NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards: Version 5 Revisions for Low Impact BES Cyber Systems

i-PCGRID

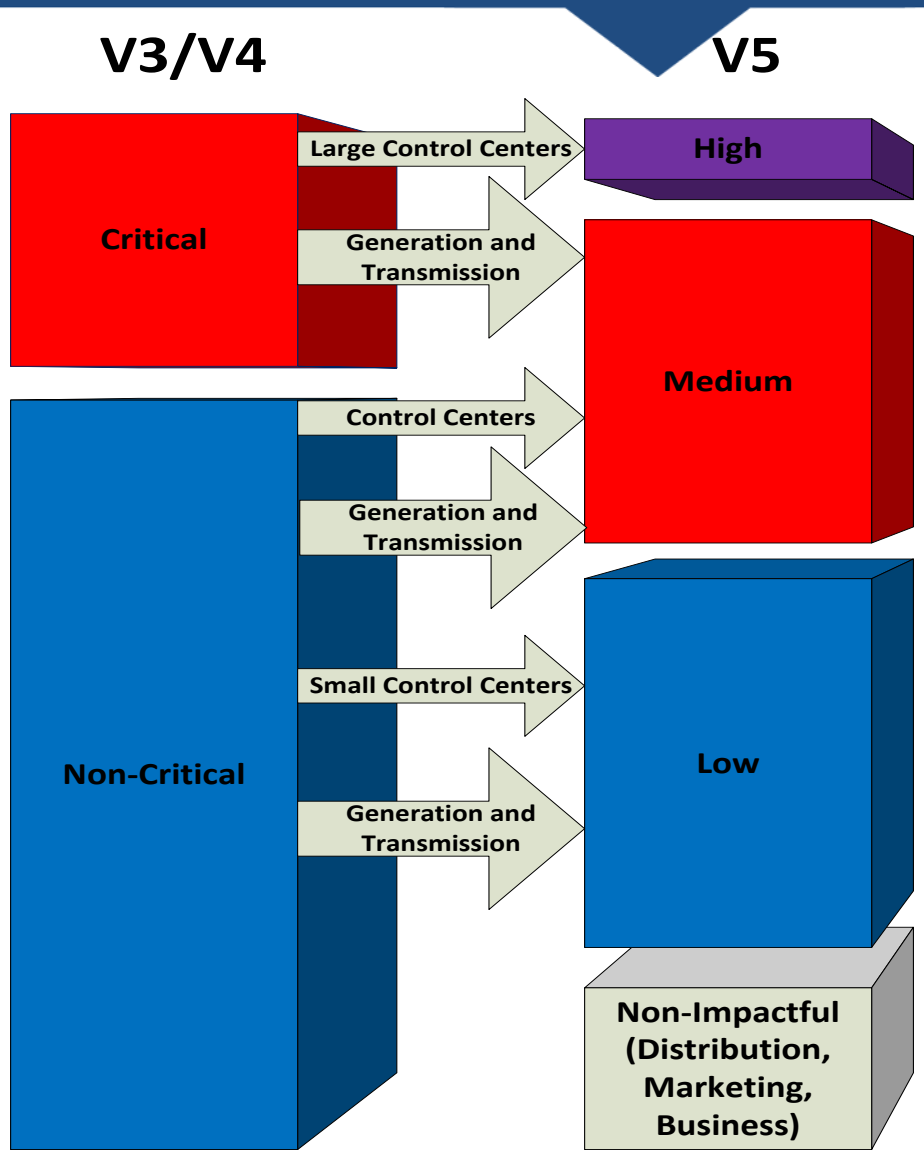
March 27, 2015

RELIABILITY | ACCOUNTABILITY




CIP Standards – Version 5

- High Impact
  - Large Control Centers
  - CIP-003 to 009 V3 "plus"
- Medium Impact
  - Generation and Transmission
  - Control Centers
  - Similar to CIP-003 to 009 V3
- All other BES Cyber Systems (Low Impact) must implement a policy to address:
  - Cybersecurity Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Incident Response



Low Impact BES Cyber Systems

- FERC concerned with lack of objective criteria for evaluating Low Impact protections
  - "Introduces unacceptable level of ambiguity and potential inconsistency into the compliance process"
  - Open to alternative approaches
  - "… the criteria NERC proposes for evaluating a responsible entities' protections for Low impact facilities should be clear, objective and commensurate with their impact on the system, and technically justified."
- No detailed inventory required … list of locations / Facilities OK

Low Impact BES Cyber Systems

- SDT maintained all low impact requirements in CIP-003
  - "Low-only entities" only need to comply with CIP-002 and CIP-003
- Added CIP-003 Part 1.2 dealing with security policy for low impact BES Cyber Systems
- Added Attachments dealing with the technical requirement and measures
  - Kept four original "areas"

Low Impact BES Cyber Systems

- Security Awareness
  - "… reinforce, at least every 15 calendar months, cyber security practices…"
- Incident Response
  - Modeled from medium impact
  - 5 elements (of 9: collapsed process requirements and update requirements together; no documentation of deviations or specific record retention – but still need to demonstrate compliance)
- Physical Security
  - "…control physical access based on need…"

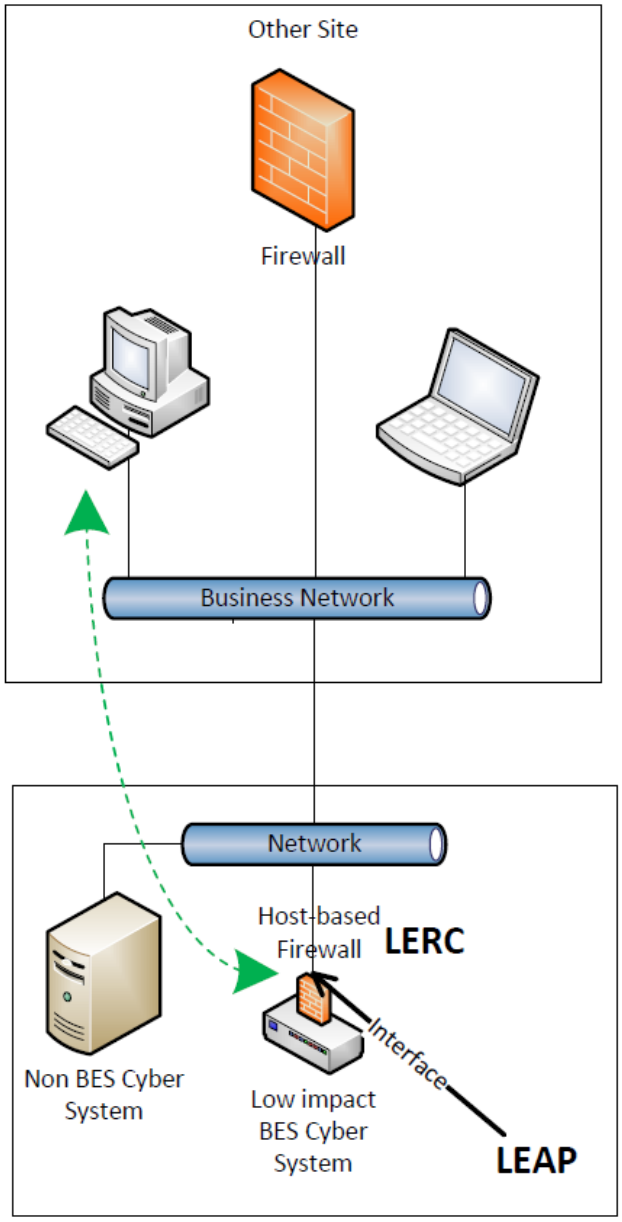
Low Impact BES Cyber Systems

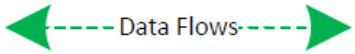
- Electronic Security
  - Two new definitions – LERC and LEAP
  - Similar to but different from ERC and EAP concepts at medium & high
- "…permit only necessary inbound and outbound bi-directional routable protocol access…"
- "…authentication for all Dial-up Connectivity…"
- Seven "reference model" drawings showing LERC & LEAP in Guidelines and Technical Basis section

Low Impact BES Cyber Systems

- **Low Impact External Routable Connectivity (LERC):** 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).
- **Low Impact BES Cyber System Electronic Access Point (LEAP):** 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.

Low Impact BES Cyber Systems

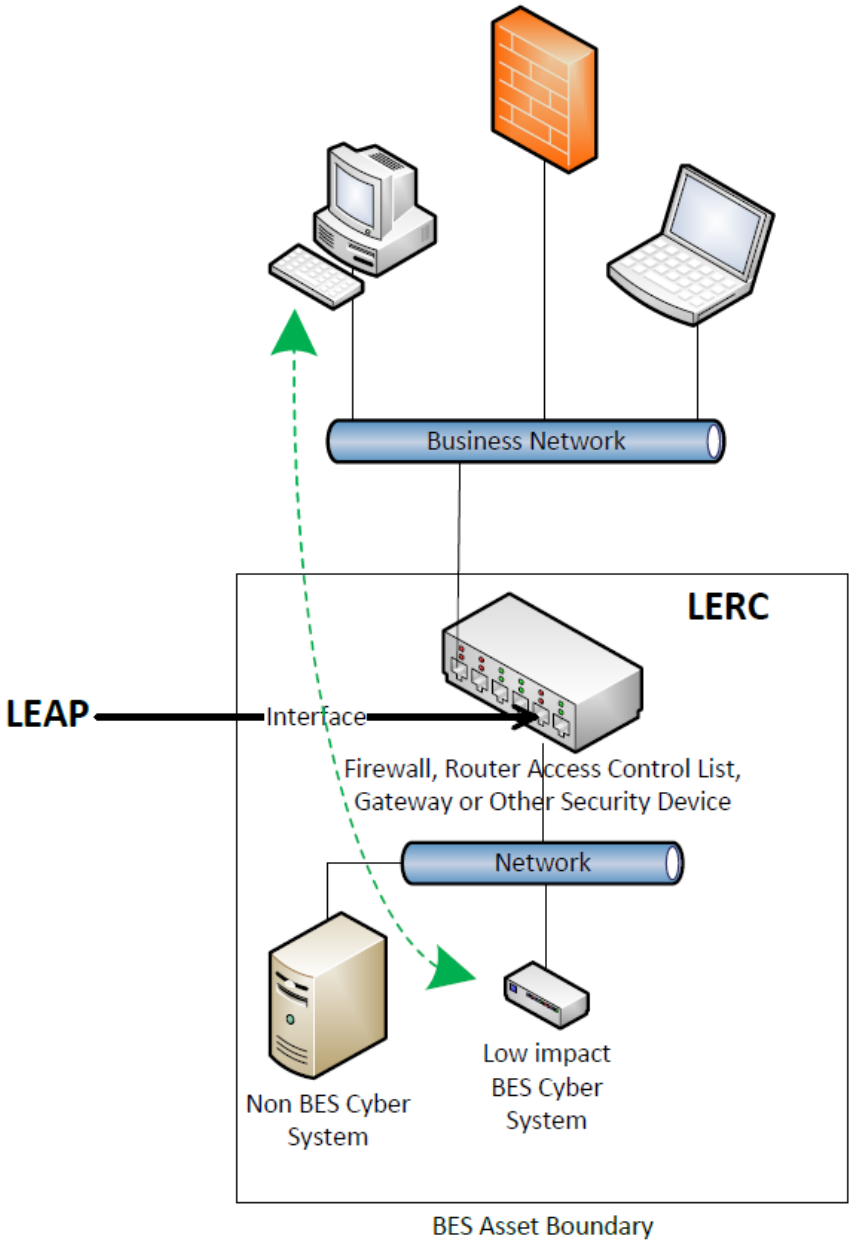




REFERENCE MODEL - 1

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A host-based firewall is configured on the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

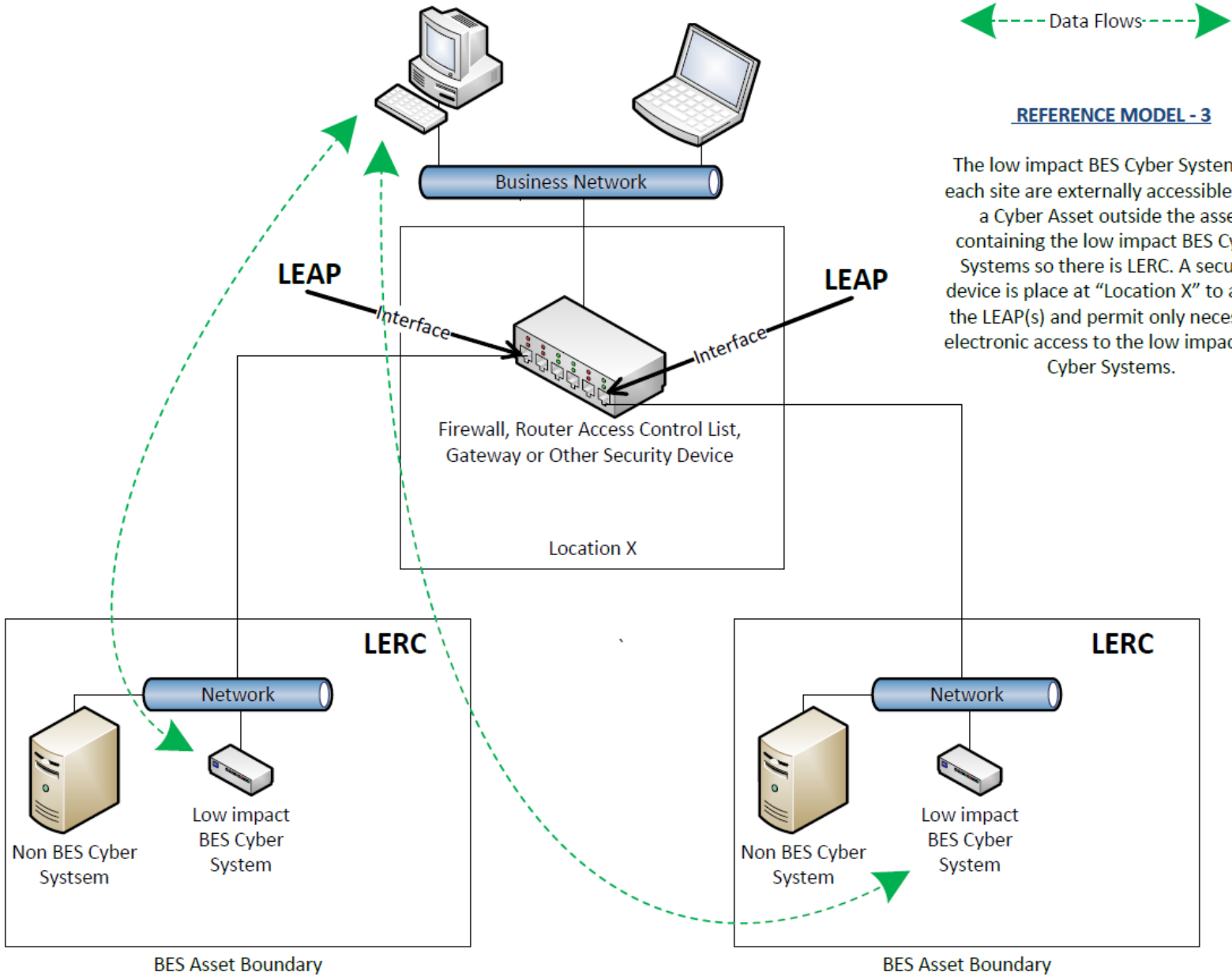
Low Impact BES Cyber Systems



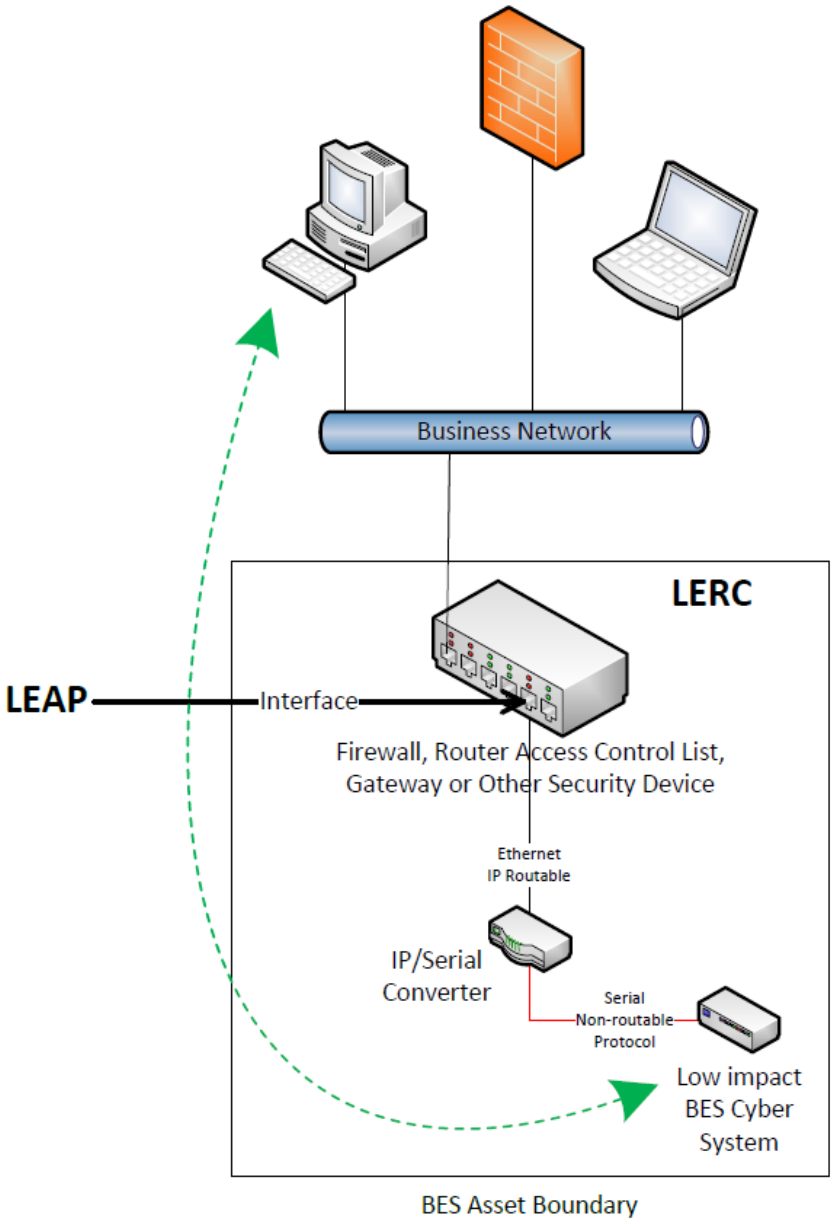
REFERENCE MODEL - 2

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System so there is LERC. A security device is placed between the business network and the low impact BES Cyber System to act as the LEAP and permit only necessary electronic access to the low impact BES Cyber System.

Low Impact BES Cyber Systems



Low Impact BES Cyber Systems

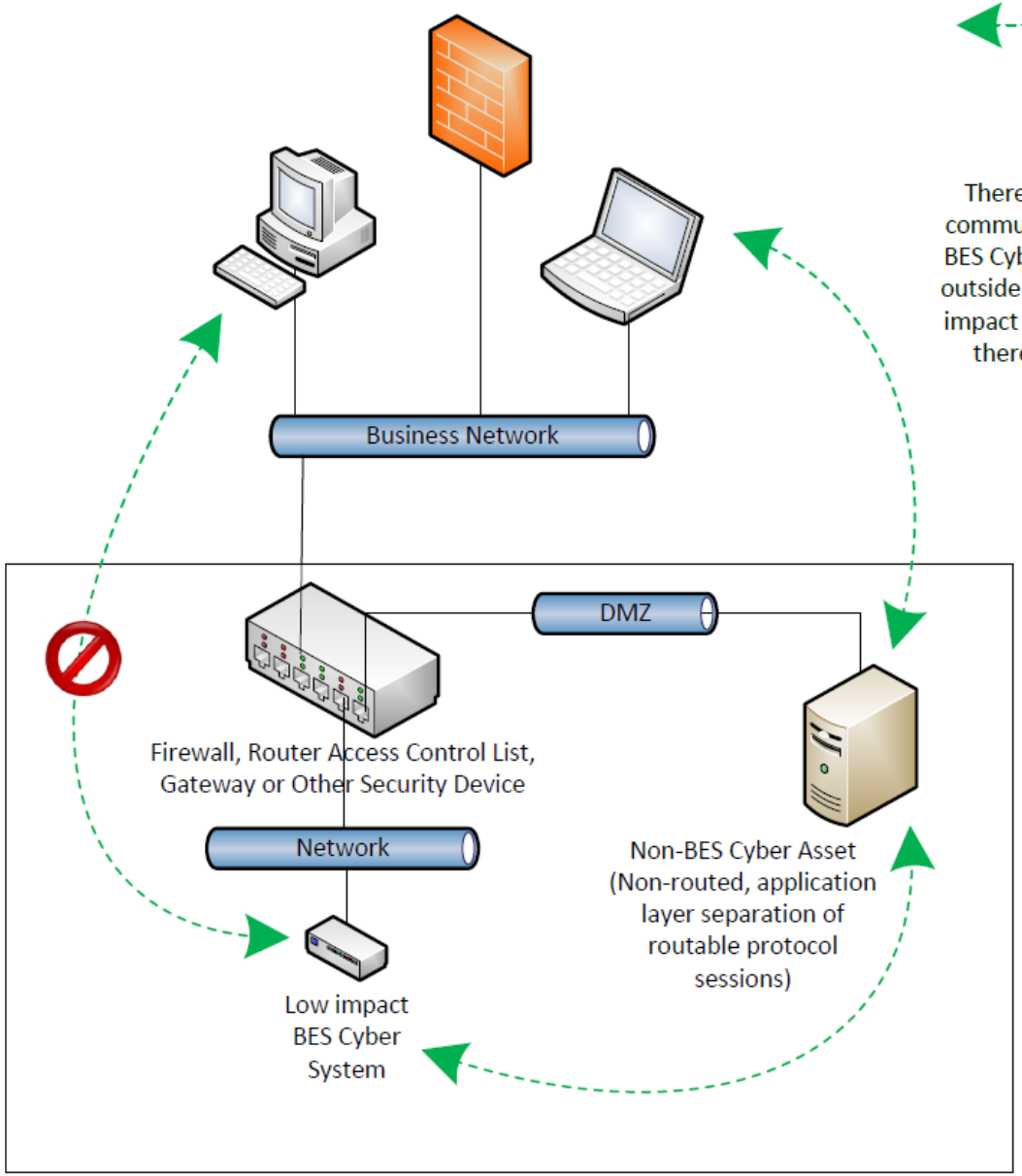


Data Flows

REFERENCE MODEL - 4

The low impact BES Cyber System is externally accessible from a Cyber Asset outside the asset containing the low impact BES Cyber System. There is LERC because the IP/Serial converter is extending the communication between the business network Cyber Asset and the low impact BES Cyber System is directly addressable from outside the asset. A security device is placed between the business network and the low impact BES Cyber System to permit only necessary electronic access to the low impact BES Cyber System.

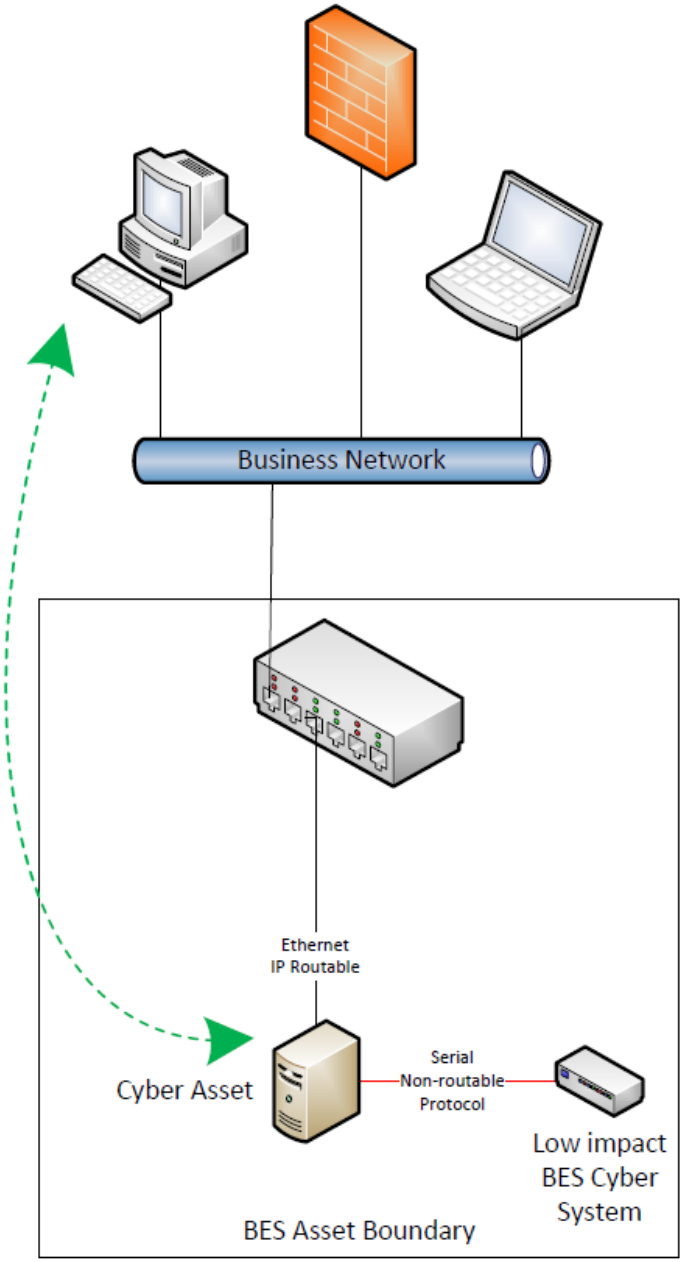
Low Impact BES Cyber Systems



REFERENCE MODEL - 5

There is no bi-directional routable communications between low impact BES Cyber System(s) and Cyber Assets outside the asset containing those low impact BES Cyber System(s) therefore there is no LERC in this example.

Low Impact BES Cyber Systems

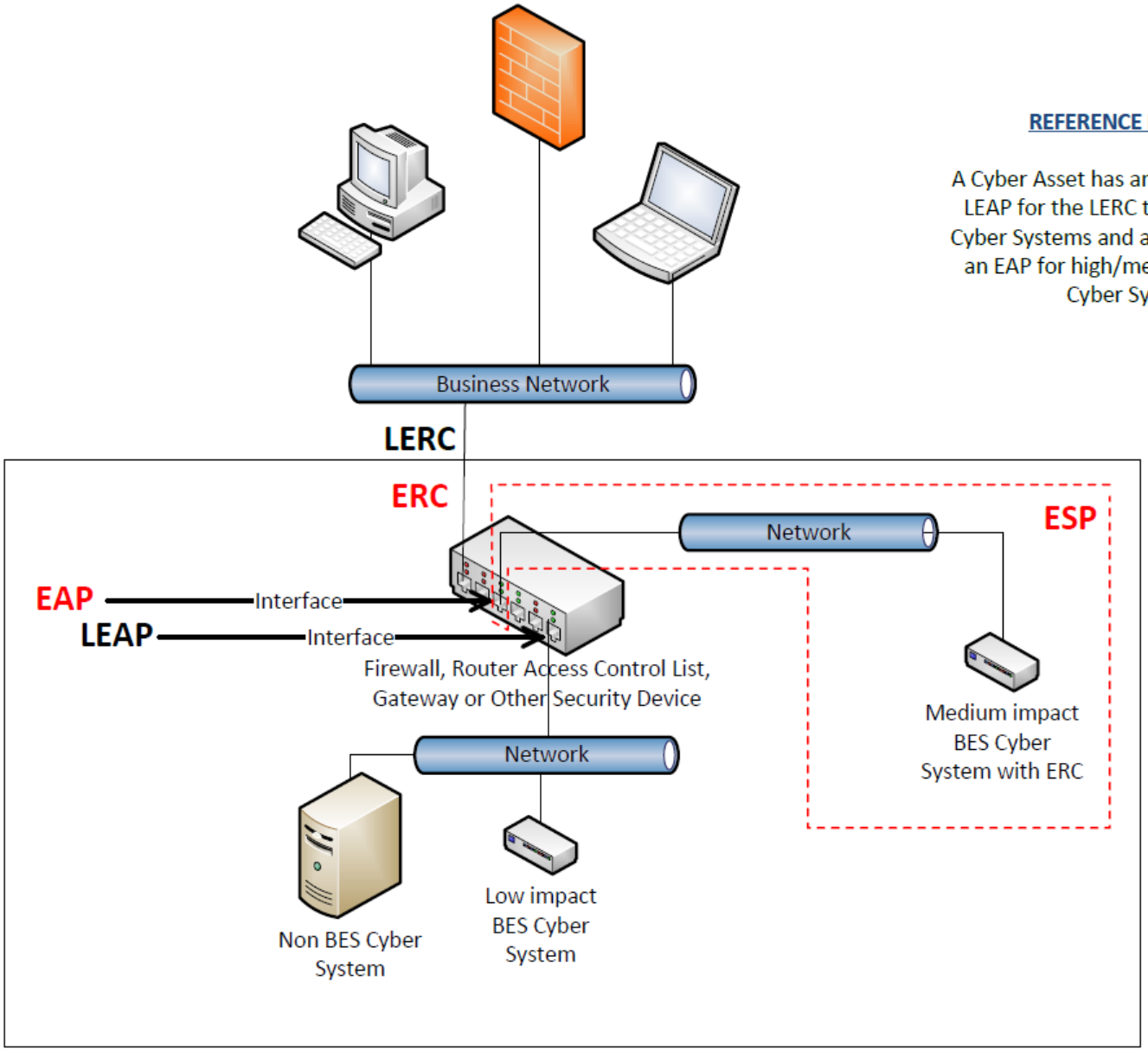


Data Flows

REFERENCE MODEL - 6

In this example, a Cyber Asset stops the direct access to the low impact BES Cyber System. There is a layer 7 application layer break or the Cyber Asset requires authentication and then establishes a new connection to the low impact BES Cyber System. There is no LERC in this example.

Low Impact BES Cyber Systems



REFERENCE MODEL - 7

A Cyber Asset has an interface that is a LEAP for the LERC to low impact BES Cyber Systems and another interface is an EAP for high/medium impact BES Cyber Systems.

Implementation Plan

- Phased implementation plan:
  - IAC – no change (4/1/16)
  - Communication Networks – 9 months after the effective date of the standard
  - Transient Devices – 9 months after the effective date of the standard
  - Low Impact
    - Latter of 4/1/17 or 9 months after the effective date of the standard for policy, plan, security awareness, and response
    - Latter of 9/1/18 or 9 months after the effective date of the standard for physical and electronic security

Current Status

- NERC Board approved responses to IAC and Communication Networks directives on November 13, 2014
- NERC Board approved responses to Low Impact and Transient Device directives on February 12, 2015
  - Board action adjusted version numbers to -6 and -3
- All four directive areas filed with FERC on February 13, 2015 (10-day extension granted due to scheduled NERC board meeting)
- FERC must go through its approval process

CIP Standards – "Version 5"

- CIP-002-5.1*: BES Cyber Asset and BES Cyber System Categorization
- CIP-003-6**: Security Management Controls
- CIP-004-6**: Personnel and Training
- CIP-005-5: Electronic Security Perimeter(s)
- CIP-006-6: Physical Security of BES Cyber Systems
- CIP-007-6**: Systems Security Management
- CIP-008-5: Incident Reporting and Response Planning
- CIP-009-6: Recovery Plans for BES Cyber Assets and Systems
- CIP-010-2***: Configuration Management and Vulnerability Assessments
- CIP-011-2***: Information Protection

* - Changed "Devices" to "Systems" in background section

** - Developed as version 7 *** - Developed as version 3

References

- Project 2014-02 Development History:
- CIP Version 5 Revisions page:
  - http://www.nerc.com/pa/Stand/Pages/Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx
- CIP Version 5 Transition page:
  - http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions

Scott Mix, CISSP
Senior CIP Technical Manager
scott.mix@nerc.net
215-853-8204

RELIABILITY | ACCOUNTABILITY