Australian Government

Ansto

Considerations for deploying a security information and event management system supporting physical protection systems in nuclear facilities

IAEA CN-254

Authors

- Mitchell HEWES
  Australian Nuclear Science and Technology Organisation
  Lucas Heights, Australia
  Email: mitchell@ansto.gov.au

- Alan COWIE
  Australian Nuclear Science and Technology Organisation
  Lucas Heights, Australia
  Email: ajc@ansto.gov.au

Outline

- Physical Protection Systems within a Facility
- Components of an ECS
- Where does a CSS fit in?
- Sensitive Information
- Information Security Assurance
- CSS monitoring a PPS
- Conclusion

Terminology

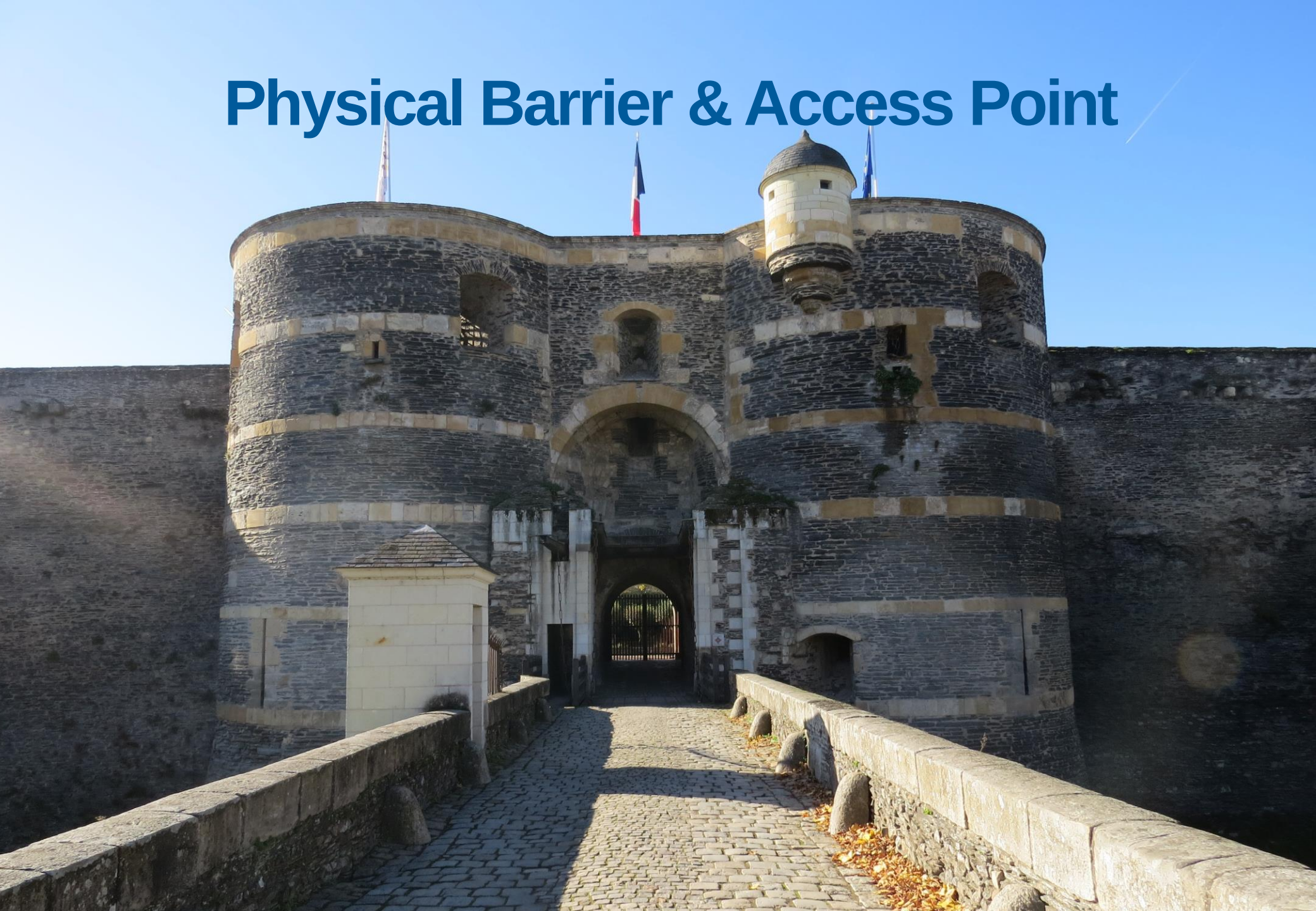
- PPS – Physical Protection System
- ECS – Electronic Control System
- CSS – Computer Security System

Physical Protection Systems within a Facility

Typical physical protection systems

- Physical barriers necessitate access points e.g. doors, gates, lifts
- Mechanical locks & keys
- Photo identification cards & documentation
- Guard personnel
- Access protocols & procedures
- Access log books & visitor lists

Physical Barrier & Access Point

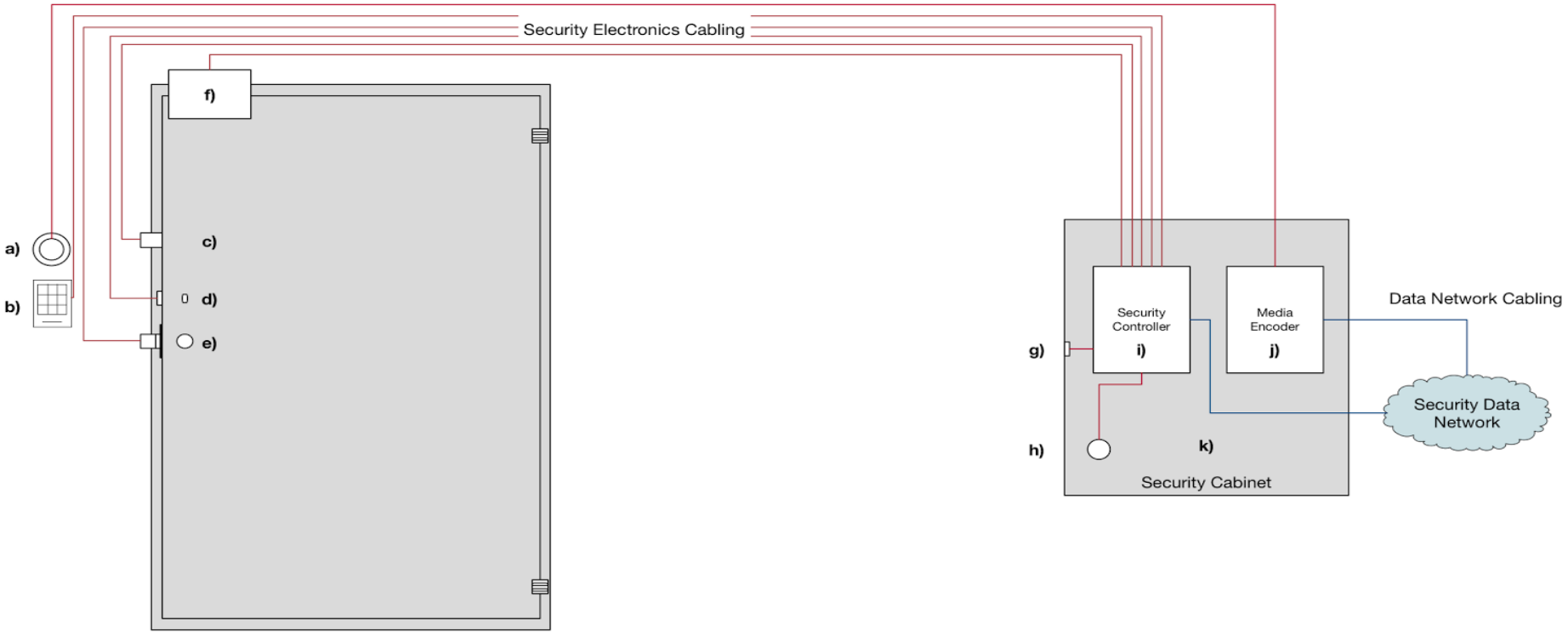


Guard Personnel

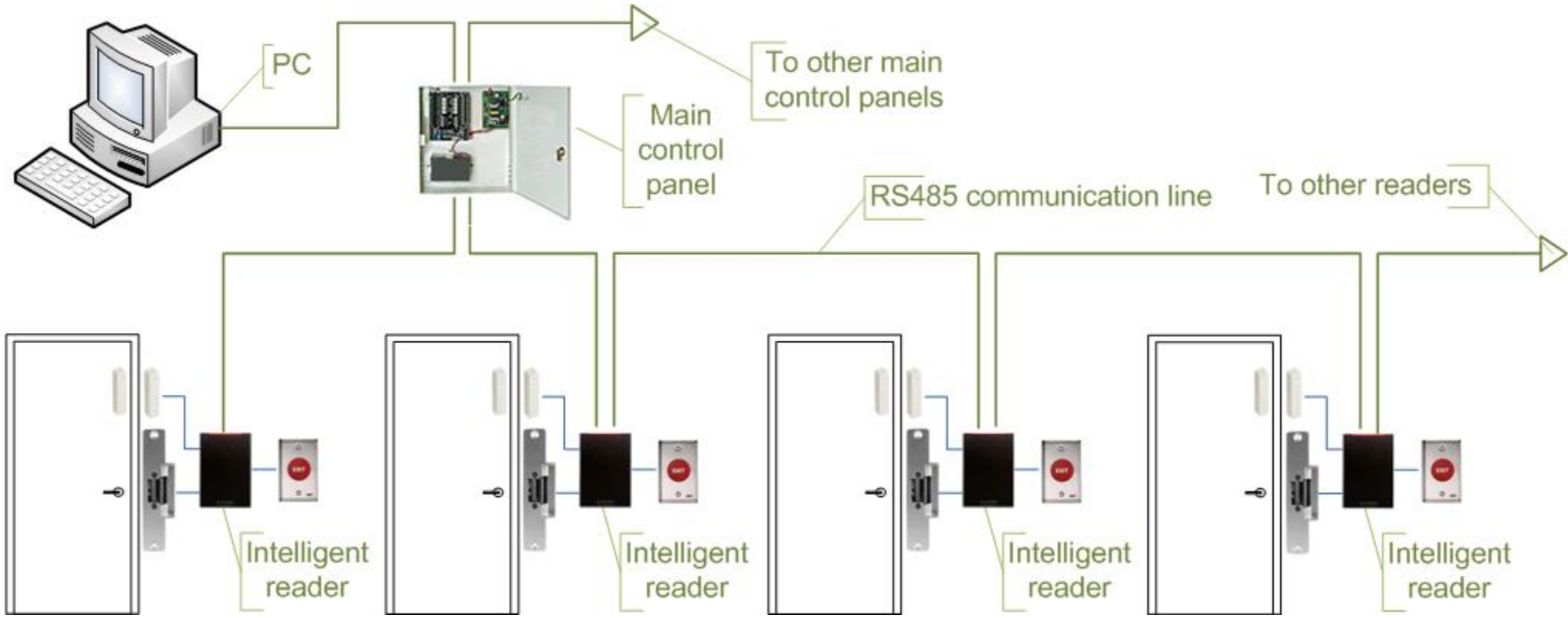
Components of an ECS

Electronic card/token & reader

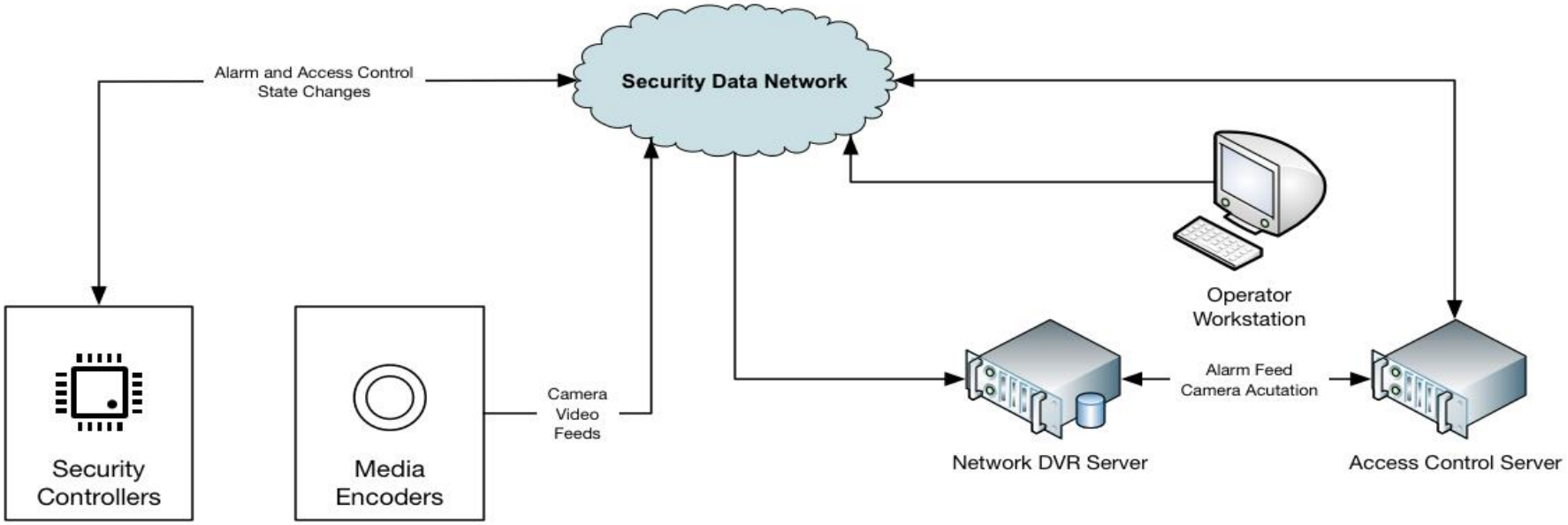
Access Controlled Door



Centralized Access Control



Computer-based components of an example networked security system.



Biometric Identification & Data

Purpose & Benefits of ECS

- Greater efficiency – augment physical
- Managing keys
- Robust record of actions undertaken
- Negate need for a guard at each door
- Monitoring and recording of the state of electro mechanical components
- Programmatic automation of Physical Processes e.g. Enforcement of a “no alone” zone

Where does a CSS fit in?

- In our example the Computer Security System forms an overwatch function for the ECS
- It would sit within a different security zone and take in inputs from multiple facility functions to be able to provide correlation for monitoring and response on attacks spanning multiple systems.
- How can we enable this while protecting the function of the ECS?

Sensitive Information

Sensitive Information

Automated State Change

- Items used in granting automated access
  - Card ID
  - PIN Number
  - Biometric Templates
- State information of electromechanical assets

- CCTV Camera video feeds
- Computer configuration
- New EACS parameters supplied to make system changes

Contextual State Change

Computer Security Measures for PPS

- Host integrity checking
- Sub zone network segregation
- Netflow - record capture and parsing
- Port monitoring
- Port security
- Wifi rogue monitoring/suppression

Data Flow Model Between PPS and CSS

- Sensitive information that could affect an automated state change within a facility function should not leave it’s source security zone while it is still functionally significant.
- Sensitive information that could affect an automated state change within a facility function must not be generated by a system at a lower security level.

Information Security Assurance

Goals

- Ensure the confidentiality, integrity, and availability of the automated operation of the PPS and the accuracy of information supplied to an operator to make contextual changes
- Monitor the operation of the computer-based hardware components and software for indicators of compromise.
- Provide independent computer security measures to ensure a defence in depth against a single computer security vulnerability.
- Enable the response, remediation, and restoration of verifiable normal operation.

Transitive from PPS: Deter, Detect, Delay, Respond

CSS Monitoring a PPS

- Monitor the computer-based components of the physical protection system and the computer security measures protecting them.
- Monitor the effectiveness of zone-decoupling measures for computer security zones interacting with the PPS.
- Decouple from the PPS itself - limit the information flow to prevent information important to automated operation of the PPS from being captured by the CSS. E.g. through a data diode.
- Provide the potential to correlate with the monitoring of other computer security zones to monitor the overall facility computer security defence in depth posture.

Conclusion

Conclusion

1. A nuclear facility PPS augmented with an ECS increases defence in depth from physical attack.
2. An ECS transfers some risk from a physical compromise to an computer-based compromise, thus the need to incorporate computer security measures to maintain defence in depth.
3. A CSS monitors computer security measures. Just as the ECS monitors the physical security measures.
4. A well thought out and implemented CSS, which preserves the confidentiality of sensitive information critical to PPS automation, is required to provide continued assurances of defence in depth.