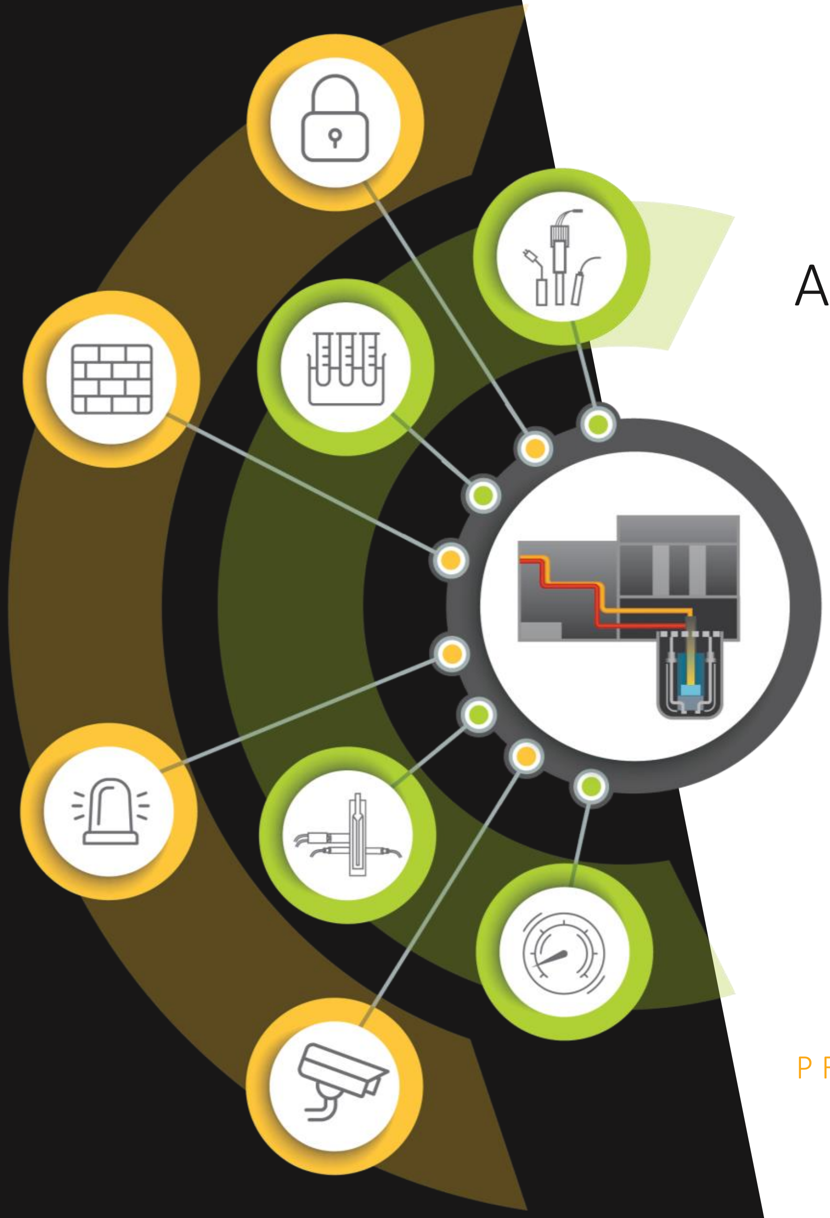
SAND-02224PE



ADVANCED REACTOR SAFEGUARDS

PPS-Cyber Security Modeling

PRESENTED BY

Michael Higgins

4/18/23

Controlled by: Sandia National Laboratories, Michael Higgins

Outline

- Introduction
- Physical Protection System (PPS) Cyber Defensive Architecture
- Work for Remaining FY
- Conclusions

The goal of this work is to incorporate the physical security work of previous years for microreactors and quantify the impact a blended cyber-physical attack would have on the success of the attack

NRC requirements for reactor physical protection systems

10CFR73 describes the requirements for **physical protection systems (PPSs) of plants**, special nuclear material (SNM) in transit, and SNM at fixed sites.

The NRC is currently discussing an addition to 10CFR73 to include cyber security requirements within 10CFR73.110

- 73.110 – Technology neutral requirements for protection of digital computer and communication systems and networks
- Similar to the new rulemakings, 73.110 calls for a graded approach to cyber security for advanced reactors.

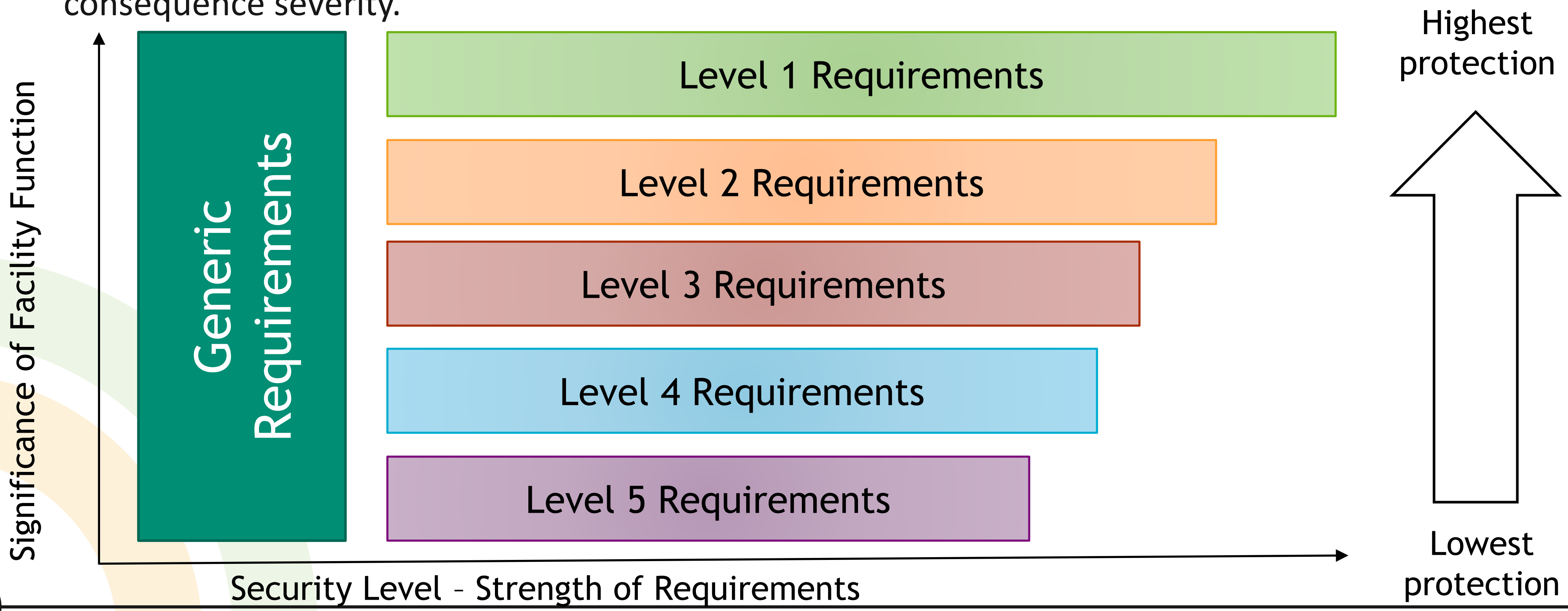
A Cyber Enabled Physical Intrusion Scenario (CEIS) (blended attack) has specific requirements under 10CFR73.110

- 73.110(2)(a) covers the consequences where a cyber attack adversely impacts the digital assets used by the licensee to prevent unauthorized removal of SNM, source material, and byproducts materials.

Graded Approach

NRC implements a graded approach:

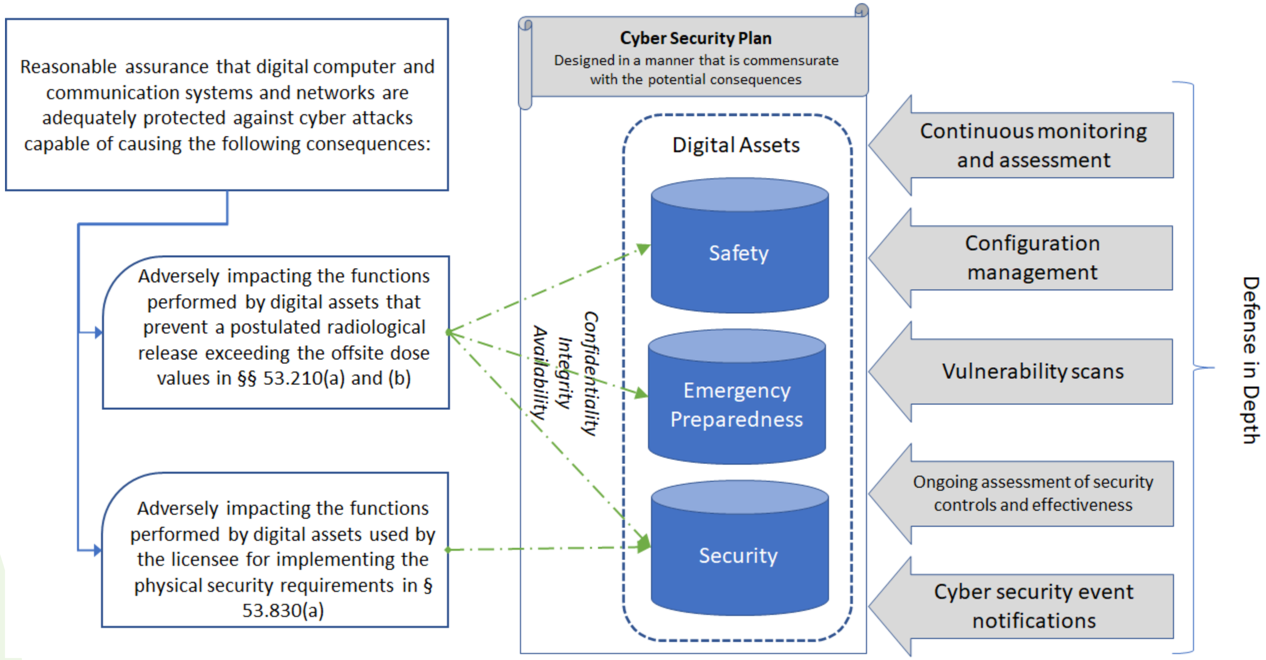
- Security requirements increase with the relative significance and value of the facility function
- Demands increasingly stringent requirements that increase effort on security commensurate with consequence severity.



Cyber Requirements for Vendors

CEIS may be used to validate assumptions made during PPS design and implementation. The assumptions include:

- No detection identified via Digital Technology with no indication of failure
- Failure of one or more of the detect, delay, respond to, or recover capabilities
- Unexpected behaviors or actions of digital equipment concurrent with the commencement of a physical intrusion.



Reasonable assurance that digital computer and communication systems and networks are adequately protected against cyber attacks capable of causing the following consequences:

Adversely impacting the functions performed by digital assets that prevent a postulated radiological release exceeding the offsite dose values in §§ 53.210(a) and (b)

Adversely impacting the functions performed by digital assets used by the licensee for implementing the physical security requirements in § 53.830(a)

Cyber Security Plan

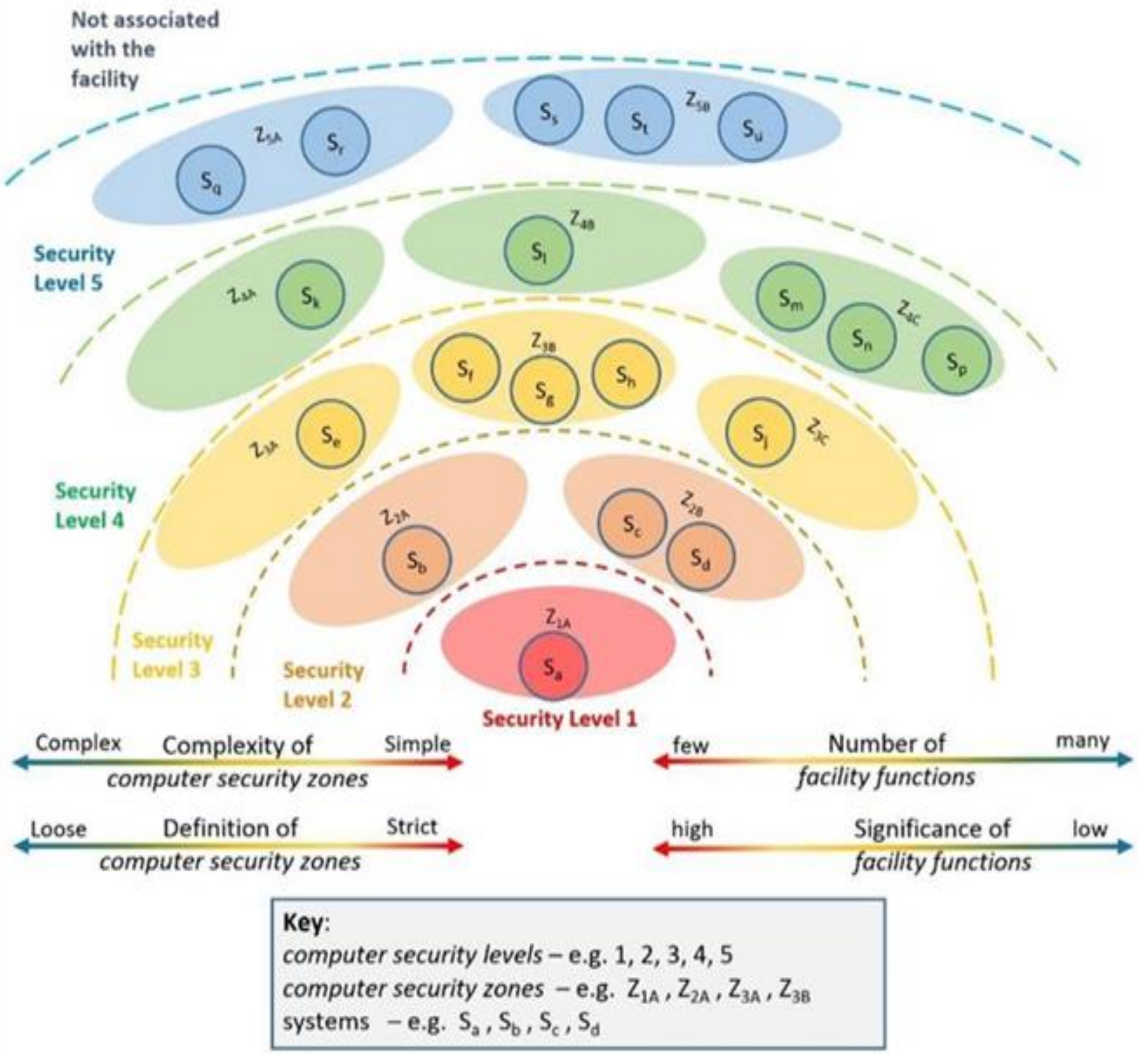
Designed in a manner that is commensurate with the potential consequences

Defense in Depth

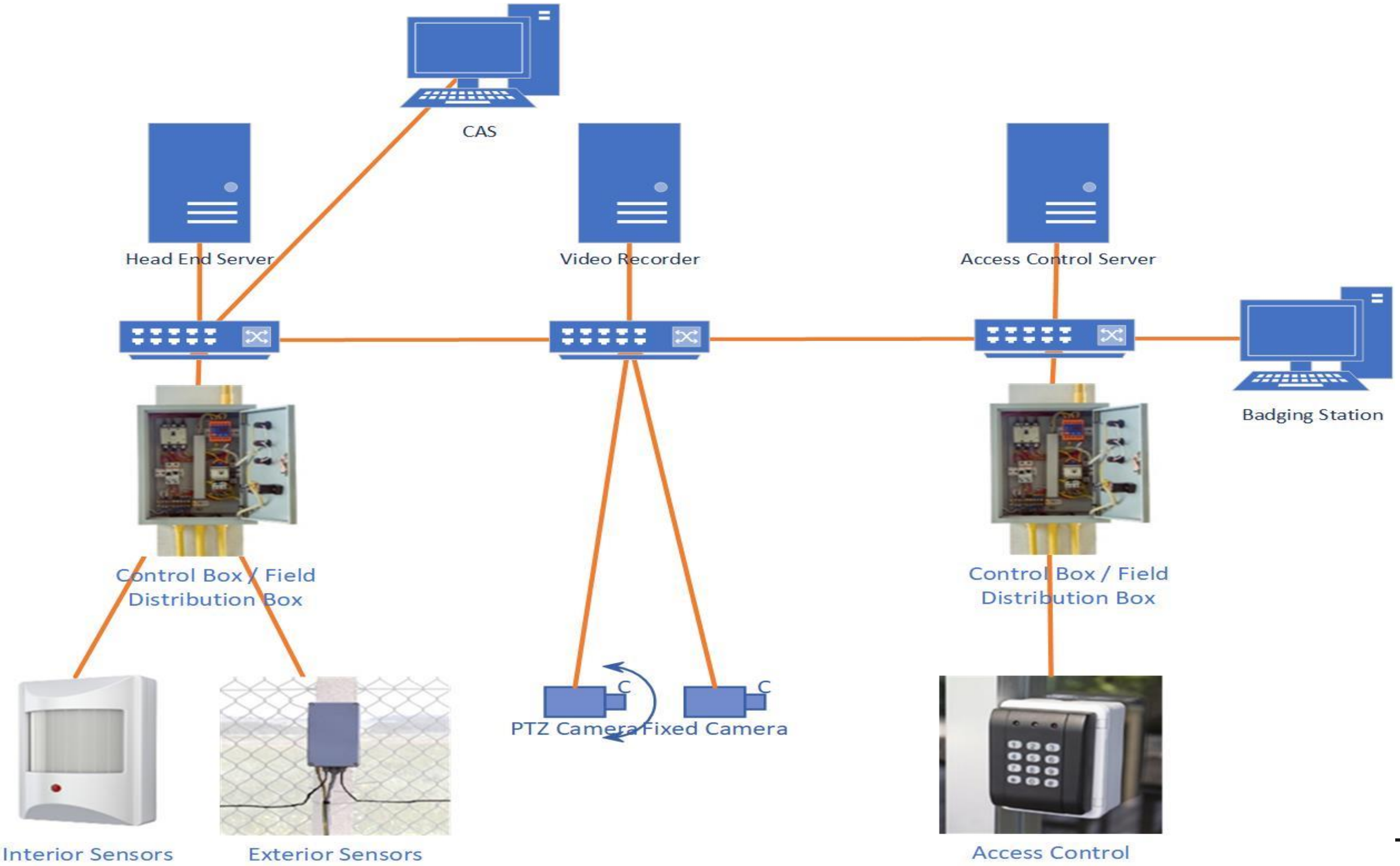
Defensive Computer Security Architectures (DCSA) are a vital element in the application of computer security to nuclear facilities.

Demands a DCSA that increases the difficulty of the adversary to access or have opportunity to sabotage vital equipment (Safety) or steal attractive material (security).

Computer Security DCSA is based on safety goals as compromise is an act of sabotage.



Generic computer infrastructure of a PPS Design

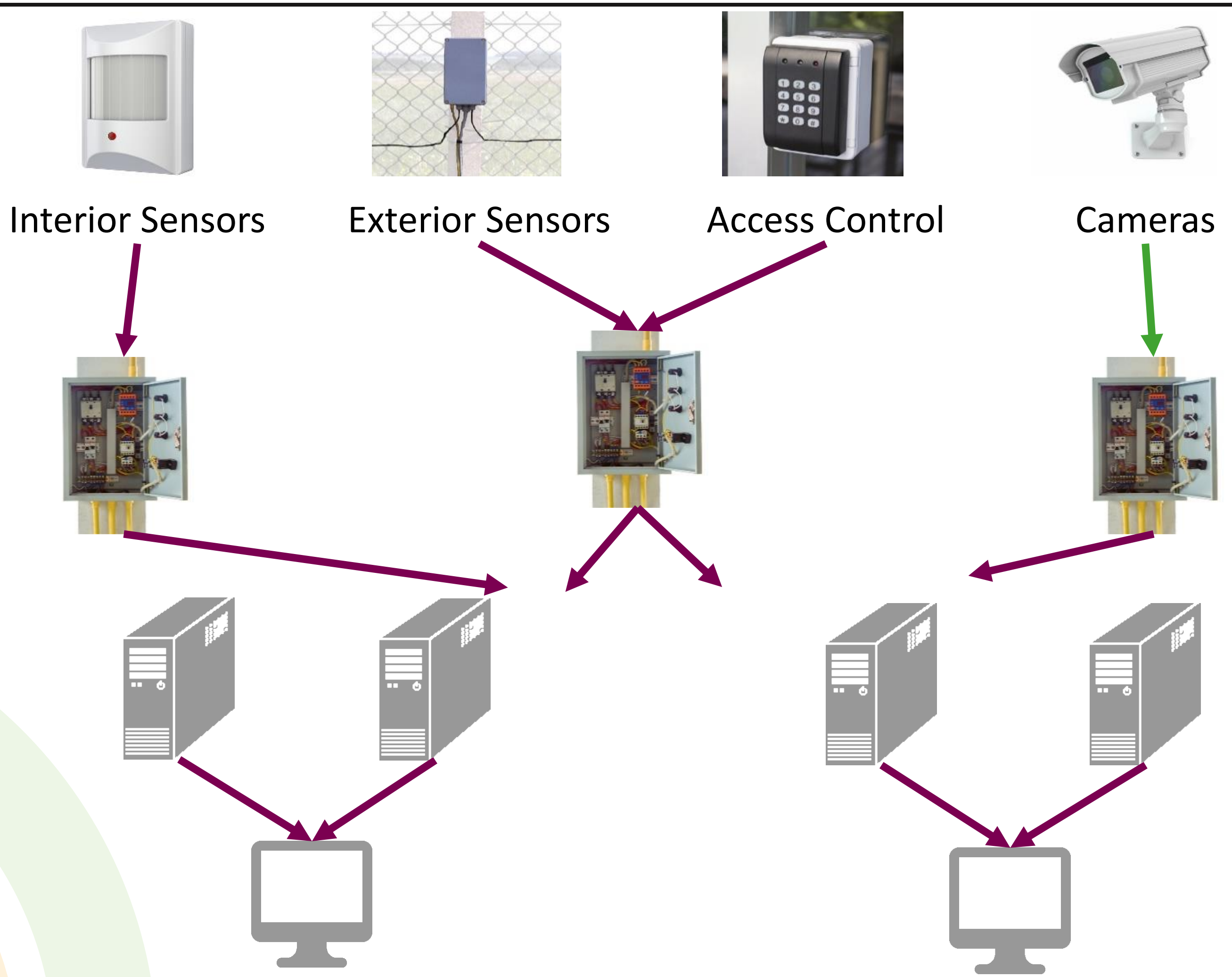


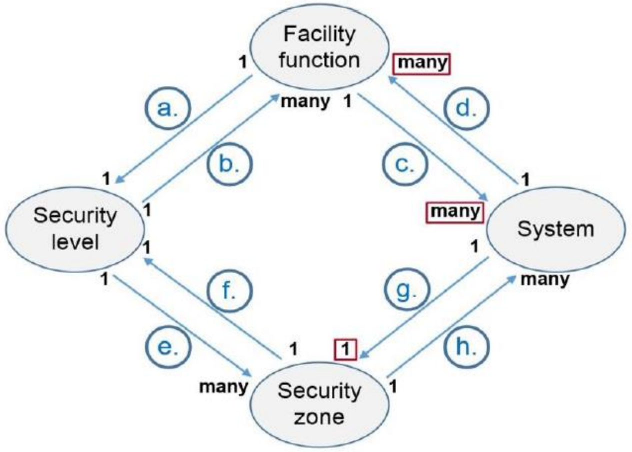
PPS Architecture – Single Level/Single Zone

Edge Devices

Control Box/ Field Distribution Box (FDB)

Head End System (AC&D)





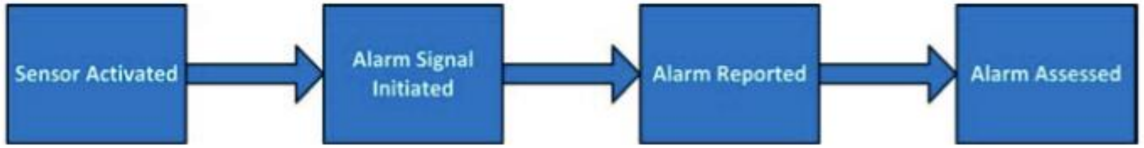
Confidentiality, Integrity, & Availability (CIA) Requirements for PPS

Confidentiality

- This is linked to the ‘prevent’ function of PPS
- “Prevent” is accomplished by restricting access only to authorized personnel
- Supported by information flows from the head-end system, including badging office, where the authentication information (biometrics, pin, card) are recorded.
- Authentication information is used to verify the identity of the person (or entity) requesting access to protected areas at the edge devices (pin, biometrics, card reader).
- Information used for authentication is personal identifiable information (PII) – needs to be protected

Integrity (Accuracy and Completeness)

- Information and data of PPS should be accurate and complete (e.g. true, unaltered, no gaps)
- Detect example:
  - Alarm signals generated by sensors need to be accurate and complete.
- Examples of Integrity failure:
  - Alarm not received (failure to detect)
  - Alarm received but not valid (spurious or nuisance alarm)
  - Alarm received but modified (video feed from camera, change in time, location)



Sensor Activated → Alarm Signal Initiated → Alarm Reported → Alarm Assessed

CIA Requirements for PPS - Continued

Availability

Typically, access control will fail-secure (prevent access) but this places burden on the security staff as manual checks will need to put into place.

More significantly, complete loss of perimeter monitoring will not be able to be compensated by available staff at the facility (i.e. not enough to monitor all zones).

This will lead to gaps in monitoring which would result in serious degradation of overall performance of the PPS.

- **Priority (highest to lowest)**
- **Integrity** – without complete and accurate alarms, the adversary has increased likelihood of success to evade detection before reaching the critical detection point.
  - Compromise of integrity can be accomplished through 'stealth' and therefore not identified by security staff without specific computer security measures in place.
- **Confidentiality** – disclosure of PII can lead to an adversary using the PII (e.g. copy prox card, crack passwords), modifying PII (changing biometric data, integrity of Access Control Lists) or adding new credentials.
  - Can be done through 'stealth' or even exfiltrated and done offline (cracking passwords)
- **Availability** – failures are immediately detectable and typically procedures and processes are put into place. Many PPS designs will fail-secure.

Necessity of Security Levels and Security Zones

Graded Approach

- Typical approach is to place PPS in the highest and/or second highest (most stringent) level
- Key control – isolation using a prevent access paradigm

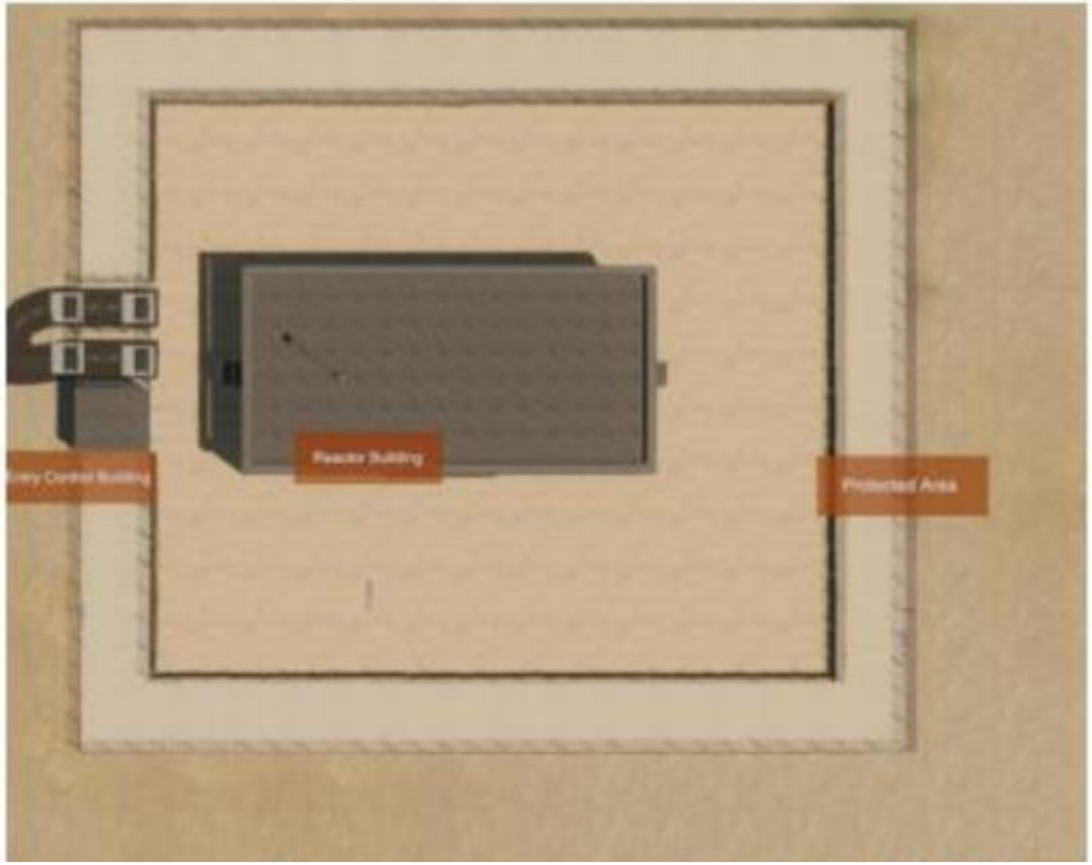
Defense-in-Depth Approach

- Typical approach is to place a PPS into a single zone (or multiple isolated zones)
- AES (advanced encryption standard) encryption used for communications within digital connections
- Line supervision to ensure no tapping, disruption, or ‘cutting’ of communication lines
- However, ‘data in use’ vulnerable to authorized insiders or adversaries able to exploit ’unknowing’ insiders
- Head-end systems are vulnerable

SCRIBE3D Simulations of CEIS

Work remaining for FY:

- Develop specific Defense-in-Depth strategies for the microreactor models utilized within previous ARS studies
- Measure and quantify the impact of success cyber attacks have on CEIS
- Do successful cyber attacks impact the PPS's ability to protect the material?



Conclusion

Under potential NRC rulemaking updates (10CFR73.110), PPS will be required to develop cyber security plans for their reactor sites

Current work has identified key requirements for the cyber components of PPS for microreactors

Remaining work is to develop and run SCRIBE3D simulated attacks (CEIS) where cyber attacks have been successful to quantify the impact cyber has on protecting the material

Thank you!