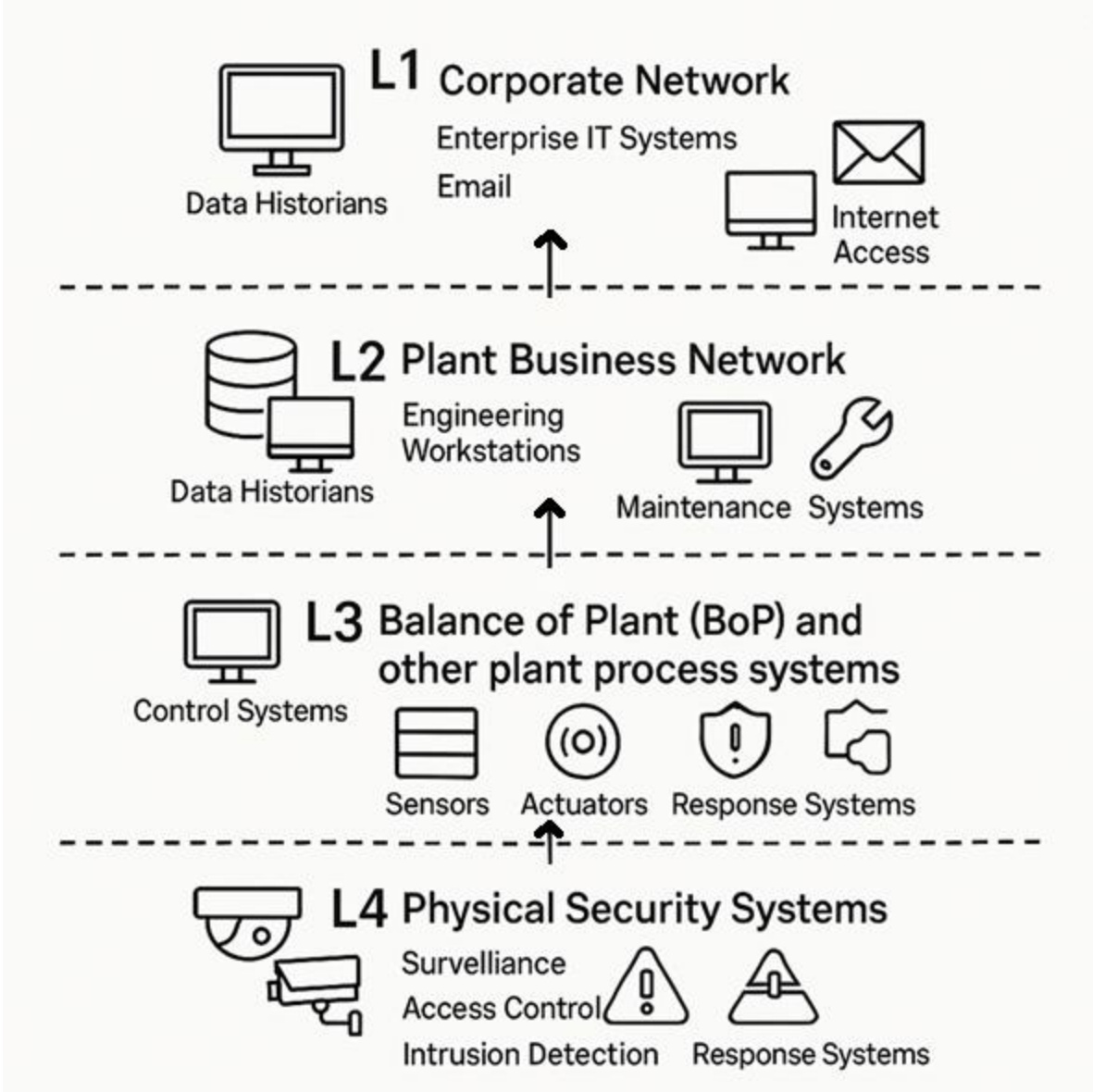
- Digital assets associated with safety, important to safety, and security functions should be located at the highest security level and protected from all lower levels.



Innovation at Work

Reverse Purdue Model of Cyber Security Layers

Defense Model Architecture



How Mirion SIS can help you…

How can Mirion SIS help you…

Please Contact Me:

Ben Ranayhossaini

branayhossaini@mirion.com

Questions?

Questions?

Thank you

Technology Stack

Runs on commercial off-the-shelf (COTS) hardware and software

Utilizes VMware Virtual Infrastructure, Microsoft OS, and Intel processors

Incorporates multiple cyber vendors to avoid single vendor blind spots

System Resilience

- Clustered virtual infrastructure

- Hardware redundancy

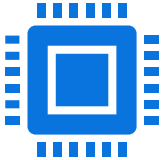
- Fault-tolerant software for mission-critical functions

Logical Access Control

• Identity Management System for user identification and access control

• Centrally managed role-based access control (RBAC)

• Supports least privilege access and separation of duties



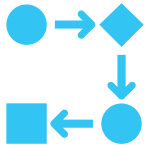
• Applies to servers, workstations, switches, and other systems

Telemetry, Data Logging, and Analysis

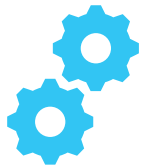
- Protects system availability and integrity
- Detects hardware faults and malicious events
- Alerts on threats to system integrity or availability
- Tools: SIEM, NIDS, NMS

System Maintainability

• Onboard maintenance and troubleshooting



• Enables preventative and corrective actions

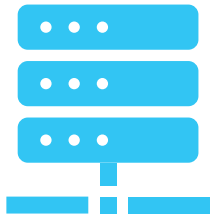


• Ensures continuous optimal system performance

• Tools: WSUS, VAS, COTS

Transmission Integrity / Cryptographic Mechanism

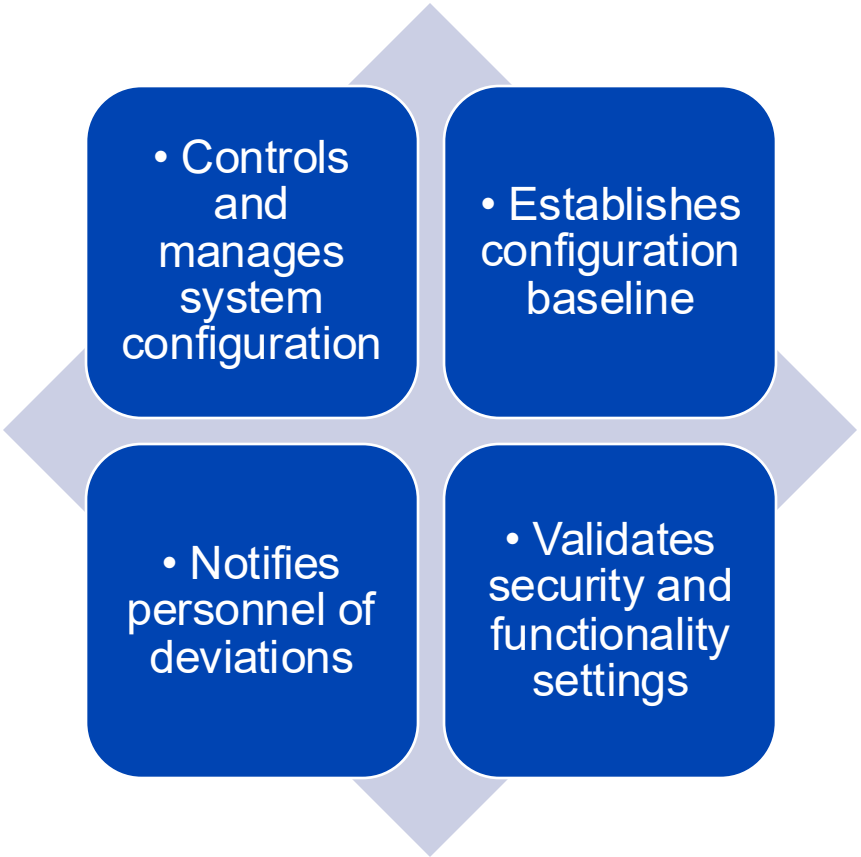
• Protects data in transit from unauthorized changes



• Prevents man-in-the-middle (MITM) attacks

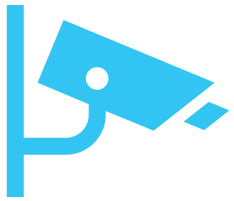
• Encrypts data for CDAs to ensure secure transmission

Configuration Management and Baseline



Endpoint Protection

• Protects against malicious applications and unauthorized media



• Host-based intrusion detection

• Auditable abnormal activity