LERC before you LEAP

2015 Webinar

December 10, 2015

Shon Austin
Lead Compliance Specialist

SPP Southwest Power Pool Regional Entity

Expectations

- Build on the following presentations:
  - CIP V5 Identifying BES Cyber Systems
  - SPP RE Low Impact BES Cyber Systems
- Provide a brief refresher of:
  - Requirements for Low Impact BES Cyber Systems
  - What is LERC?
  - What is LEAP?
- Explain how you must LERC before you LEAP
- Determine LERC and LEAP
- Implement LERC and LEAP
  - Overview of the “reference model” drawings

Refresher

- **Must** identify each asset that contains a Low Impact BES Cyber System
- **NO** requirement to provide an itemized list(s) of:
  - Low Impact BES Cyber Systems
  - Low Impact BES Cyber Assets

What is LERC?

Low Impact External Routable Connectivity (LERC) is defined in the NERC Glossary of Terms as:

Direct user-initiated interactive access or a direct device-to-device connection to a Low Impact BES Cyber System(s) from a Cyber Asset outside the asset containing those Low Impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing Low Impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).

What is LEAP?

Low Impact BES Cyber System Electronic Access Point (LEAP) is defined in the NERC Glossary of Terms as:

> A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

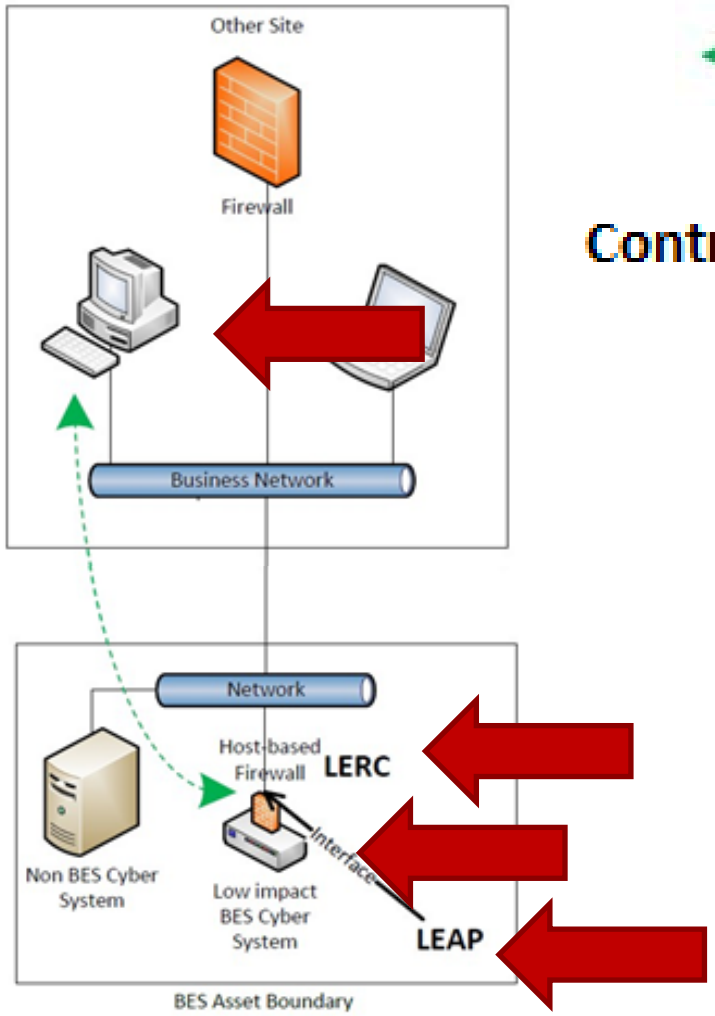
Requirements

- **Cyber Security Awareness**
  - "… reinforce, at least every 15 calendar months, cyber security practices…"
- **Cyber Security Incident Response**
  - "…Identify, classify, and response to Cyber Security Incidents…"
- **Physical Security Controls**
  - "…control physical access based on need…"
- **Electronic Access Controls**
  - "…permit only necessary inbound and outbound bi-directional routable protocol access…"
  - "…authentication for all Dial-up Connectivity…"

Determining LERC/LEAP

1. Are there any routable protocol communications in the network used to communication with assets containing Low Impact BES Cyber Systems?
2. Is the communication bi-directional?
3. Does the routable communication connect to the Low Impact BES Cyber Systems?
4. Are there “protocol breaks” between the Low Impact BES Cyber Systems and cyber assets communicating outside of the assets?

Applying LERC and LEAP concepts

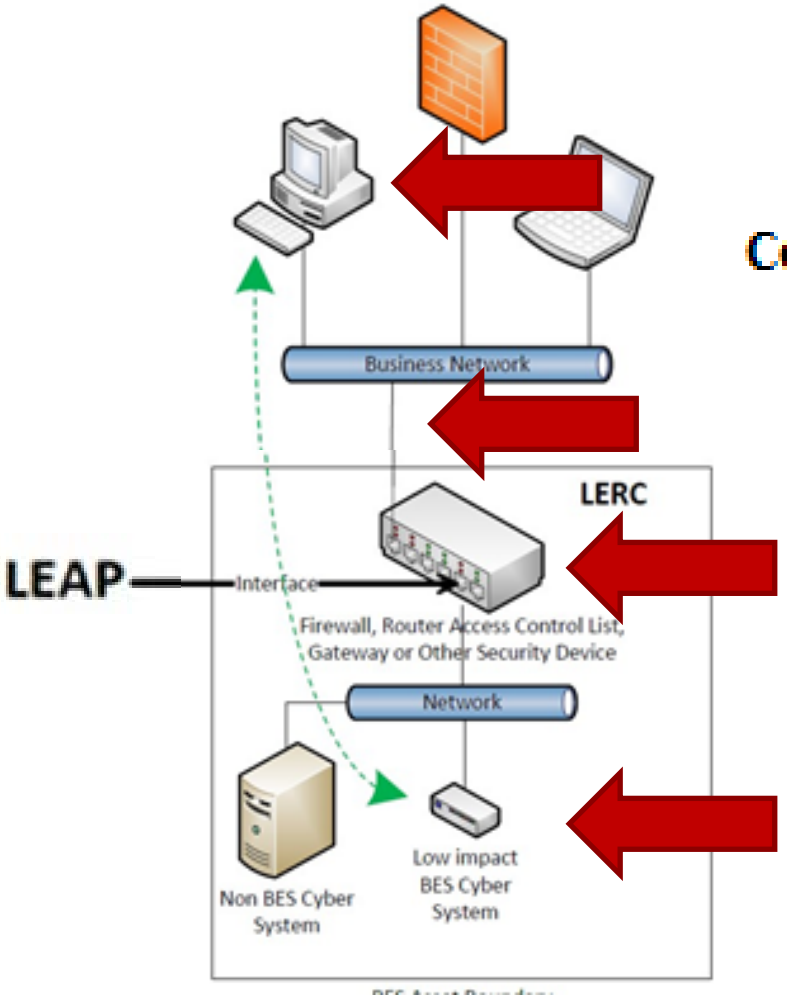


Data Flows

Control Center

Substation A

Applying LERC and LEAP concepts

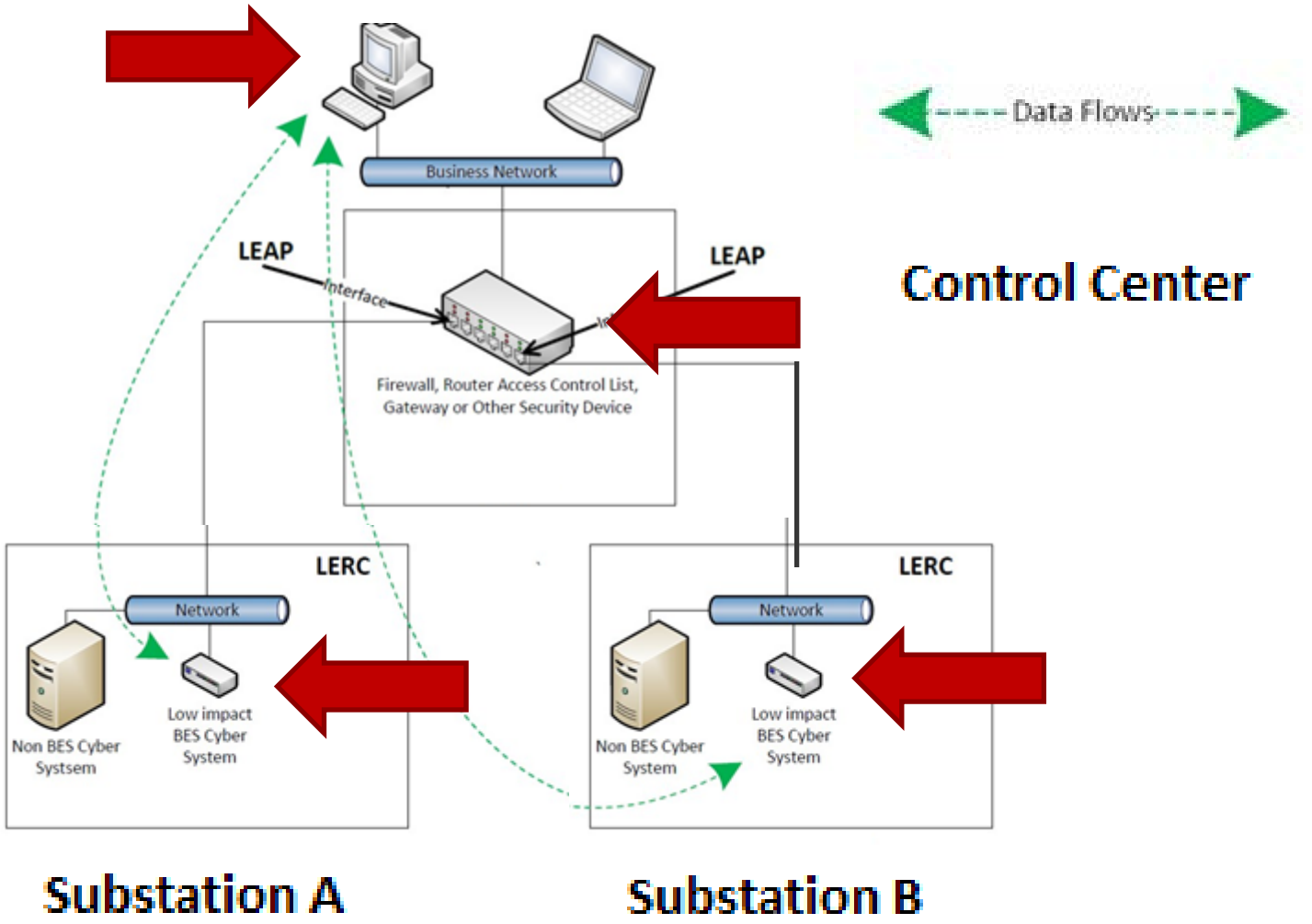


Data Flows

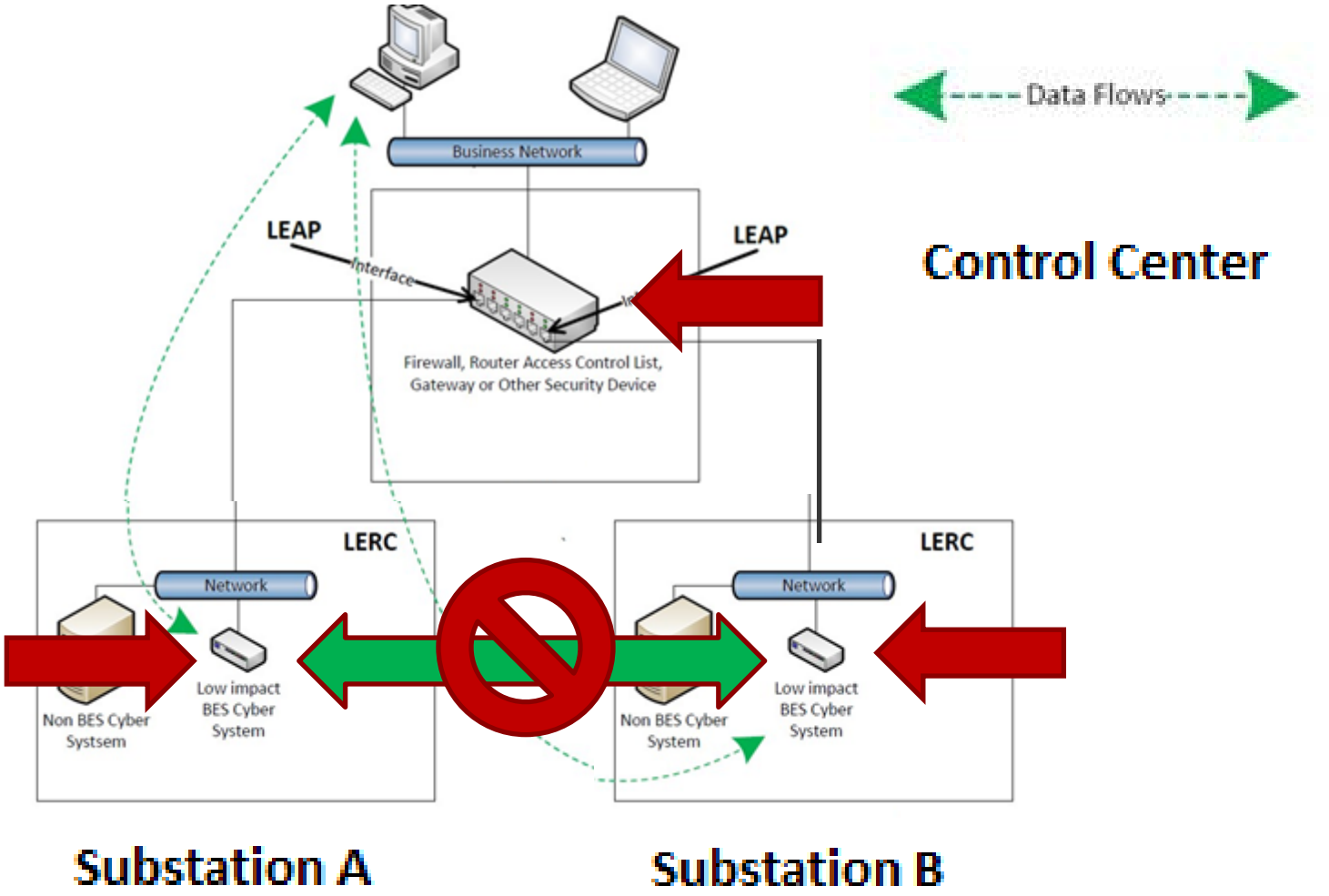
Control Center

Substation A

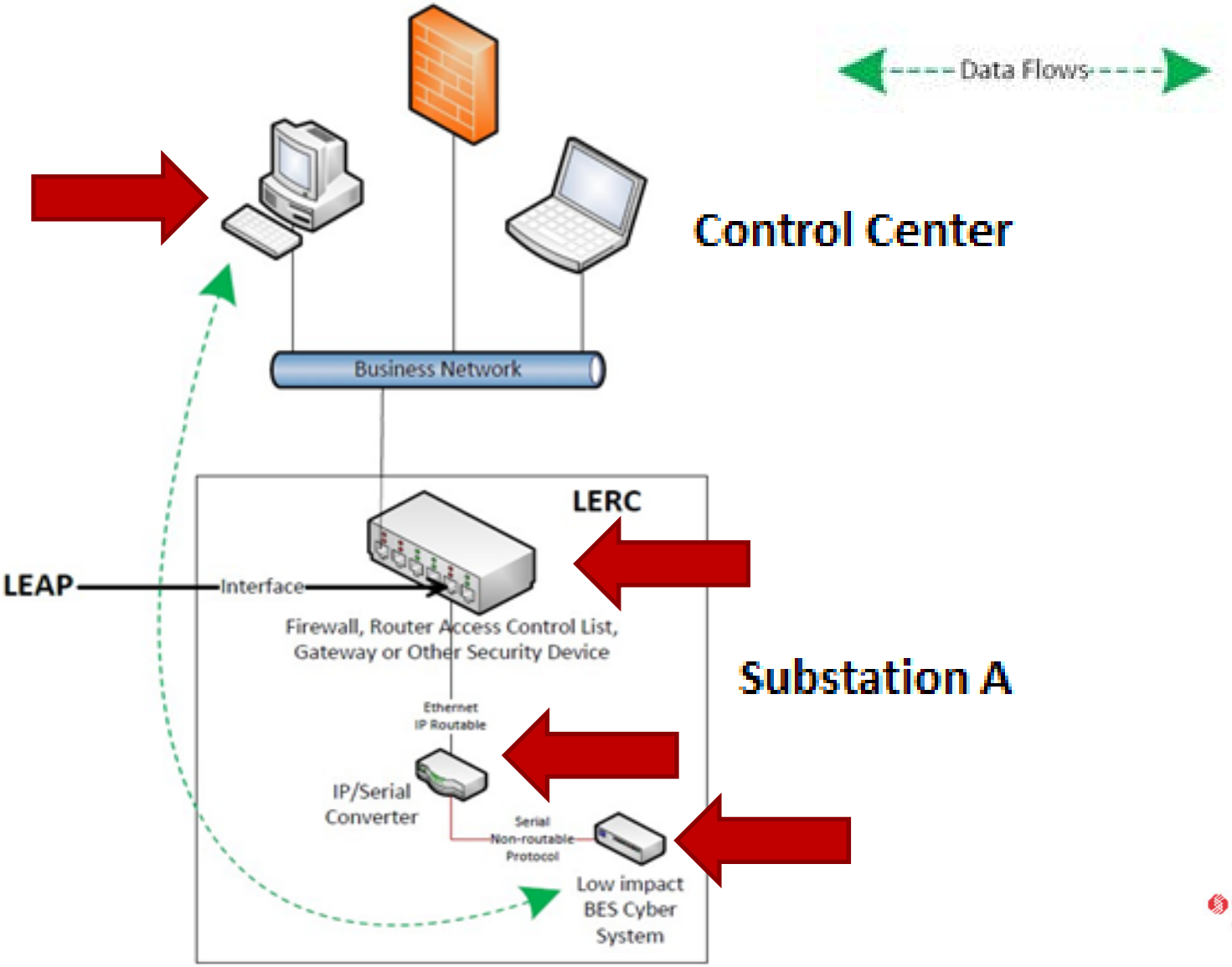
Applying LERC and LEAP concepts



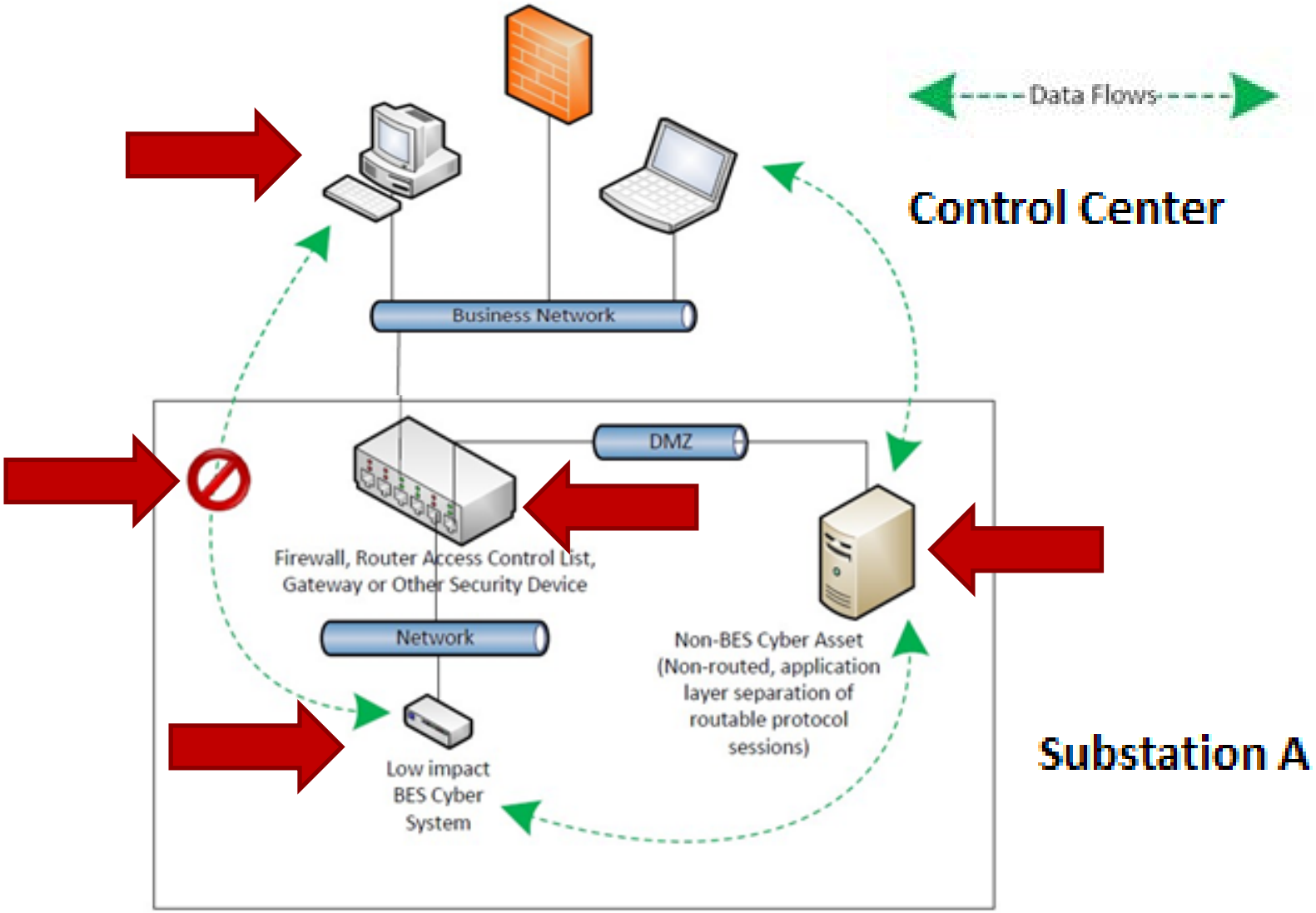
Applying LERC and LEAP concepts



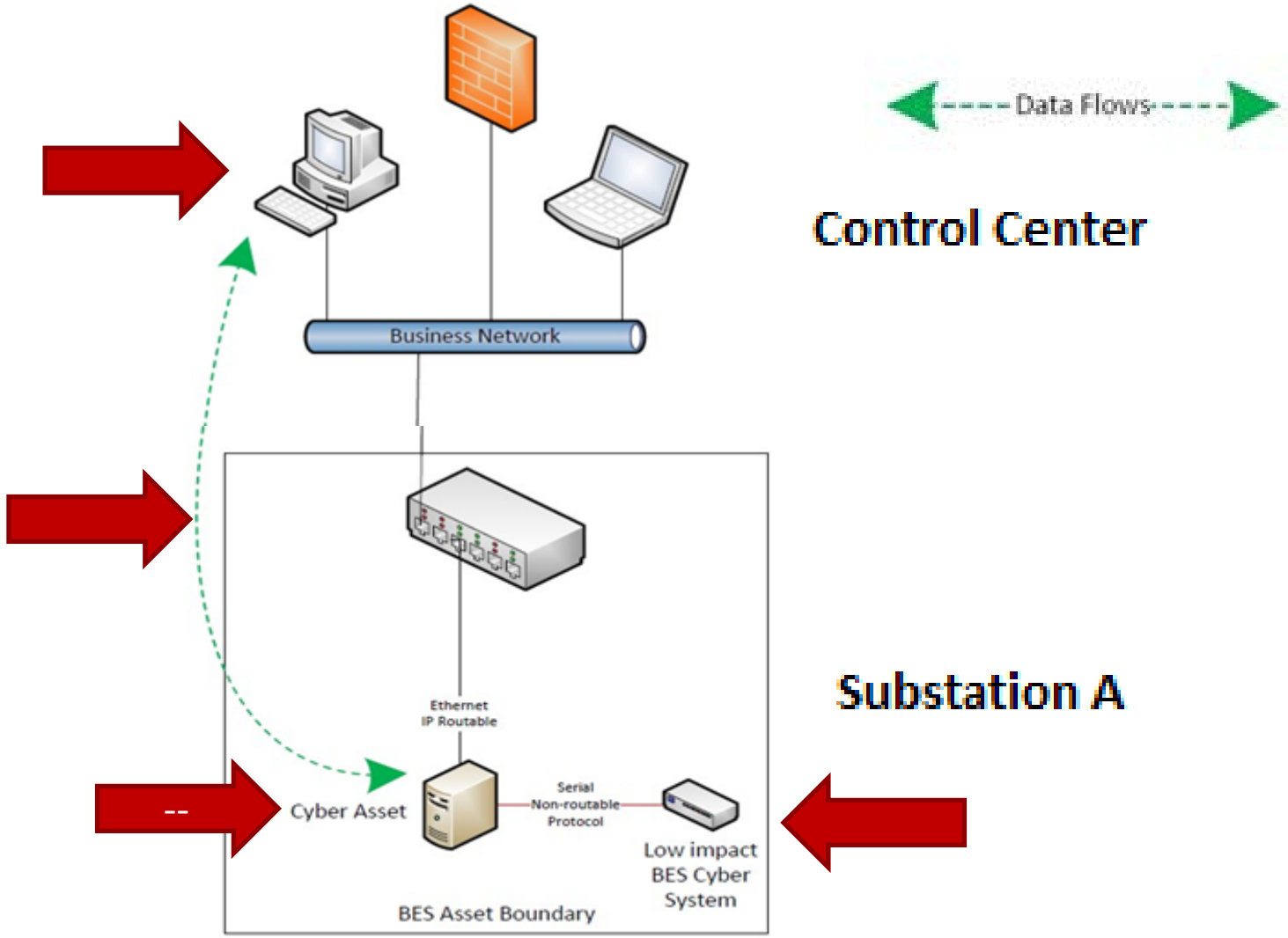
Applying LERC and LEAP concepts



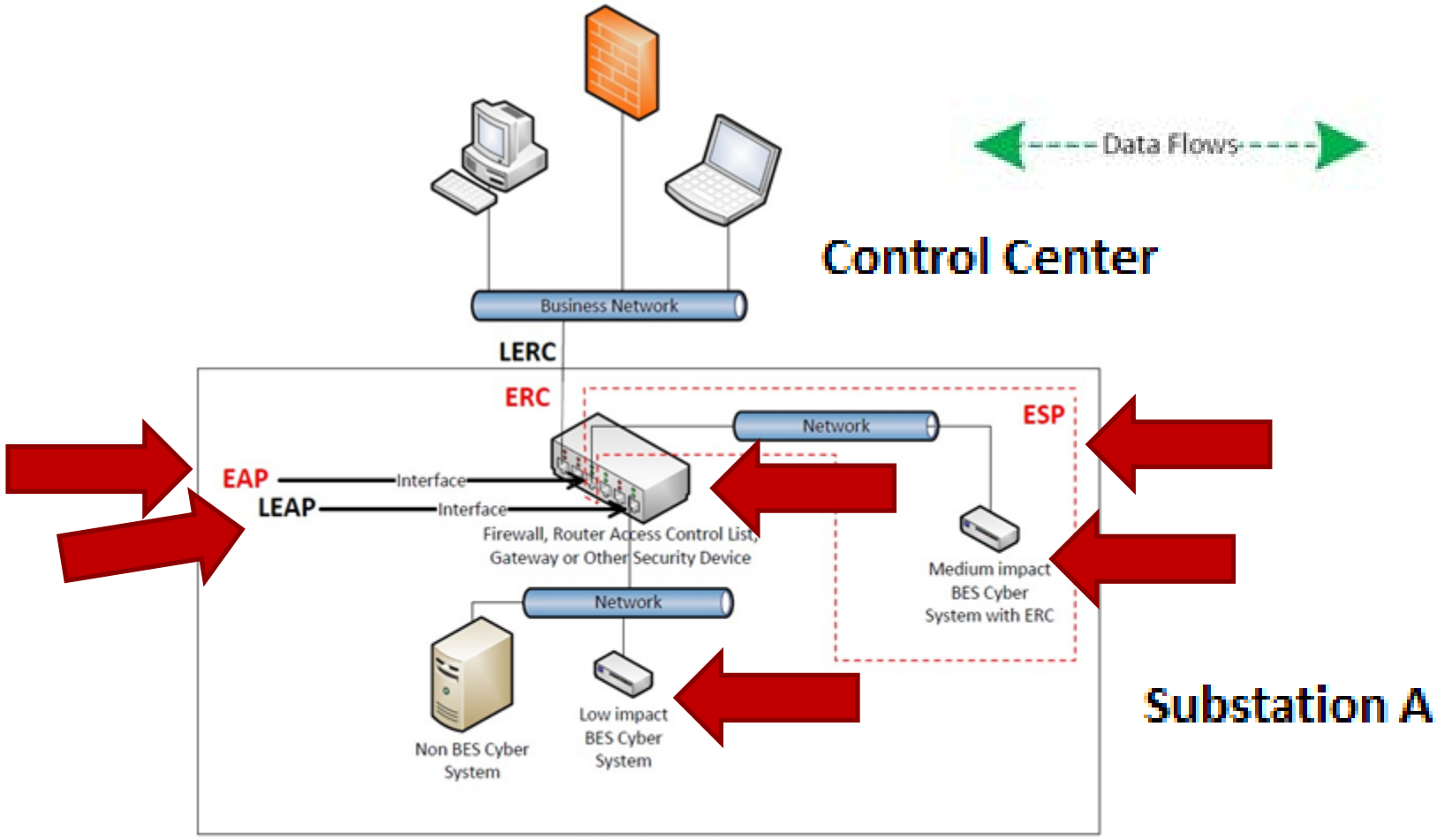
Applying LERC and LEAP concepts



Applying LERC and LEAP concepts



Applying LERC and LEAP concepts



Suggested Evidence

- Network diagrams/drawings/configurations
- Pictures/video tour of the asset (facility) with Low Impact BES Cyber Systems
- Dial-up Connectivity protections

References

- CIP-003-6 — Cyber Security — Security Management Controls
- https://vimeopro.com/sppcompliance/re/video/129885268
- https://vimeopro.com/sppcompliance/re/video/129885273

SPP RE CIP Team

- Kevin Perry, Director of Critical Infrastructure Protection
  (501) 614-3251
- Shon Austin, Lead Compliance Specialist-CIP
  (501) 614-3273
- Steven Keller, Lead Compliance Specialist-CIP
  (501) 688-1633
- Jeremy Withers, Senior Compliance Specialist-CIP
  (501) 688-1676
- Robert Vaughn, Compliance Specialist II-CIP
  (501) 482-2301
- Sushil Subedi, Compliance Specialist II-CIP
  (501) 482-2334