Cyber Insider Threat Mitigation in Industrial Environments

Sultan Al Owais

Problem Definition

- Cyber is the protection against unintended consequences of an engineered system through adversarial action.
- Systems are the combination of man, machine, measures, and environment.
- Security of industrial systems and critical infrastructure lags, definitionally, behind state of the art
- OT more difficult to reach and generally isolated to some degree, therefore harder to exploit.
- Motivated adversaries must direct their efforts to subverting 1) insiders and 2) supply chains

Cyber to Physical Security Comparison

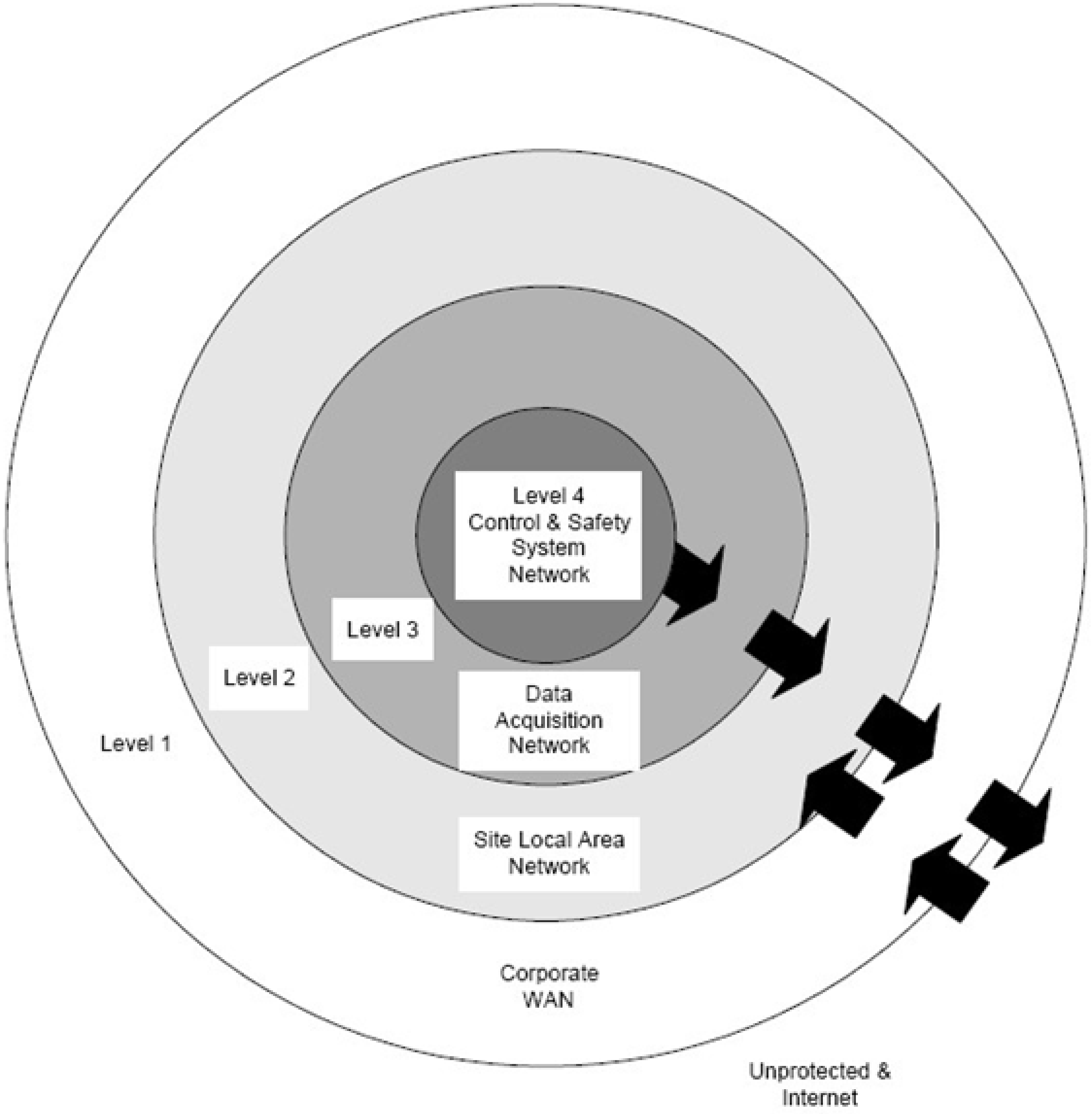
- Traditional physical security measures contribute greatly to cyber threat mitigation programs
  - **Personnel Security**
  - **Fitness for Duty**
  - **Management Observation**
  - **Perimeter Security**
  - **Physical Access Control**

- ..I use the word 'traditional' because cyber brings unique challenges
  - **Asymmetrical Impact:** The damage possible is not proportional to the number of adversaries
  - **Non-Obvious Harm**: Malicious actions may remain undetected due to the
  - **Complexity and non-intuitiveness** of computerized systems

High Level Design Principles

Integrity First

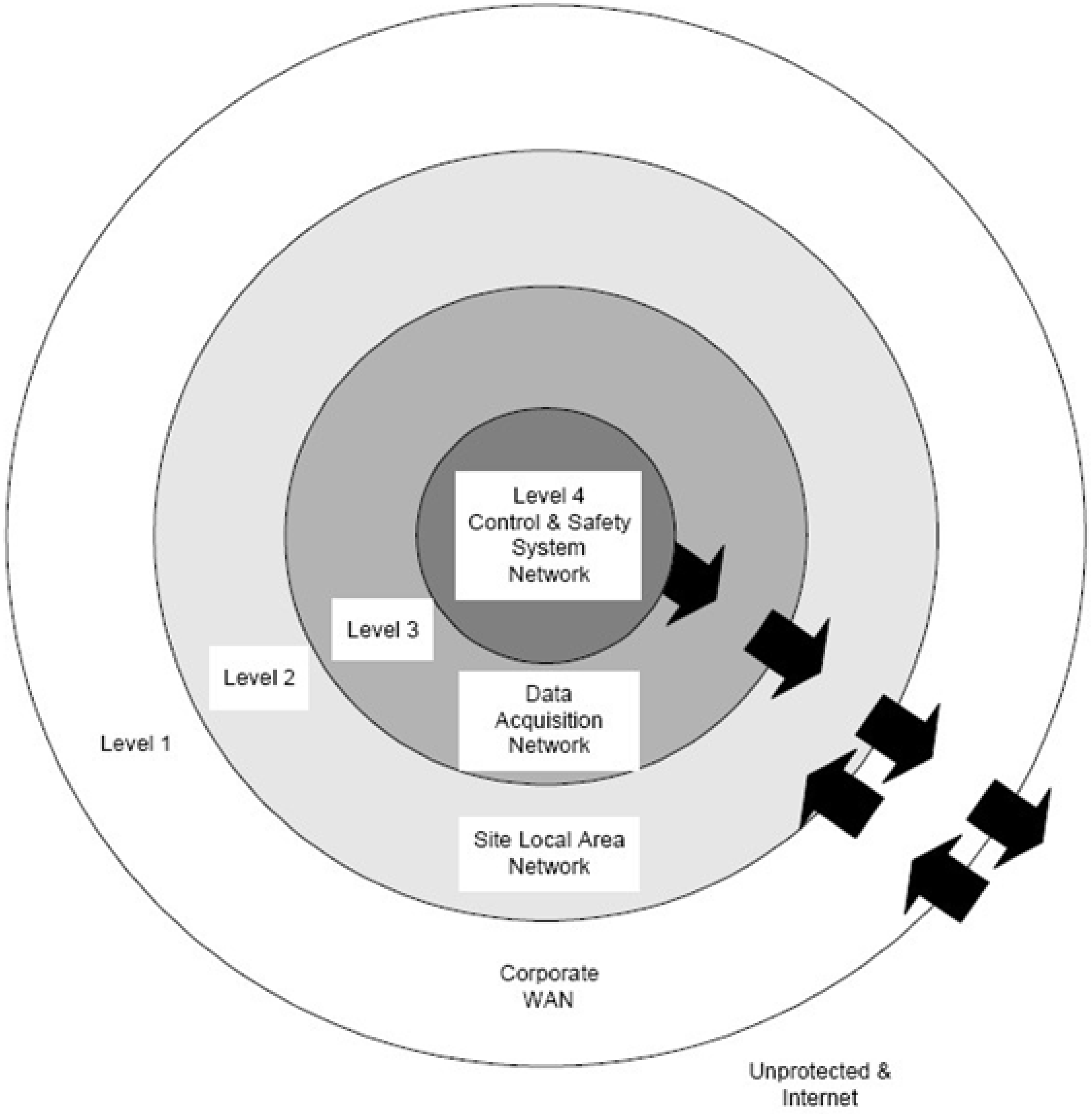
- Information flows out and not in to higher security levels
  - Data acquisition and export occur per design
  - No changes or traffic allowed into high critical systems
  - Authorized personnel in controlled area make authorized changes in accordance to procedure



High Level Design Principles

This is only a model

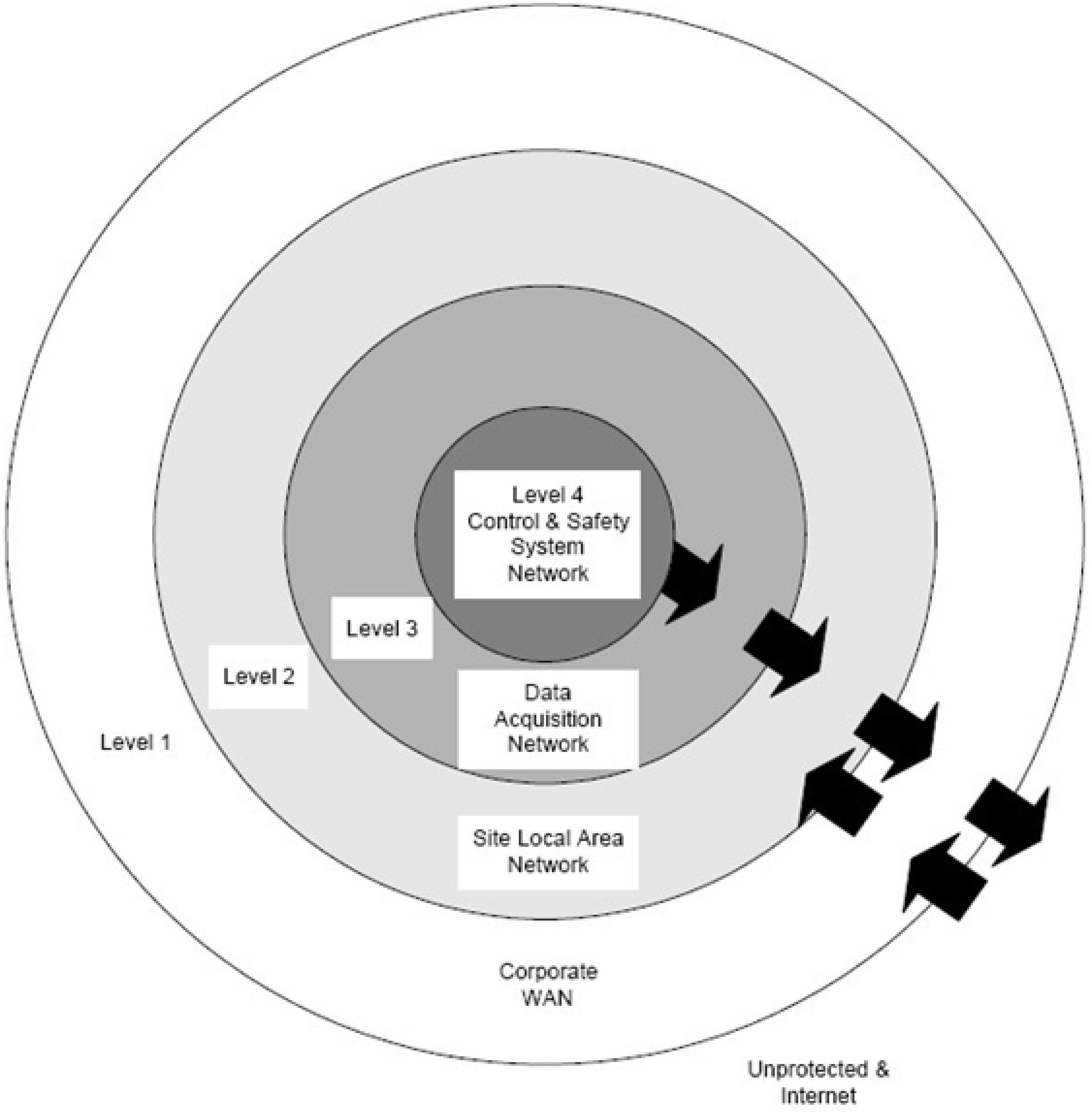
- Industrial design prioritizes safety, with redundant communication paths and direct connections
  - This includes dual-homed machines that connect **directly** to higher security levels
  - Remote connections, direct data connections, maintenance arrangements, EP, vendors, regulators
- A model not uniformly enforced is therefore partially and locally effective



High Level Design Principles

This brings unique challenges

- Observation of Cyber Actions harder than physical actions
    - Non obvious, asymmetrical, complex, counterintuitive technology
    - Security monitoring is best effort, slow to develop and implement, disruptive, and lags behind attackers
- Unique identification of Actors is not common or simple
    - Shared accounts, points of failure, compartmentalization
    - Justified safety bias, conservative decision making
    - “Shared nothing authentication”



Areas of Proposed Focus

- **Passive Monitoring:** with minimal impact to an industrial network, a replica of network traffic can be obtained, deduplicated, and studied out-of-band
- Using network taps, a new out-of-band security and operations management layer can be proposed.
- **This enables troubleshooting, problem analysis, and security**
- **Statistical Monitoring:** Actions in a controlled network are **Self Similar.** Anomalies to normal patters may indicate **unauthorized activities**
- **Network Behavior Anomaly Detection (NBAD)** and **User Entity Behavior Analysis (UEBA)** are very useful tools to detect security **AND** operational problems

Areas of Proposed Focus

- **Non-Repudiation:** Genuine, high confidence authentication and identification
- Computer actions must be uniquely linked to an **identifiable actor** if they are to leverage other security controls
- Single actor behaviors must be **linked** to actions and changes across **different security levels** to find patterns of anomalous behavior
- Multifactor authentication ideal for security but cannot be attempted in one go. Propose use of **PKI based access cards with PIN**

- **Application Whitelisting:** Procedures, training and software to include software runtime authorization in the configuration management program
- All application execution should be controlled to block **new software** that is unauthorized from running
- This is the single most significant mitigation in most environments and tops the ACSC list of strategies to mitigate cyber incidents

Summation

- **Safety** is the overriding concern; **security done right** only **supports and promotes safety.** Industrial environments are unique, and nuclear more so. The approach to security **must be informed** by the nature of the work.
- 4 mitigations are proposed which **take advantage of the special nature of industrial environments**
  - Passive Out-Of-Band Monitoring
  - Statistical Baselining and Monitoring
  - PKI access for IT Authentication (across levels)
  - Application Whitelisting
- **"There is no quick fix. There is no instant pudding."** –W. E. Deming

Thank you!

Questions, Remarks, Suggestions?