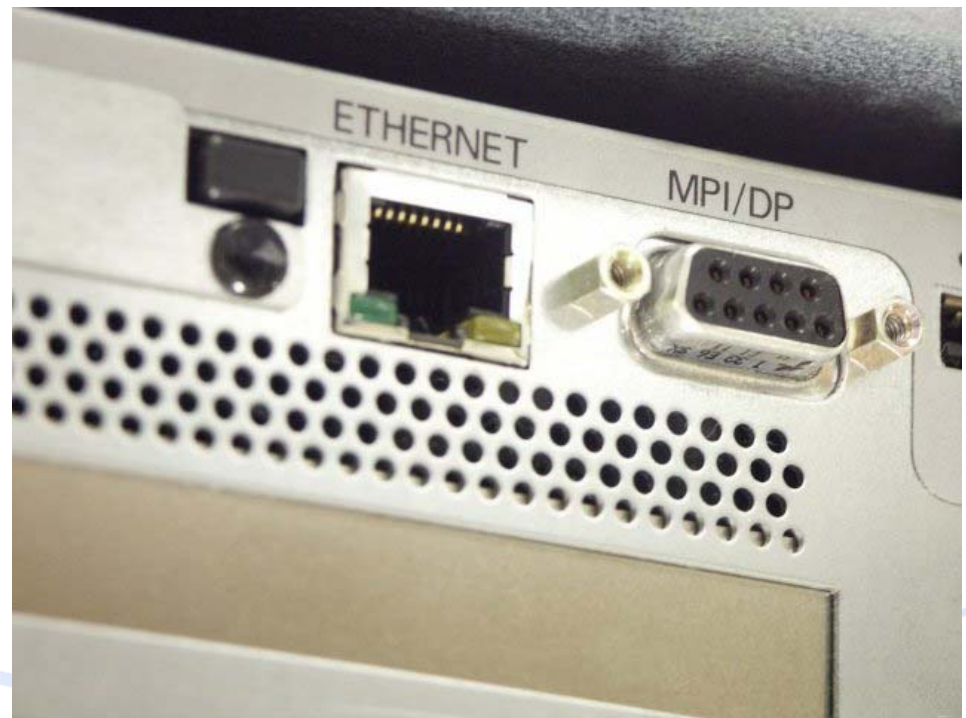


Electric Reliability Council of Texas (ERCOT)

Cyber Security Workshop

Defining the Electronic Security Perimeter

Bill Addington



Assets

- Critical Assets ->
 - Critical Cyber Assets ->
 - Electronic Security Perimeters
 - Access Control and Monitoring Devices
 - Non-Critical Cyber Asset

Requirement: Electronic Security Perimeter CIP-005/R1

- **R1 – The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.**
- **Identify and document**
 - **Electronic Security Perimeter**
 - **Can have many such perimeters in organization**
 - **All access points to the perimeter**
 - **Identify different device types used as access points**

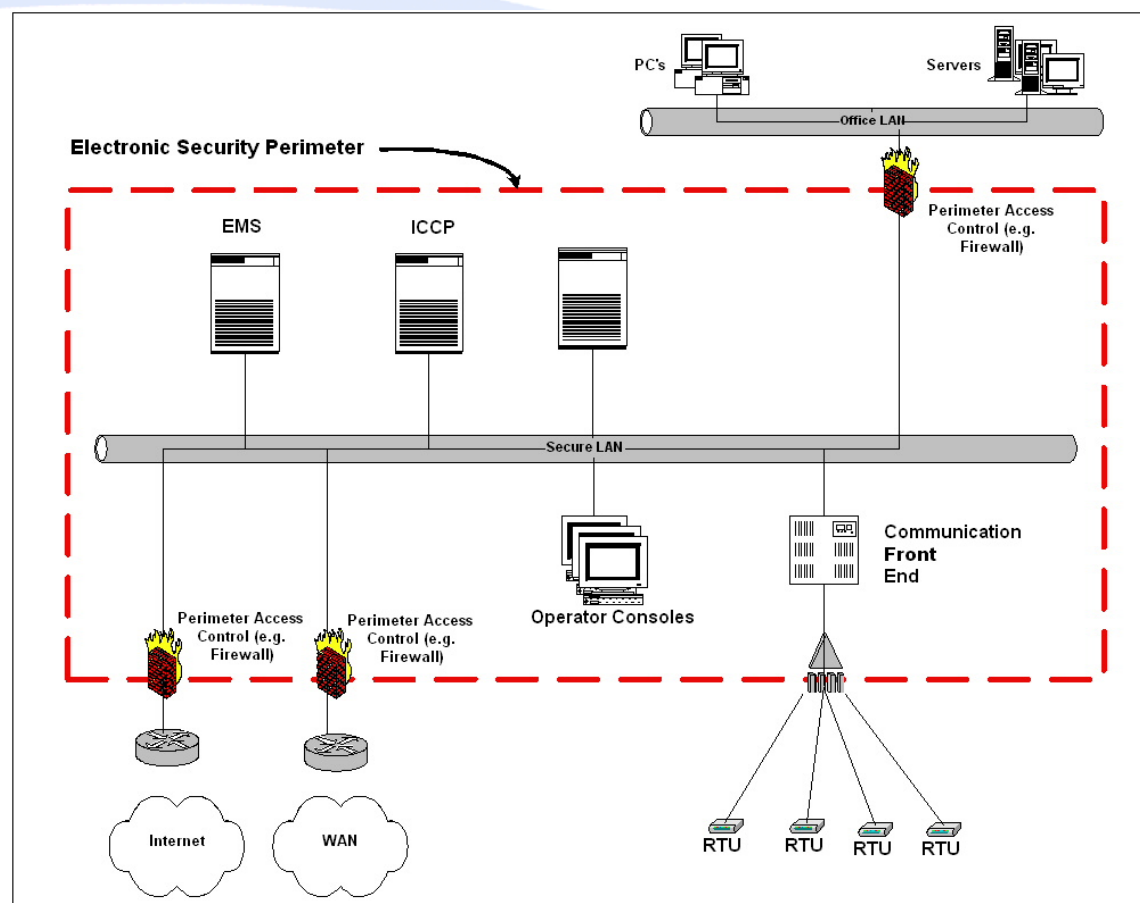
Electronic Security Perimeter (ESP)

- Logical concept
 - Doesn't physically exist
 - Cyber Assets within a defined perimeter are accessible only through a defined access point for the ESP.
- Identify
 - Provide a name or other unique identifier
- Document
 - Critical Cyber Assets within the ESP
 - Non-Critical Cyber Assets within the ESP
 - Access Points for the ESP

Access Points

- An access point is any place where electronic traffic crosses the Electronic Security Perimeter
 - Examples (not all inclusive)
 - Routers (including wireless access points)
 - Firewalls
 - Dial-Up
 - Radio Frequency (RF) devices
 - Infrared (IR) devices
- Terminates at any device within the defined ESP

ESP illustration



Evolving Network Infrastructure

- Convergence of control systems (SCADA, EMS, OMS, DMS)
- Linkage to Corporate networks
- New access points to the corporate network
 - Service providers
 - Supply chain partners
 - Customers

Evolving Substation roles

- No routable protocols (No NERC Critical Cyber Assets)
- Routable protocols within but not connected externally (No NERC Critical Cyber Assets)
- Connected to Control Center via routable protocol, connected to other substations (Yes, NERC Critical Cyber Assets)
- Connected to Corporate LAN (Video links, physical security equipment)
- Rogue access points (External links for projects, wireless for convenience)

Substations

- Regardless of importance to business, not worried about distribution load serving status UNLESS the station could affect the grid (cascading failure)
- Subset of stations could be critical assets
 - Tie Lines
 - Black start corridor
- Can apply standards to non-critical substations, but don't put on Critical Asset list
- Substations designated as critical will have to have at one defined access point

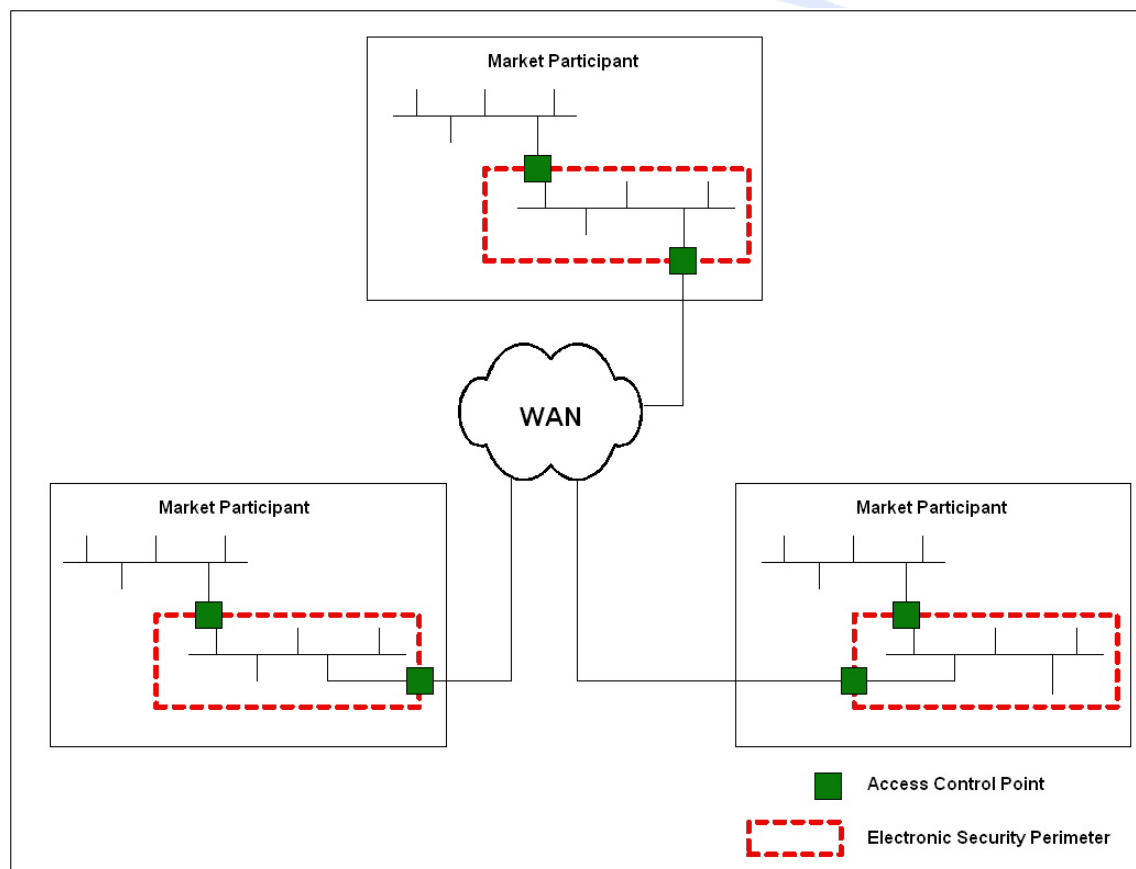
Other Considerations: Dial-up

- Dial-up connection to a single device that does not use a routable protocol requires a separate ESP be defined and documented for that device
 - ESP requires access control and logging
 - Must meet requirements defined throughout CIP for access control

Communications Links

- Links between perimeters are not part of the ESP (explicitly EXCLUDED)
- End points of those links are access points
- If substations are linked together without intervening access control points, they then lie within the same ESP and communications links ARE included for audit accountability
 - How would you physically protect them?

Communications Links



Access Control

- Access points and cyber assets used in access control and monitoring require the protective measures defined throughout the CIP standards
 - Access control management
 - Physical Security

Documentation

- Each Electronic Security Perimeter
 - All devices connected with routable protocols within the defined perimeter
 - Critical Cyber Assets
 - Non-Critical Cyber Assets
 - Consider moving non-critical assets to separate electronic perimeter
 - Electronic access points for the ESP
 - Cyber Assets required monitoring and control of the access points
- Document any changes to the ESP, access points or controls within 90 days of the change

Required Review

- **Review the defined ESPs annually and update as necessary**
 - Perimeters all defined?
 - All documentation maintained and accessible?
 - All Critical cyber assets located in an ESP?
 - Documentation process integrated into change management process?
 - All changes being reflected properly?

Substation Governance

- Many organizations, substation property is a communal asset with no centralized person or group responsible for all changes to the substation
- Change management and documentation is now essential for substations designated critical