cigre

For power system expertise

Impact of Cyber Security of Digital Substations

22/11/2023

Authors: Prasad Balasubramani, Ryan Murphy

What Is Cyber security ?

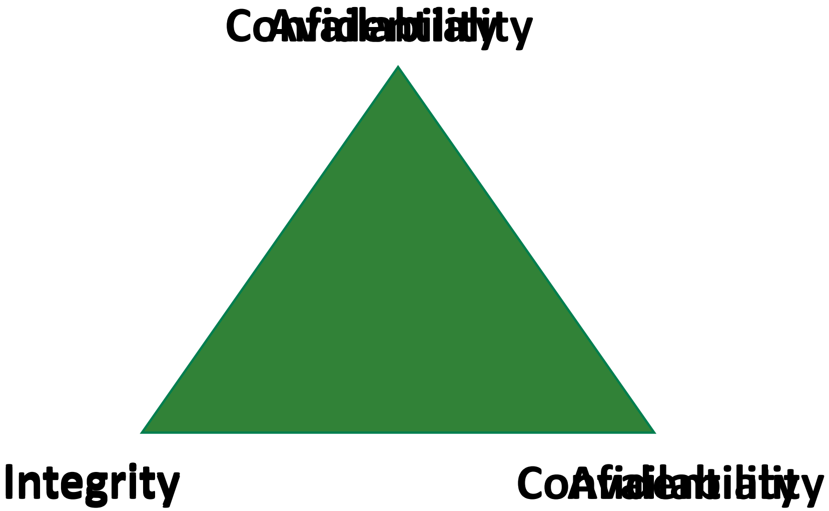
- Cybersecurity is the practice of protecting systems, networks, and programs from Cyber attacks by implementing countermeasures including the following:
  - Policies and Procedures
  - Systems and Technology
  - Maintenance

Common Myths of cybersecurity in OT ?

1. OT Systems don’t connect to internet
2. Our control systems are behind a firewall
3. Intruders are not OT knowledgeable
4. Our facility is not a target
5. Our safety system will protect us

Need for Cybersecurity

- Traditionally in IT environment it is for protection of what is called the CIA Triad.

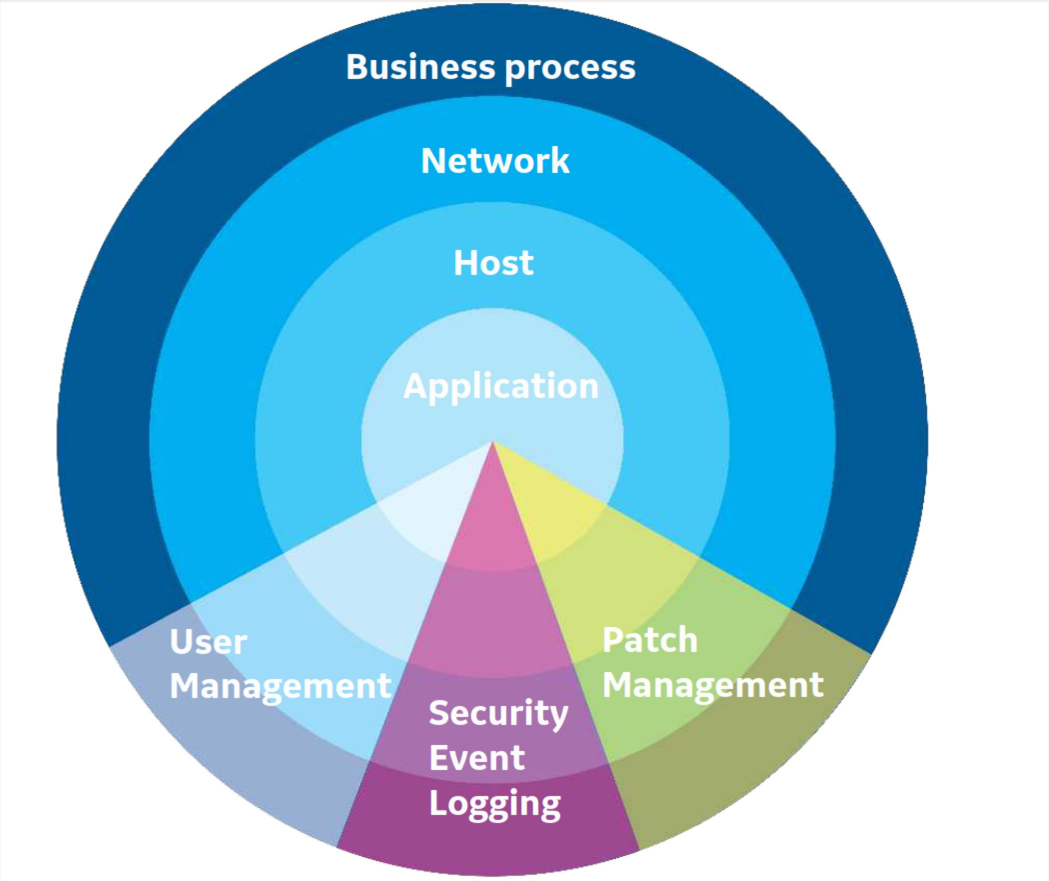


- Operational Technology (OT) cybersecurity is a key component of protecting the uptime, security and safety of industrial environments and critical infrastructure.

Defense In Depth Mechanism

- Layered counter measures

- Delay access for intruders



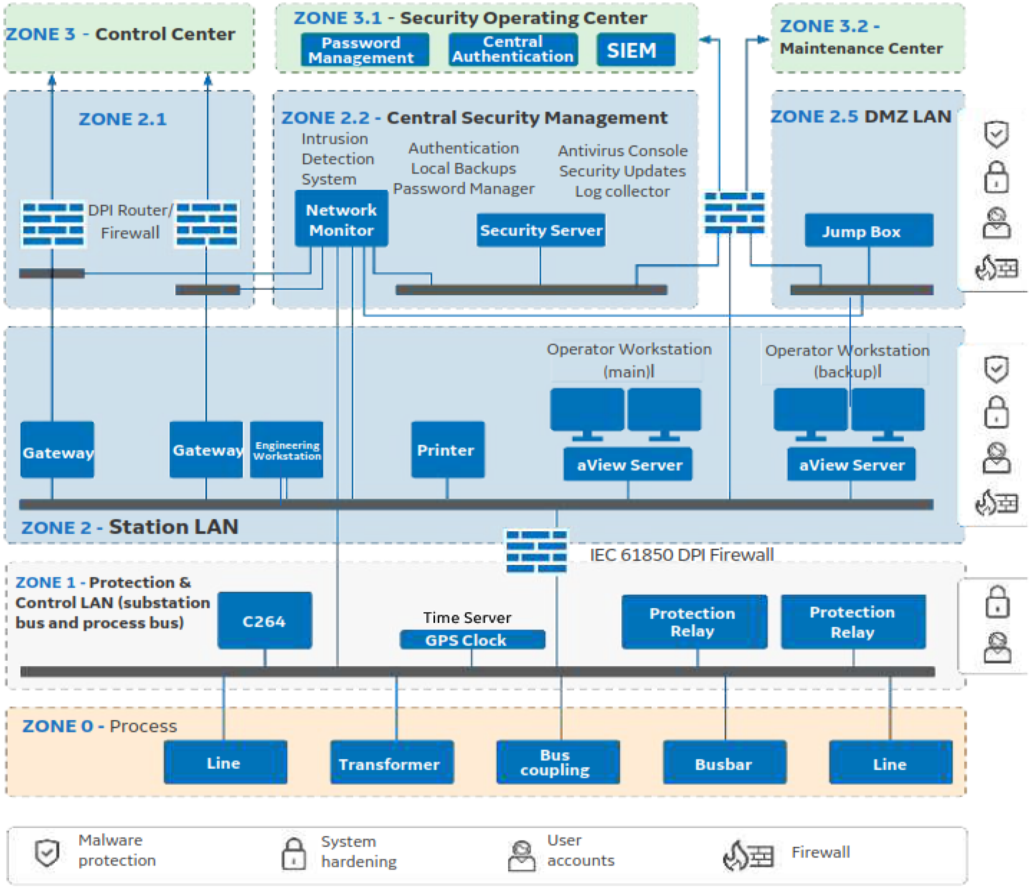
Security Level

- SL0 – No specific requirements or protection necessary
- SL1 – Protection against casual or coincidental violation
- SL2 – Protection against intentional violation using simple means with low resources, generic skills and low motivation.
- SL3 –Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL4 –Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation.
- SL-T : Security Level - Target
- SL-C : Security Level - Capable
- SL-A : Security Level – Achieved

Reference: ISA/IEC 62443

Systems and Technology Implementation

- What is a system based of:
  - Zones
  - Conduits
- Identity Management
  - Based on RBAC as per IEC 62351-8
  - RADIUS, LDAP, TACACS+
  - MFA (Multi-factor Authentication)



Reference: https://www.gegridsolutions.com/app/viewfiles.aspx?prod=cybersecurity&type=1

Systems and Technology – Encryption and Hardening

- Encryption
  - PKI (Public Key Infrastructure)
  - TLS (Transport layer security)
  - SSH

- Hardening

- SIEM (Security information and event management)

Systems and Technology – HIDS and NIDS

- HIDS (Host intrusion detection system)
  - Antivirus
  - Integrity Protection
  - Hardening
- NIDS (Network intrusion detection system)
  - Detection in depth
  - Detection of unusual data transfers or protocols
  - Asset inventory management

Systems and Technology – SOC Connectivity

- What is an SOC
  - SIEM log monitor
  - Patch Management
  - Vulnerability management
- DPI Firewall or Data Diodes
- Demilitarized Zone
- VPN (Virtual Private Network)
- MFA (Multi-factor Authentication)

Cybersecurity on Process Bus Zone

- Dedicated VLAN for SV, PTP & GOOSE traffic
- Dedicated Process bus interface
- Dedicated Management Interfaces or isolate the network using network intelligence based on VLANs or Multicast filters
- Use of SDN; Performance would be a challenge

Impacts on digital substation and Future Challenges

- Impacts:
  - Complex network Architecture
  - High demand for network and Cybersecurity knowledge
  - Future expansion of bays and substation
  - Remote management and Cybersecurity management of low SL zones (Process Bus)

- Future Challenges:
  - Performance impact while using encryptions of process bus data traffic
  - GPS spoofing and effects on process bus data
  - Non-compliance of cybersecurity functions on process bus components can reduce the SL-A of the overall system
  - Use of SDN on process bus networks

Q&A

Thank you for listening

cigre

For power system expertise