

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Primer Discussion on Cyber Security: What do the CIP Standards Mean for SynchroPhasors in the future?

NASPI Meeting

Scottsdale, AZ

February 5, 2009

Scott Mix, CISSP
Manager of Situation Awareness
and Infrastructure Security
Scott.Mix@NERC.net
215-853-8204

to ensure
the reliability of the
bulk power system

- Introduction
- The Short Answer
- What do the standards say?
- What do I need to do immediately?
- What should I consider doing?
- Examples

- Who am I?
 - Cyber Security Practitioner
 - Control Center focus
 - Knowledge of field issues
- Why is this talk necessary?
 - Confusion and concern about applicability and application of CIP standards to SynchroPhasor implementations

The Short Answer:

- SynchroPhasors are a new technology
 - Require maturity before CIP issues are clear
 - Represent an important advance and need to be promoted and deployed in a smart manner without fear
 - CIP Standards are new and are also maturing
- Most SynchroPhasor applications are not critical to the operation of the Bulk Electric System today
- **Probably not a CCA now but could become one as applications develop and mature (most likely will include some future applications and not others)**
- **This presentation will provide the context for asset owners to discuss and develop thinking about future phasor applications relative to the Critical Cyber Asset (CCA) threshold**
- Asset owners must recognize existing electronic security perimeters associated with existing Critical Cyber Assets

What do the standards say?

Critical Asset*:

- “Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”*
- Interpreted to mean substations, power plants, control centers, etc
- Industry evolution away from “facilities and equipment” analysis toward a “systems and functions” analysis
- Asset determination is based on BES impact, not Cyber Assets at the location

Characteristics of Reliability*:

1. The BES is controlled to stay within acceptable limits during normal conditions;
2. The BES performs acceptably after credible Contingencies;
3. The BES limits the impact and scope of instability and Cascading when they occur;
4. The BES's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The BES's integrity can be restored promptly if it is lost; and
6. The BES has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.

What do the standards say?

Cyber Asset*:

- “Programmable electronic devices and communication networks including hardware, software, and data.”
- Interpreted to mean computers or other devices with microprocessors

What do the standards say?

Critical Cyber Assets*:

- “Cyber Assets essential to the reliable operation of Critical Assets.”
- Interpreted to mean computer (microprocessor) devices directly supporting Critical Assets and therefore the BES
- Critical Cyber Assets only exist “in association” with Critical Assets

What do the standards say?

Electronic Security Perimeter*:

- “The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.”
- Within a substation, interpreted to mean a substation LAN to which Critical Cyber Assets are attached.

What do the standards say?

Protection Requirements:

- Critical Cyber Assets
 - Following the definitions above
- “[T]he non-critical Cyber Assets within the Electronic Security Perimeter(s).”^{*}
 - Based on network connectivity with existing Critical Cyber Assets

* NERC Standard CIP-007-1 Preamble

What do the standards say?

Is the SynchroPhasor a Critical Cyber Asset?

- Is it “associated with” a Critical Asset?
- Is it used in a “key” control process? (Future potentials)
- Is its data used to make control decisions? (Future potentials)
- Does it supply data or perform control to support the BES? (Future potentials)

What do the standards say?

In other words:

- **If** a SynchroPhasor is associated with a Critical Asset, **and**:
 - **If** the SynchroPhasor is designated as a Critical Cyber Asset by the Registered Entity in the future, **or**
 - **If** the SynchroPhasor is on the same LAN as Critical Cyber Assets designated by the Registered Entity
- Then it will be subject to the NERC Cyber Security Standards

What do the standards say?

Issues:

- Is non-critical SynchroPhasor functionality integrally embedded in a Critical Cyber Asset?
- Is the SynchroPhasor's data moving on a Critical Cyber Asset LAN?
 - Does it need to be?
- Does the SynchroPhasor share instrumentation (i.e., CT, PT) with Critical Cyber Assets?
- Does the SynchroPhasor share “intelligent instrumentation” (i.e., an instrumentation bus) with Critical Cyber Assets?
- What about 61850?

What do I need to do immediately?

- **No action**, just need to think and plan for the future. (caveat: except to respect existing ESPs)
- Assumptions? (Let's discuss)
 - The *locations* containing the SynchroPhasor devices are in direct support of maintaining reliability (as described in the ALR document)
 - The *locations* containing the SynchroPhasor devices might meet the criteria to be classified as Critical Assets, based on the application and problem being solved.

What do I need to do immediately?

- If the SynchroPhasor is designated as a Critical Cyber Asset by the Registered Entity (in the future)
 - It must comply with the CIP Standards
- If the SynchroPhasor uses the same LAN as Critical Cyber Assets
 - It must comply with the CIP standards or move to a separate LAN segment

What should I consider doing?

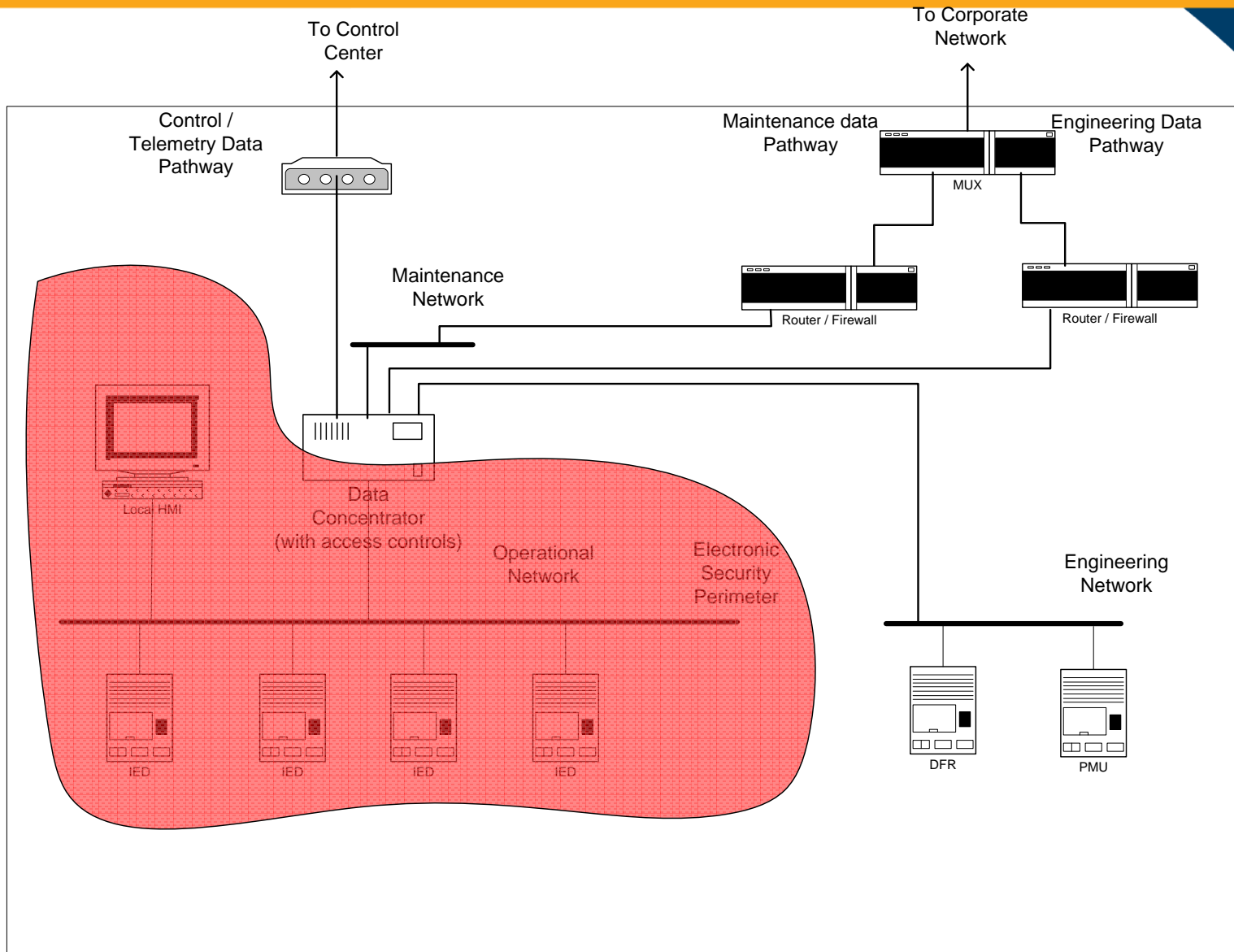
Valid assumptions?

- Applications for real-time use of SynchroPhasor data will be developed
- SynchroPhasor data and analysis tools will eventually be used for control
- SynchroPhasor data-based controls will probably be autonomous
- Some SynchroPhasors will therefore be deemed Critical Cyber Assets (subject to factors associated with how the technology is deployed and networked) by their owners

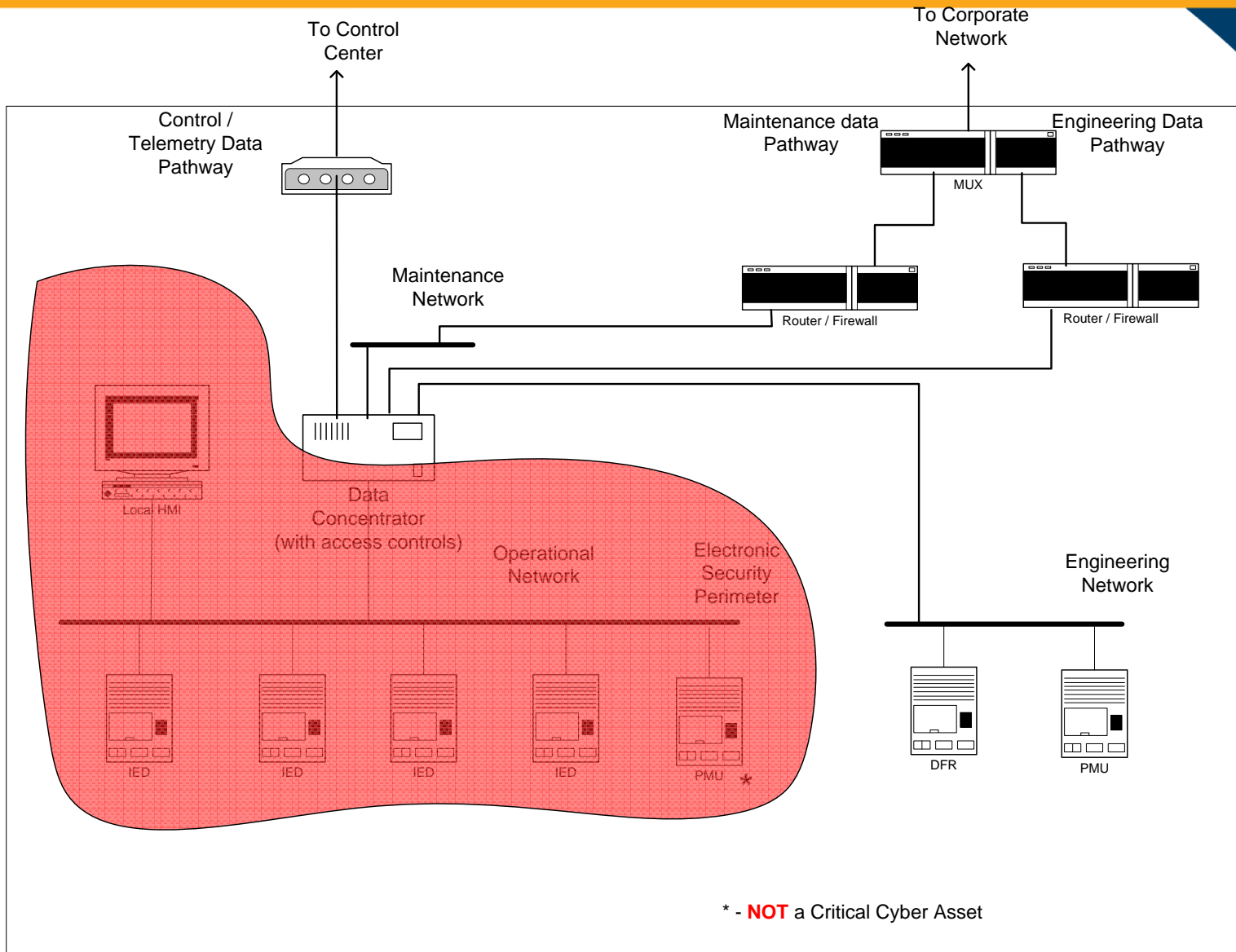
What should I consider doing?

- *Assume* that the SynchroPhasors will achieve their potential and entities *will designate them as Critical Cyber Assets* in the future
- Consider a business strategy to minimize future cost by treating them as Critical Cyber Assets when installing new SynchroPhasors
 - Even if there are no audits or other compliance actions associated with them at this time
- Analyze and plan for “upgrading” existing implementations to make them compliant with the CIP Standards to anticipate future need
 - Good business planning function

Examples: "Today"

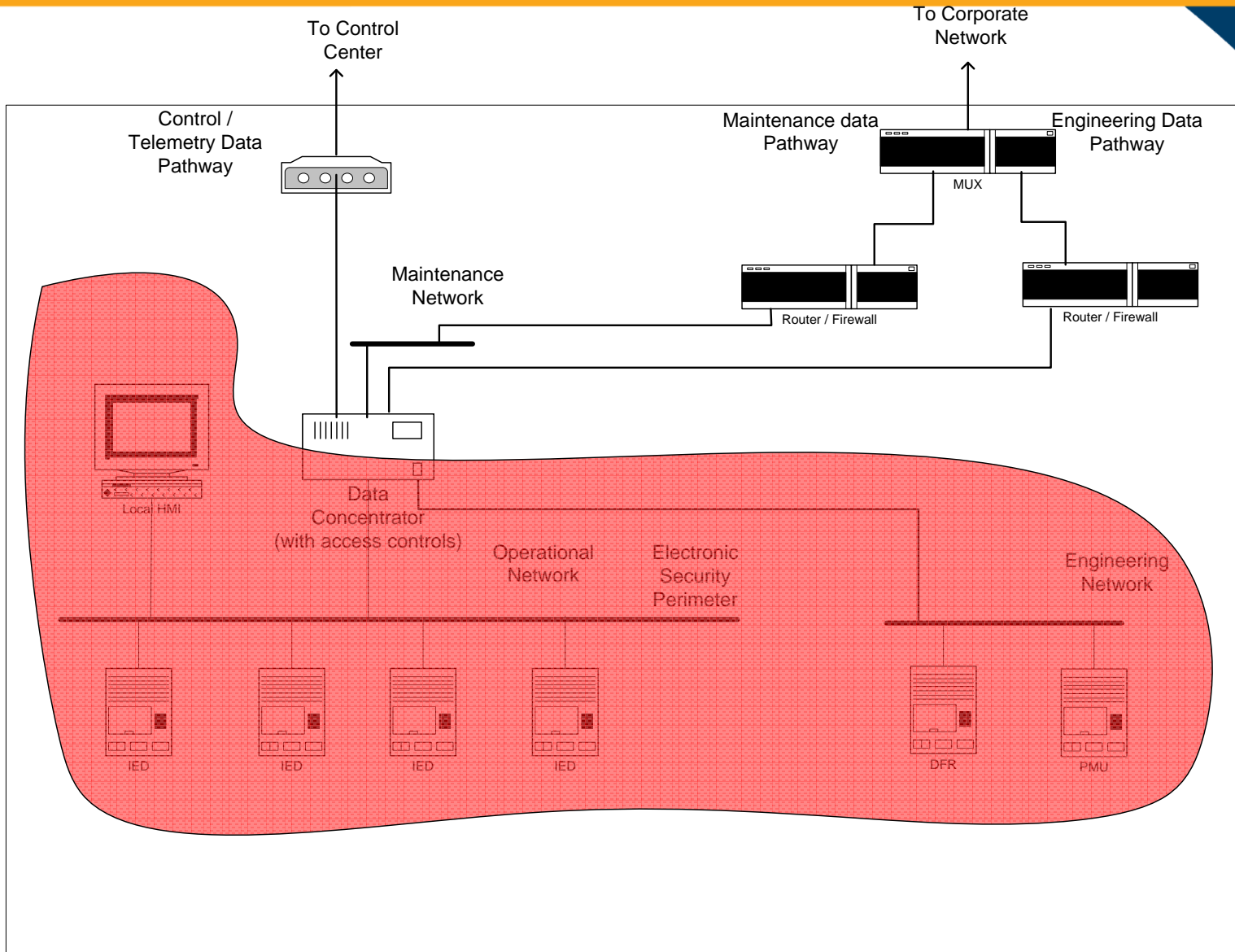


Examples: "Today"

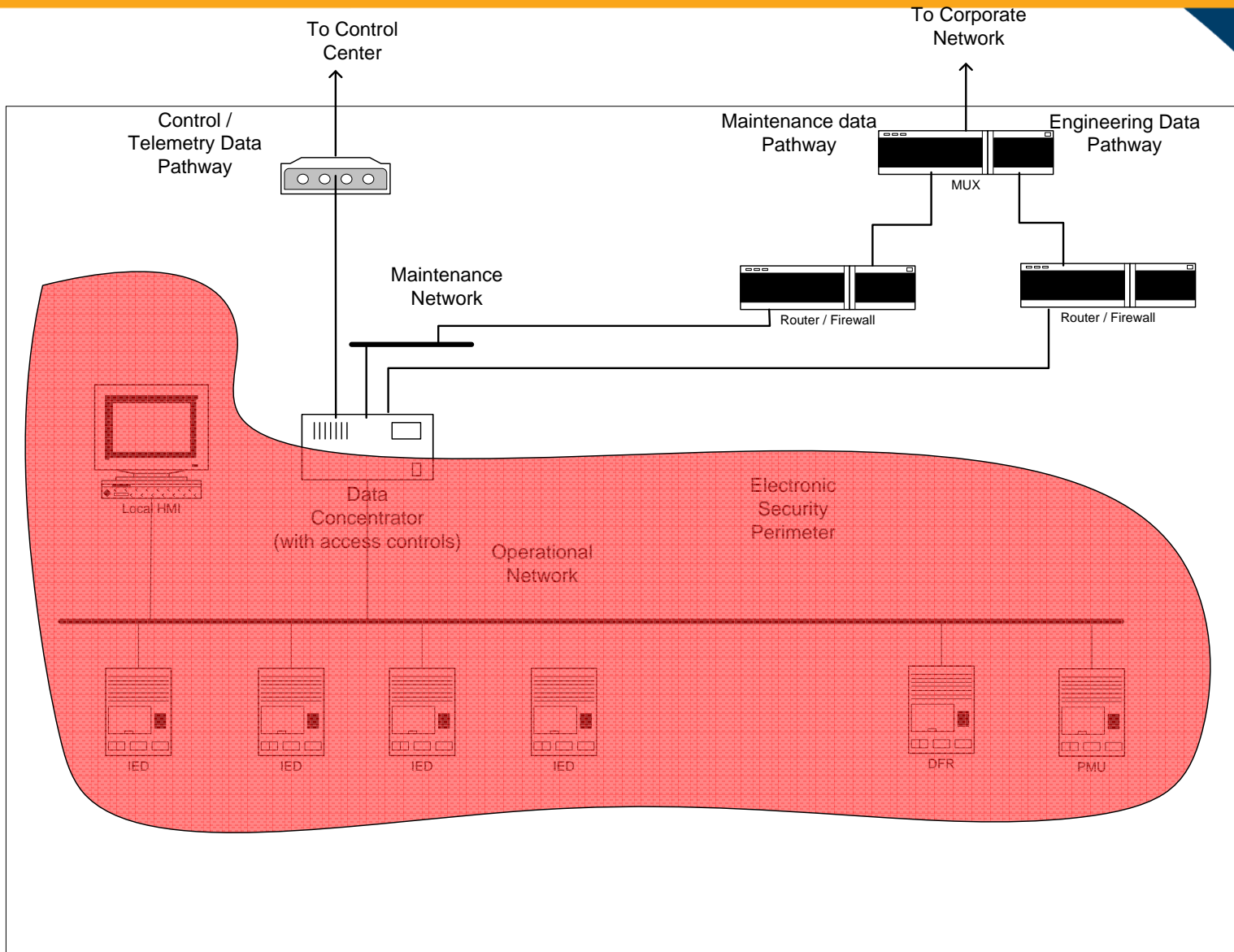


* - **NOT** a Critical Cyber Asset

Examples: "Good Practice"



Examples: "Future"



Examples: "Future Vision"

