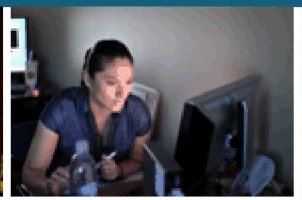
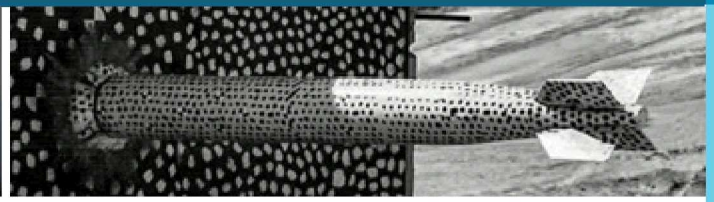
SAND2020-1669C

Evaluation of the Appropriateness of Trust Models to specify Defensive Computer Security Architectures for Physical Protection Systems



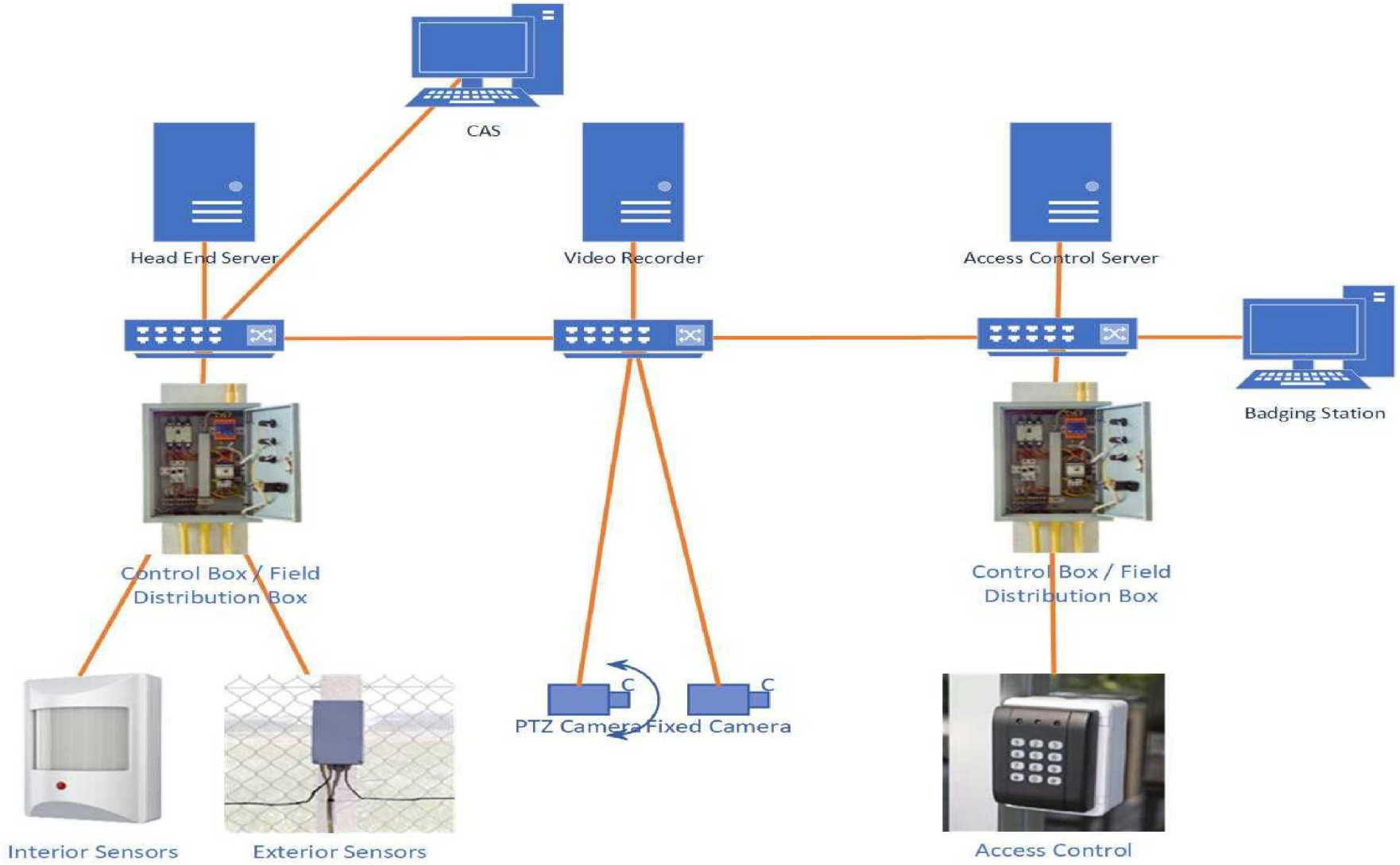


Presented By: John Sladek (CNSC)

Primary Author: Michael T. Rowland (Sandia)

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Generic PPS Design



Graded Approach

Graded Approach

Demands increasingly stringent requirements based on severity of consequence.

Ensures that level of effort to provide security is commensurate with the severity of consequence.

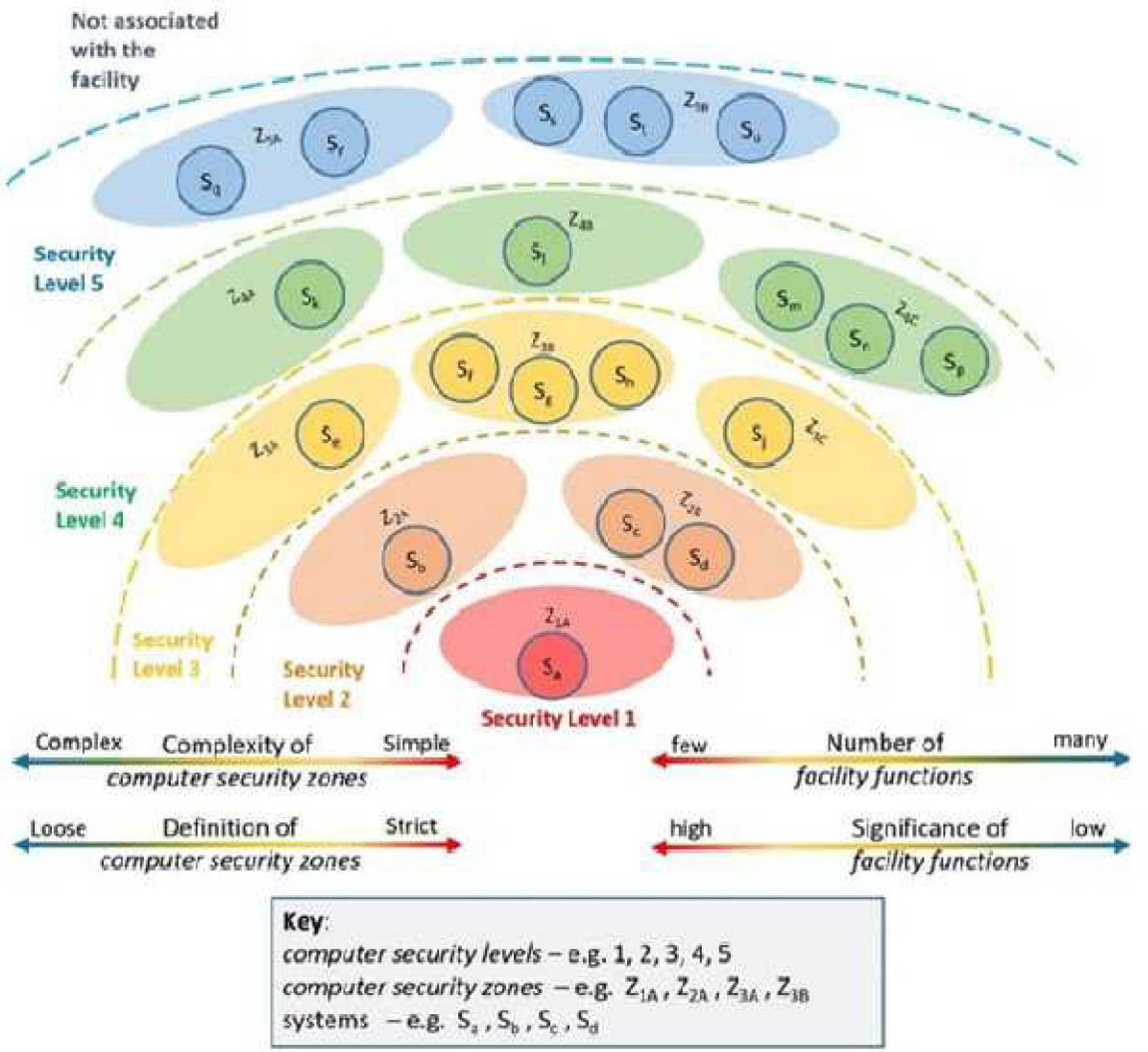
Defence in Depth

Defence in Depth

Defensive Computer Security Architecture (DCSA) increases the difficulty of the adversary accessing or having the opportunity to:

- sabotage vital equipment, resulting in safety consequence)
- gain unauthorized access to attractive material (theft of material), resulting in a security consequence.

The figure shows a DCSA based on safety goals.



Confidentiality, Integrity & Availability Requirements for PPS

Confidentiality (Example)

Example linked to PPS 'prevent' function

The prevent function is supported by restricting site access to authorized individuals

Supported by information flows from the head-end system and the badging office, where the authentication information (e.g., biometrics, PIN, card number) are recorded.

Authentication information is used to verify the identity of the person (or entity) requesting access to protected areas at the edge devices (using PIN, biometrics, card number).

Information used for authentication is PII and its confidentiality needs to be protected.

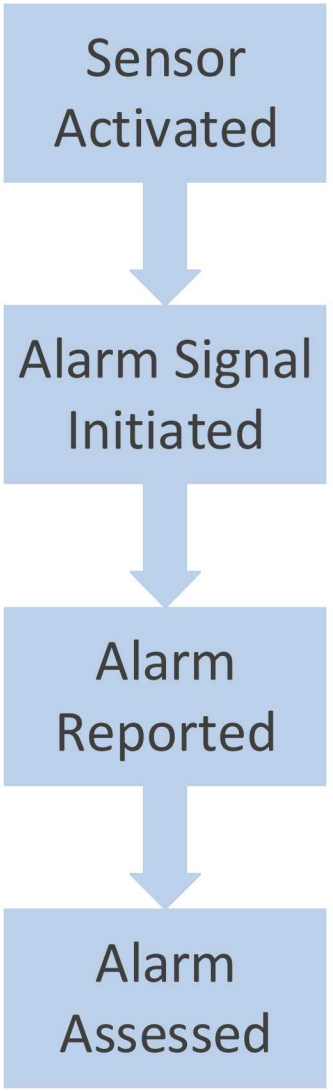
Integrity (Accuracy & Completeness)

Example taken from the 'detect' function.

Alarm signals generated by sensors need to be accurate and complete.

If integrity not provided, may result in:

- Alarm not received (failure to detect)
- Alarm received but not valid (spurious or nuisance alarm)
- Alarm received but modified (change in time or location)
- Modification of video signals used for assessment (e.g., security officer is presented old video data)



CIA Requirements for PPS - Continued

Availability

Loss of availability of PPS components will have impact on provision of security functions:

- Access control will typically fail-secure (preventing any access) but places burden on the security staff as manual checks will need to put into place.
- Complete loss of perimeter monitoring will be a significant challenging since security staff will be required to monitor the perimeter.
- If insufficient staff is available, this could result in gaps in monitoring which would result in serious degradation of overall performance of the PPS.

CIA Priority (highest to lowest)

Integrity – without complete and accurate alarms, the adversary has increased likelihood of successfully evading 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 access card, crack passwords) to modify PII (changing biometric data) or to use cracked passwords add 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 computer security measure - isolation using a “prevent access” paradigm

Defence-in-Depth Approach

- Typical approach is to place a PPS into a single zone (or multiple isolated zones)
- Line supervision to ensure no tapping, disruption, or ‘cutting’ of communication lines
- Encrypted communication (e.g., 3DES or AES)
- ‘data in use’ is vulnerable to authorized insiders and adversaries able to exploit ’unknowing’ insiders.
- Head-end systems are vulnerable.

Example Vulnerability

- Implantation of unauthorized attacker technology that can circumvent controls
- Created covert, remotely accessible, communications channel to access control server.
- John Clem, Sandia National Laboratories, IAEA-CN-254-298, ‘Potential Weaknesses in the Cyber Systems of High-Security Physical Protection Systems’

NSS 13 and NSS 27-G Requirements

Integrated (dictionary.com definition)

- organized or structured so that constituent units function cooperatively

Physical Protection System (NSS 13 definition)

- An integrated set of physical protection measures intended to prevent the completion of a malicious act.

Integration of PPS:

- mentioned 8 times within NSS 13
- Section 4 of NSS 27-G – "Developing, Implementing, and Maintaining an **Integrated** PPS"

Cyber-security impact of 'integration'

- PPS designs have an expectation of absolute and complete trust between devices
- This trust can be abused without formalized access control policies being implemented
- Requires a trust model to analyze system design to verify that CIA of PPS is protected from adversaries according to priority (e.g., I > C > A).

Functions of PPS – Demanded for Graded Approach

Physical Protection Functions are ‘detect’, ‘delay’, and ‘response’

These function descriptions do not allow for easy gradation and assignment to security levels.

IAEA NST047 states that ‘Facility Functions’ are:

- A coordinated set of actions and processes that needs to be performed at a nuclear facility.
- Each function is associated with specific purpose or goal that must be accomplished

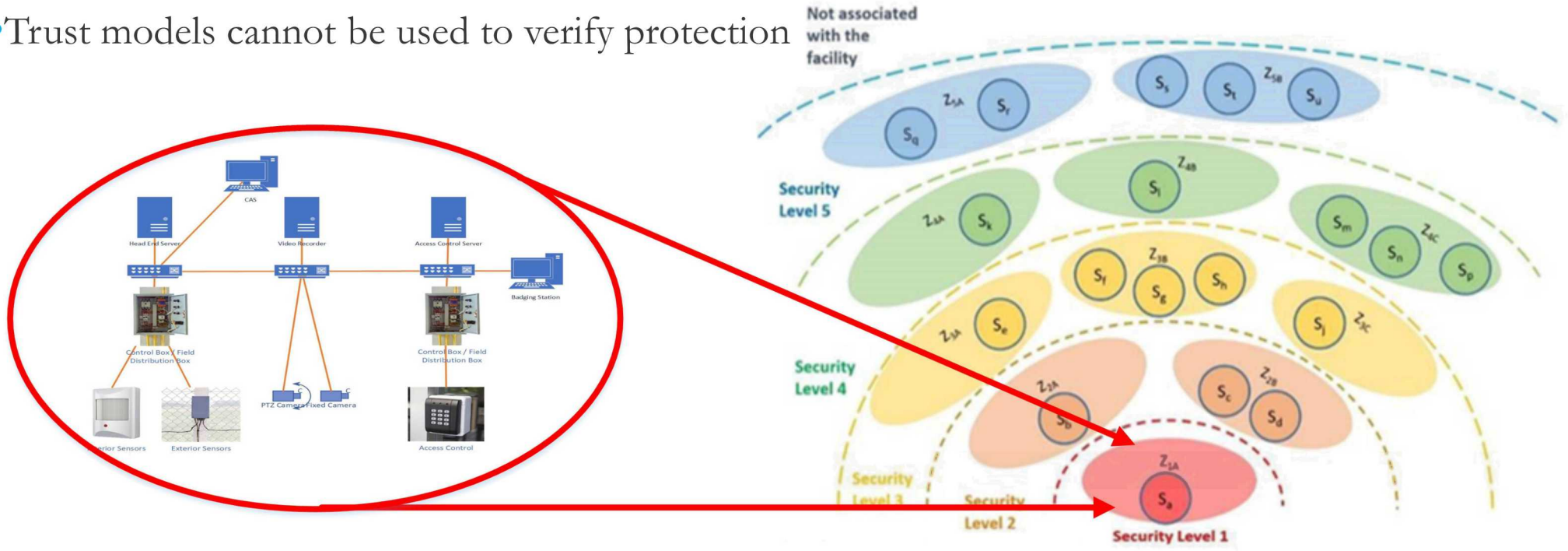
Detect, delay and response lacks the completeness required for assessment

Potential descriptions of PPS functions that can be assessed are:

- Detection of intruder at a Critical Detection Point
- Control of access at the protected area perimeter
- Detection of contraband entering protected area
- Visual assessment of potential security events at protected area boundary
- Detection of radioactive material in vehicles leaving the facility

PPS Architecture – Single Level/Single Zone

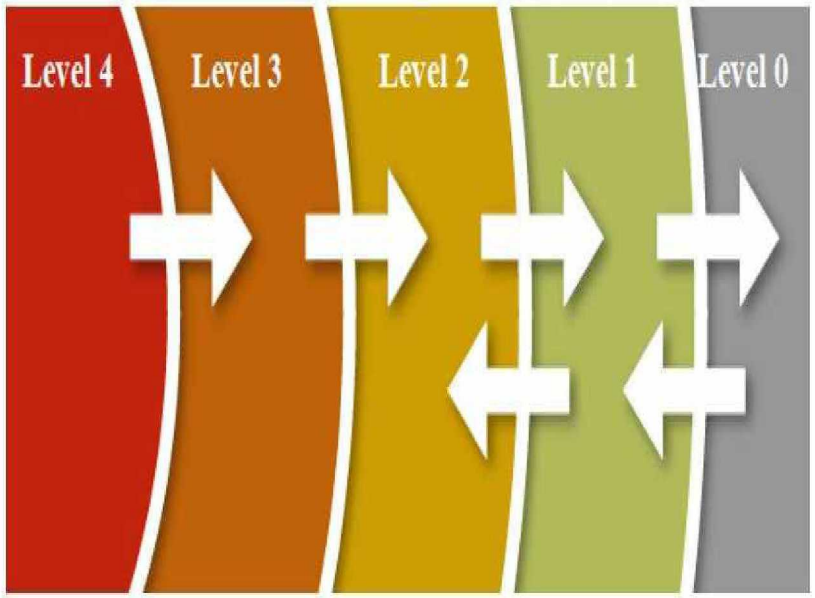
- Physical protection functions of 'detect', 'delay', and 'response' do not allow for assignment to security levels (no graded approach).
- Lack of grading (and focus on integration) does not support creation of security zones (no computer security defense-in-depth)
- May result in strategic vulnerabilities in architecture (e.g., all devices within PPS trust each other)
- Trust models cannot be used to verify protection



Biba and Bell-LaPadula

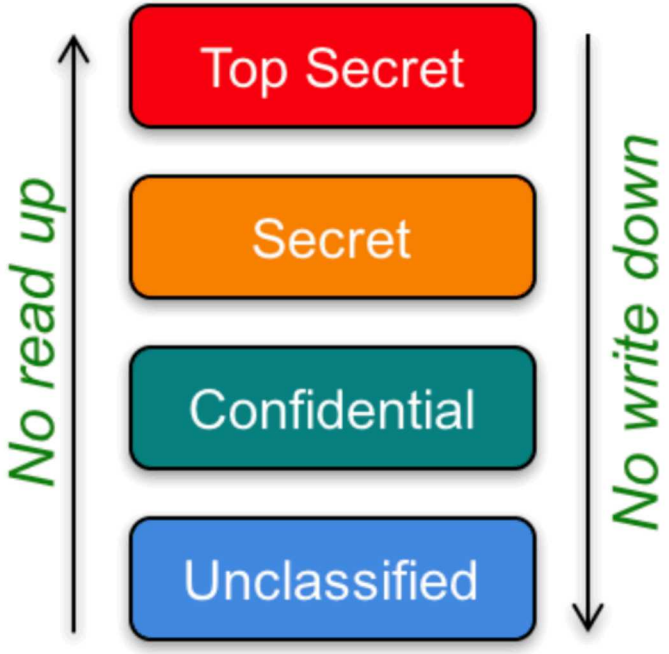
Biba Integrity Model

- Prioritizes the protection of Integrity
- Nuclear Safety systems – DCSA are built based upon or informed by this model.
- NEI 08-09 Rev 6 implementation



Bell-LaPadula

- Prioritizes the protection of Confidentiality
- Protection of Classified Information is informed by this model
- Inverse of Biba Integrity Model



References – Biba (NEI 08-09); Bell-LaPadula https://www.cs.rutgers.edu/~pxk/419/notes/access.html

Clark-Wilson

- Not a single specific policy, but a framework to specify 'class' of policies
- Addresses security requirements of commercial applications

  Reference: David D. Clark and David R. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, 1987 IEEE Symposium on Security and Privacy

- Enforces Integrity:
  - Only authorized users are allowed to make changes to the system.
  - Authorized users can't make unauthorized changes
  - Internal and external consistency are maintained

- Integrity requirements consist of two parts:
  - Internal consistency – properties of internal system state; enforced by the computer system (integrity verification procedures)
  - External consistency – relation of the internal system state system to real world; enforced by 'auditing'

- Mechanisms
  - Well-formed transactions – data can only be manipulated by a specific set of programs (transaction processes); users have access to programs and not data.
  - Supports separation of duties (no single user can manipulate data or circumvent the security system)

Clark Wilson

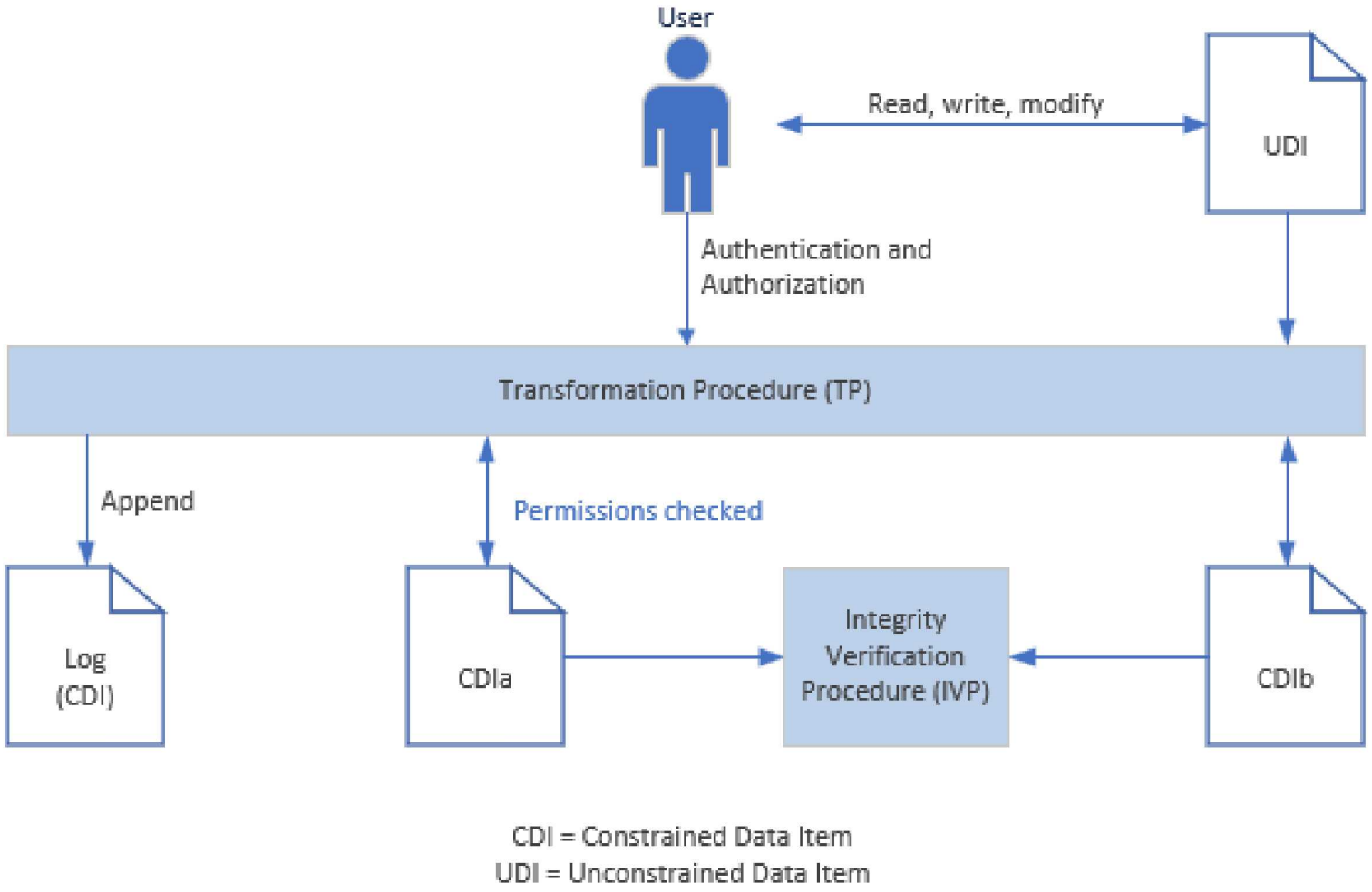


Figure based on: Dieter Gollman, *Computer Security (3rd Edition)*, John Wiley and Sons, 2011

Conclusion

PPS systems rely heavily on 'prevent' paradigm for computer security; increasing difficulty for a application of a graded approach or implementation of defence-in-depth for computer security.

Trust Models are useful to evaluate the design of systems and potentially inform new designs to implement nuclear security principles.

PPS systems need to prioritize Integrity; but Confidentiality shares almost equal priority.

Biba and Bell-LaPadula do not provide for near-equal prioritization

Clark-Wilson potentially allows for both; but more research is required to determine whether existing designs are or can be structured to generally comply with a framework of access control policies.

Thank you!