NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP V5 TAG Modifications ERC and IRA

Project 2016-02 CIP Modifications SDT
May 7, 2020

RELIABILITY | ACCOUNTABILITY




NERC Antitrust Guidelines

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers, or any other activity that unreasonably restrains competition.

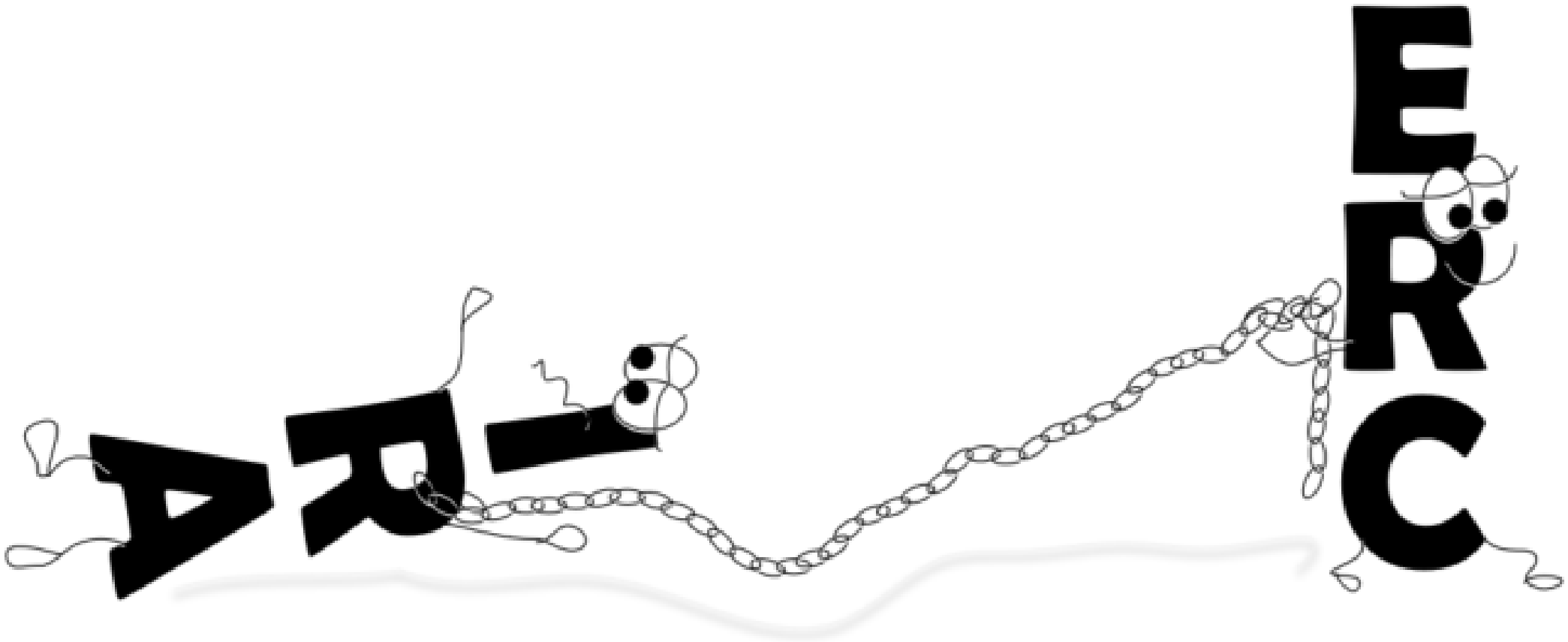
V5TAG identified issue

Project 2016-02 Standards Authorization Request (SAR) includes:

Network and Externally Accessible Devices – **V5TAG** recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) including:

- The meaning of the word ‘associated’ in the ERC definition.
- The IRA definition placement of the phrase “using a routable protocol” in the definition

V5TAG identified issue



V5TAG identified issue

ESP *- The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.*

ERC *- The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*

IRA *- User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.*

V5TAG identified issue

Compliance technicality:

A non-routable BCA **cannot** have **ERC** or **IRA!**

But…

Actual capability: we can “interactively” control with these BCAs “remotely.”

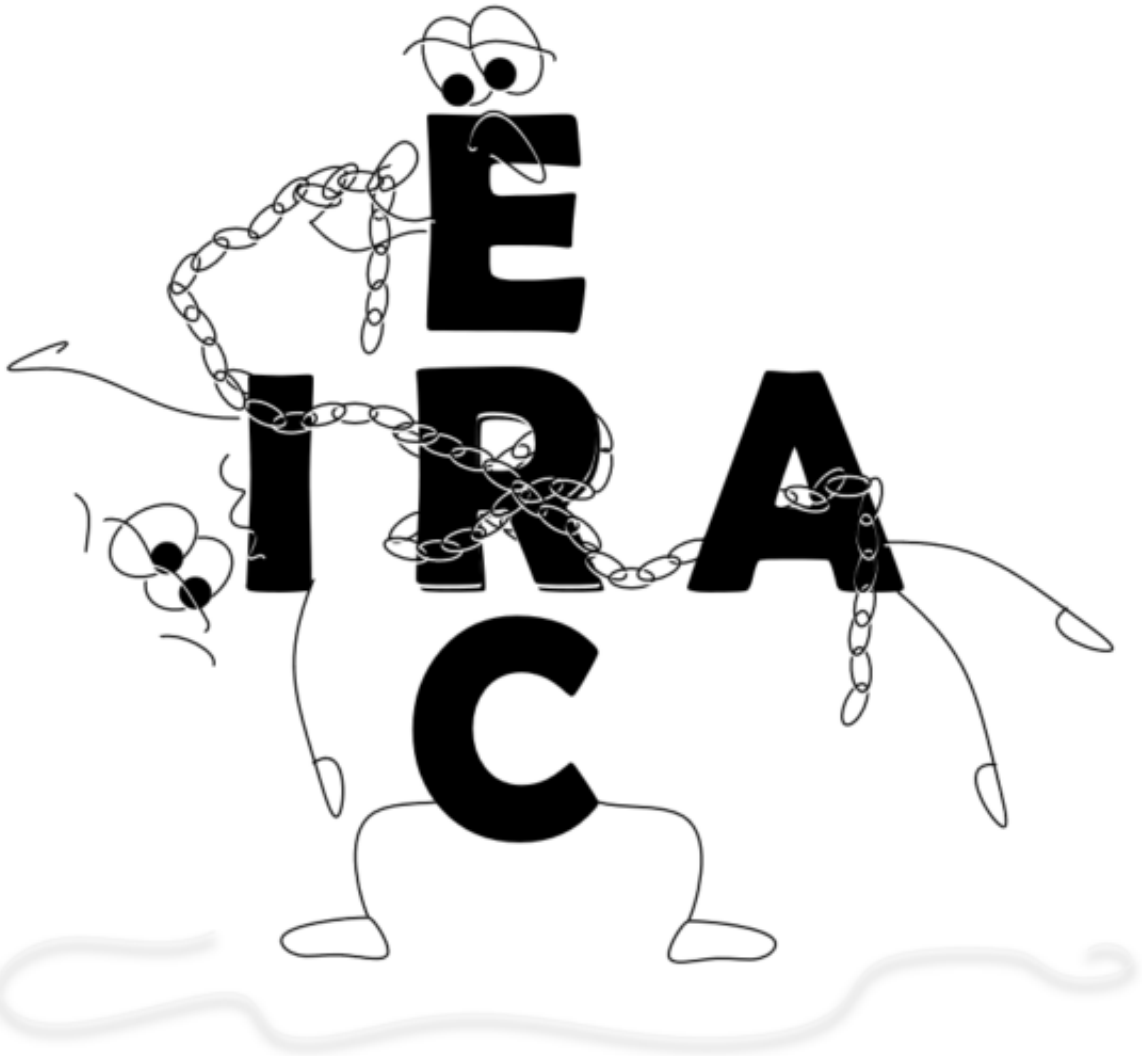
This creates a **Security Gap**, where interactive remote access (lowercase) has no required controls.

Objective

Safe, secure, resilient, and reliable operation of the Bulk Electric System…

Secure cyber systems to keep
the ill-intended from doing intentional harm
and the well-intended from screwing up,
whether a routable protocol is at play or not.

V5TAG identified issue



ERC ≠ IRA

External Routable Connectivity (ERC) and Interactive Remote Access (IRA)

External Routable Connectivity (ERC) is used in the CIP standards for different purposes, including:

1. Establishing when EAPs are required
2. Limiting scope of ~38 requirement parts to those locations that have a high enough level of remote connectivity to support the requirement

Proposed Solution

Compliance technicality:

- Make IRA all about the human access and use.
- Leave ERC alone and continue to use as a scoping mechanism in the Applicable Systems column for clarity on machine to machine security controls.

Actual capability: Come to industry agreement that we can “interactively” control these BCAs “remotely” and we should fix the IRA definition.

Security Risk: Mitigate the risk of unauthorized remote access by applying IRA protections to interactive routable and non-routable connections to BES Cyber Systems.

Immediate Benefits

Recognition within the Requirement language and Applicable Systems that ERC ≠ IRA results in:

- Reduced confusion of any implied overlap between the terms by un-nesting them
- Ultimate clarity that ERC and IRA are independent, serve different purposes, and have discrete security and compliance requirements
- Alignment of these terms with the reliability and security objectives of the CIP Standards

Objective

Interactive Remote Access (IRA)

User-initiated access by a person employing a remote access client.

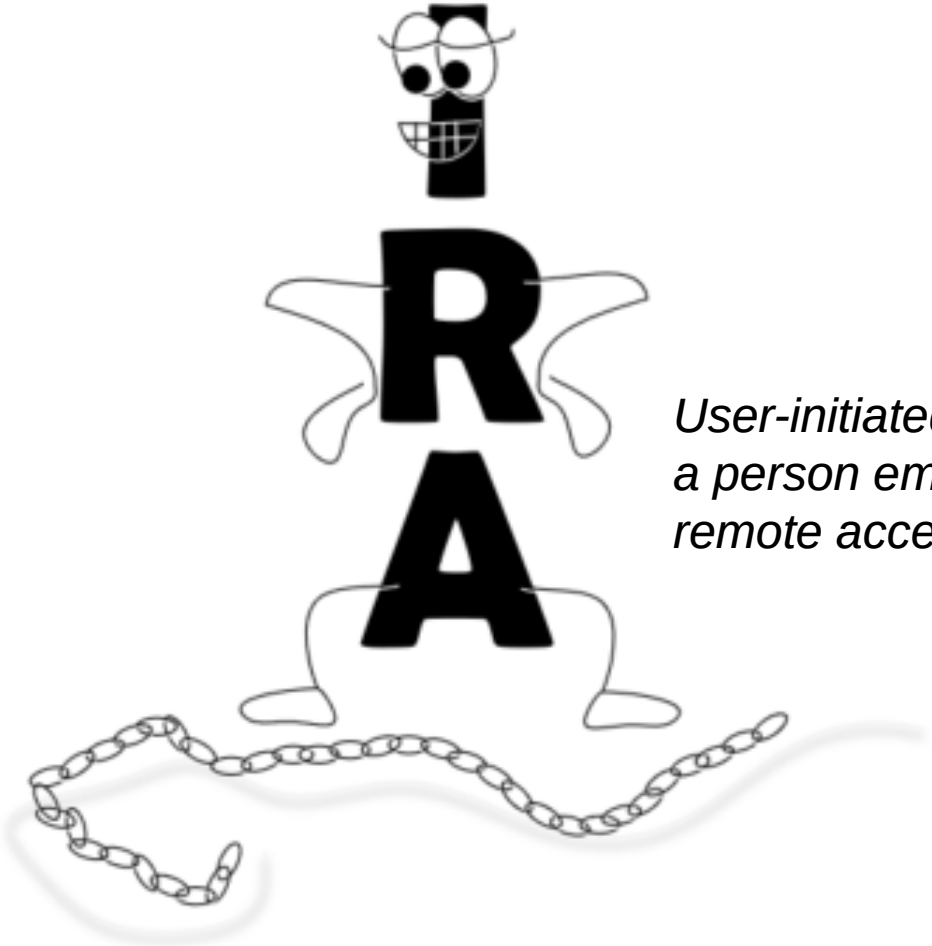
The SDT has kept ERC with conforming changes in order to not disrupt its scoping function.

The modified IRA definition becomes a simple glossary definition that:

- Removes embedded requirements and scoping mechanisms that were within it, and moves them to CIP-005 R2.
- References to ownership of the remote client become immaterial to the definition and CIP-005 requirements.
- The reliance on “using a routable protocol” has been removed

V5TAG issue SOLVED!

The ability to access a BES Cyber System from a Cyber Asset or Virtual Cyber Asset through a system controlling communications to and from the BES Cyber System via a bi-directional routable protocol connection.



User-initiated access by a person employing a remote access client.

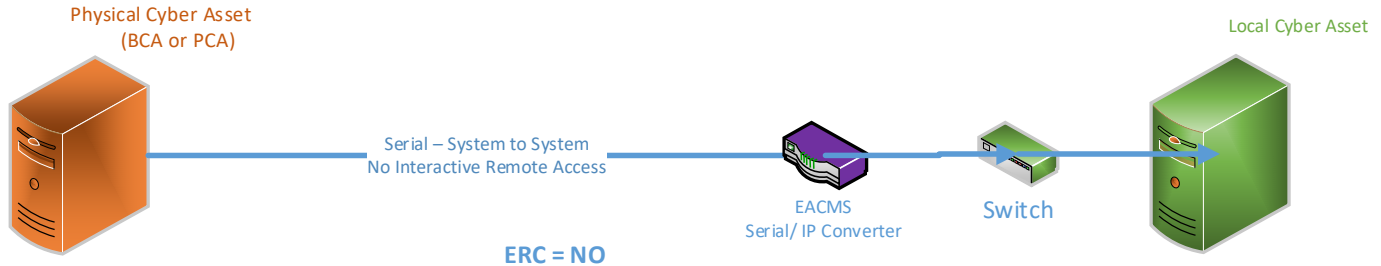
Objective

The following diagrams show different scenarios and whether ERC and/or IRA exist in the situation.

- Local Serial Data
- Remote Serial Data with IP Conversion
- Remote Serial Access
- Remote Routable Data
- Remote Serial Data
- Remote Serial Access from Another BCS
- Diode
- Remote Routable Access

Use Case #1

Serial Example 1 – Local Serial Data



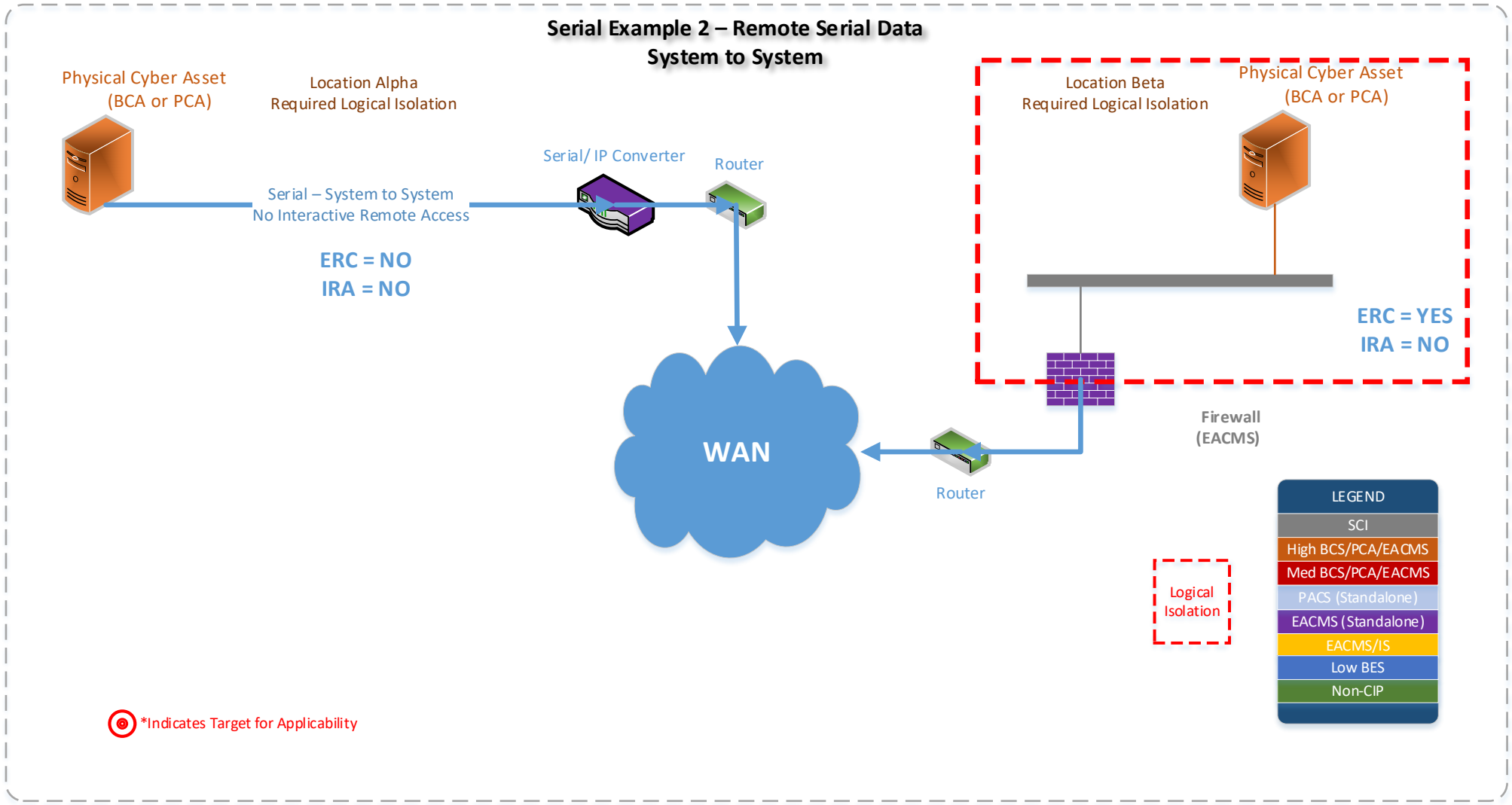
ERC = NO
IRA = NO

Logical Isolation

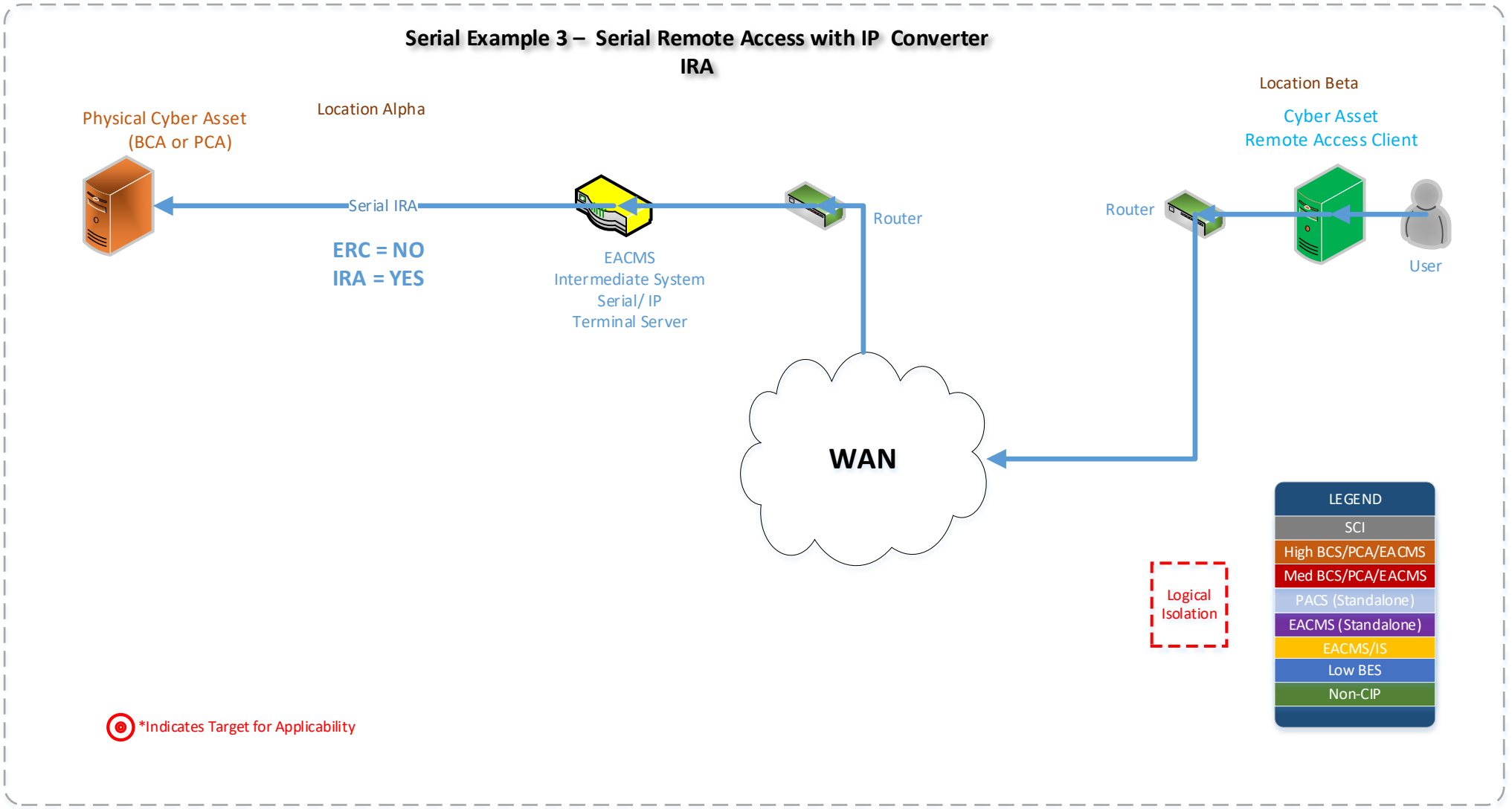
LEGEND
- SCI
- High BCS/PCA/EACMS
- Med BCS/PCA/EACMS
- PACS (Standalone)
- EACMS (Standalone)
- EACMS/IS
- Low BES
- Non-CIP

*Indicates Target for Applicability

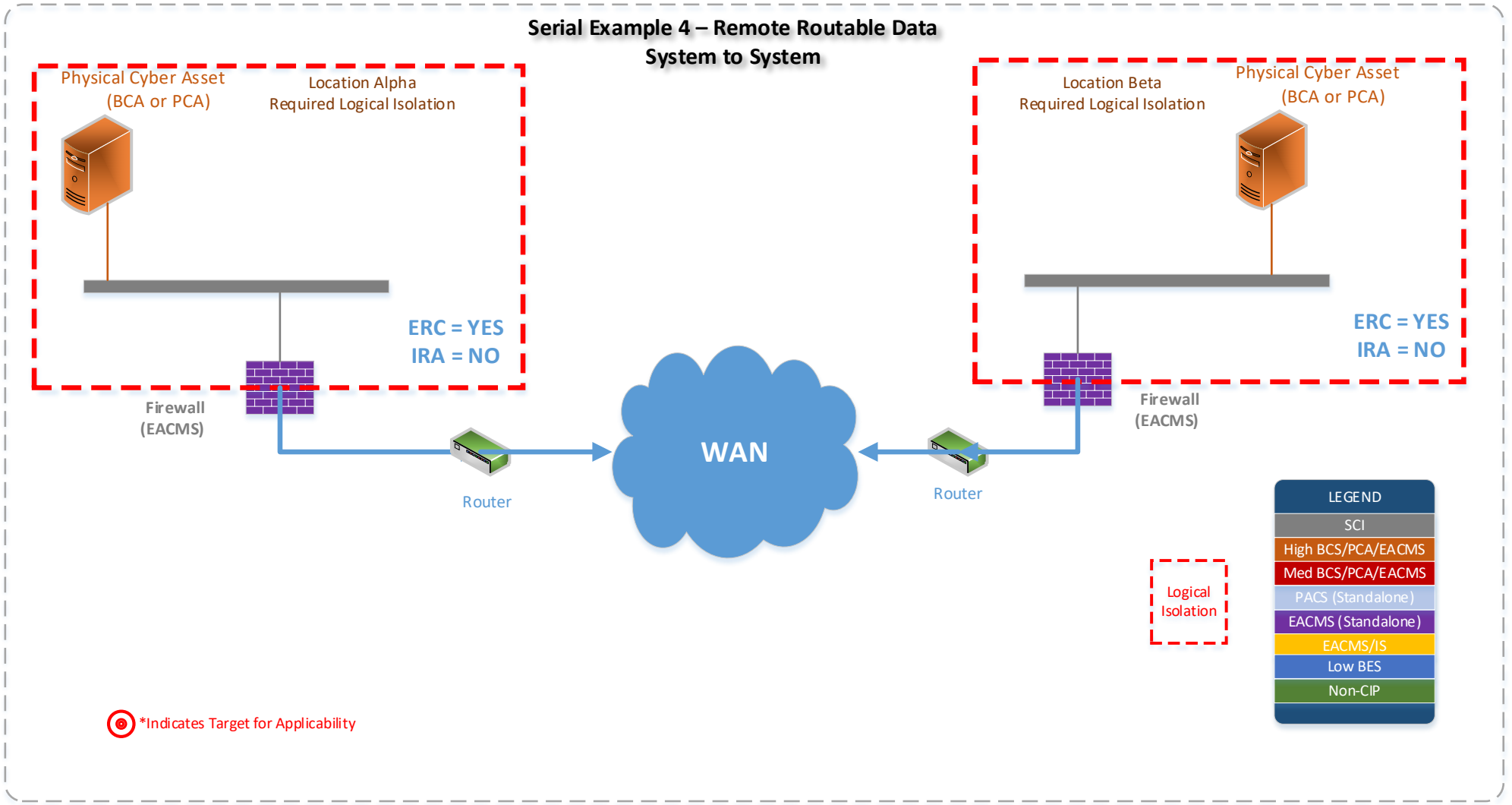
Use Case #2


Serial Example 2 – Remote Serial Data System to System
Physical Cyber Asset (BCA or PCA)
Location Alpha
Required Logical Isolation
Serial/ IP Converter
Router
Serial – System to System
No Interactive Remote Access
ERC = NO
IRA = NO
Location Beta
Required Logical Isolation
Physical Cyber Asset (BCA or PCA)
ERC = YES
IRA = NO
Firewall (EACMS)
WAN
Router
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
Logical Isolation
*Indicates Target for Applicability

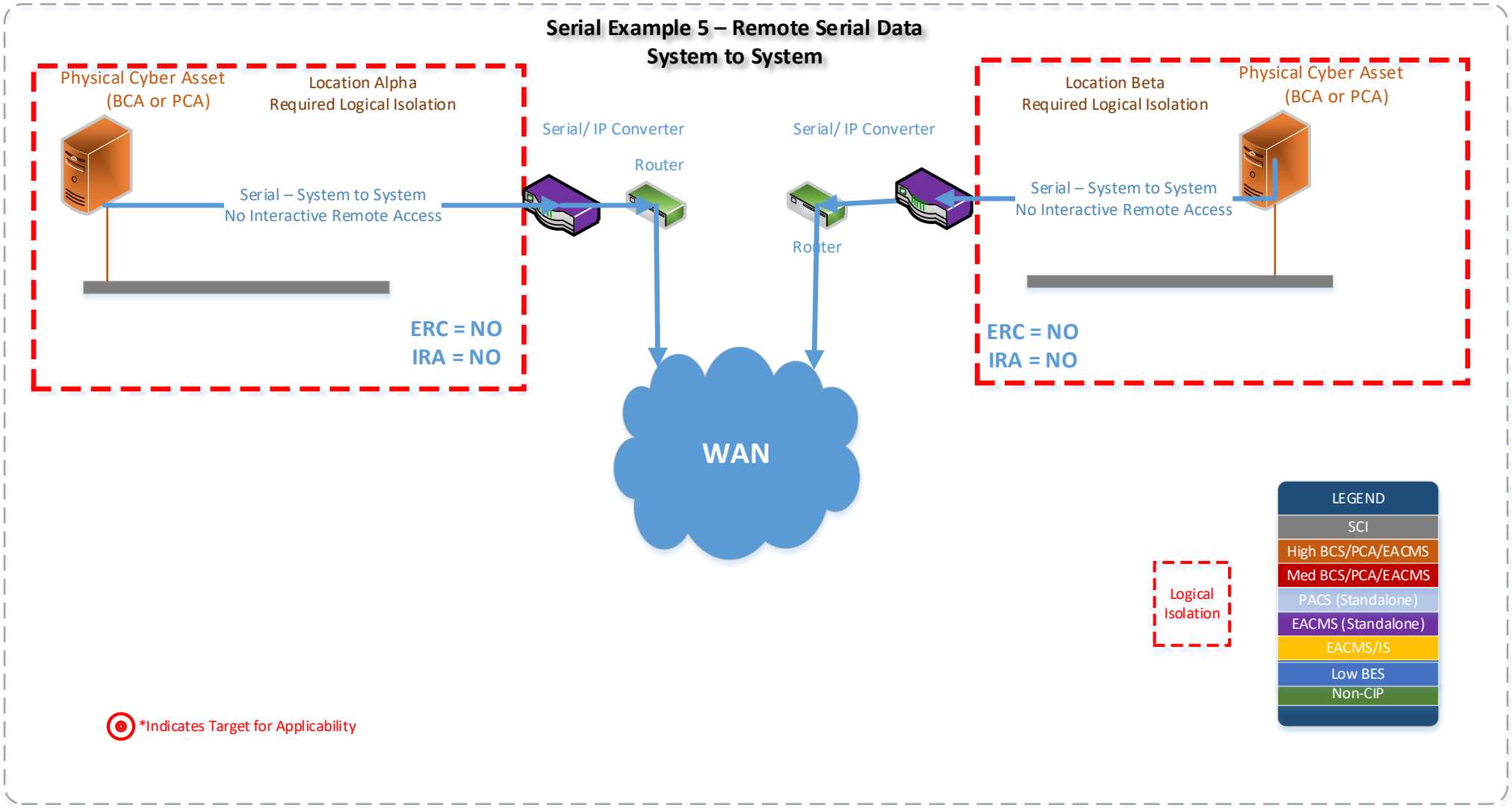
Use Case #3


Serial Example 3 – Serial Remote Access with IP Converter
IRA
Location Alpha
Physical Cyber Asset
(BCA or PCA)
Serial IRA
ERC = NO
IRA = YES
EACMS
Intermediate System
Serial/ IP
Terminal Server
Router
WAN
Location Beta
Cyber Asset
Remote Access Client
Router
User
Logical
Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

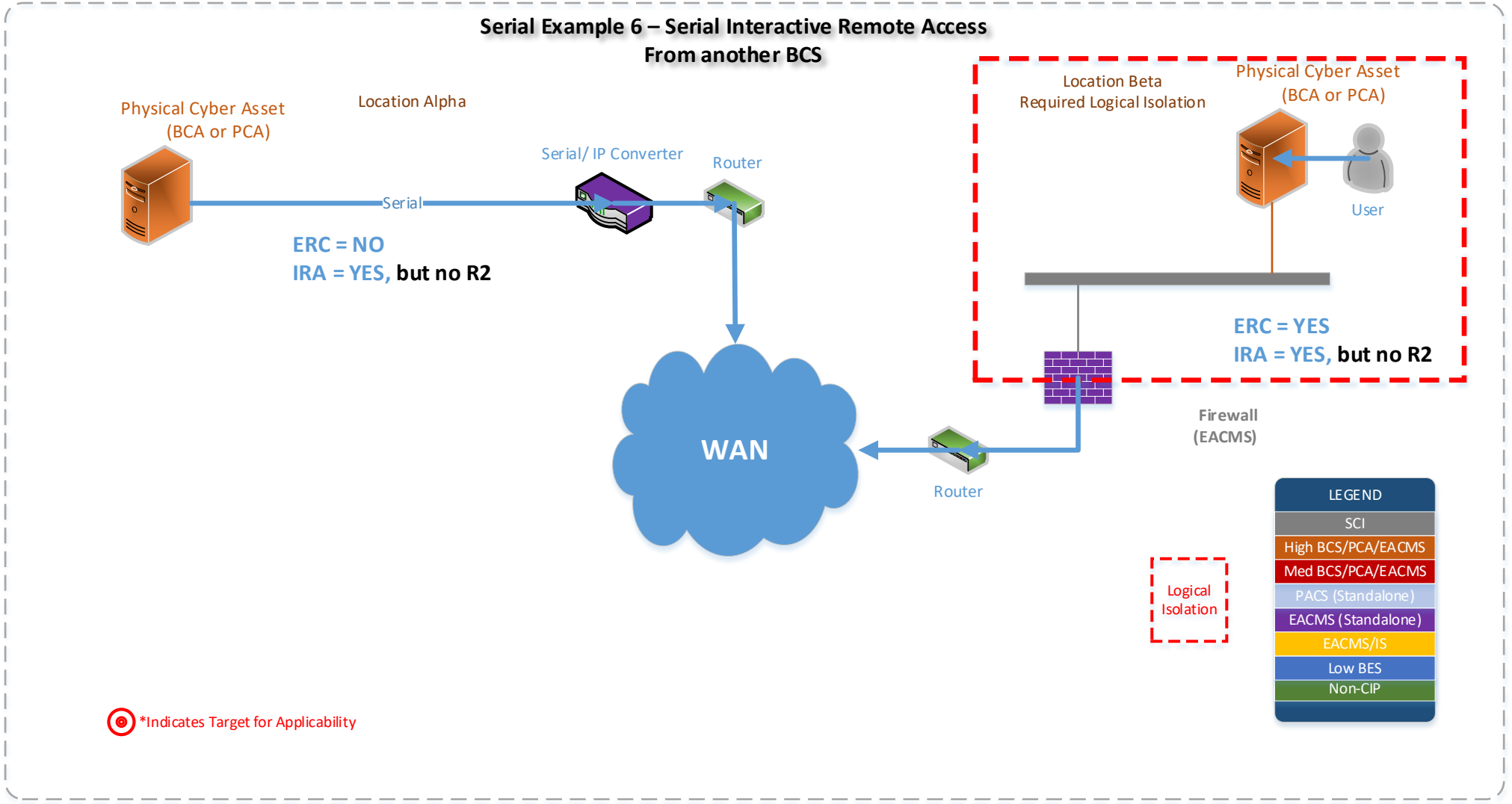
Use Case #4


Serial Example 4 – Remote Routable Data System to System
Physical Cyber Asset (BCA or PCA)
Location Alpha
Required Logical Isolation
ERC = YES
IRA = NO
Firewall (EACMS)
Router
WAN
Router
Firewall (EACMS)
Location Beta
Required Logical Isolation
Physical Cyber Asset (BCA or PCA)
ERC = YES
IRA = NO
Logical Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

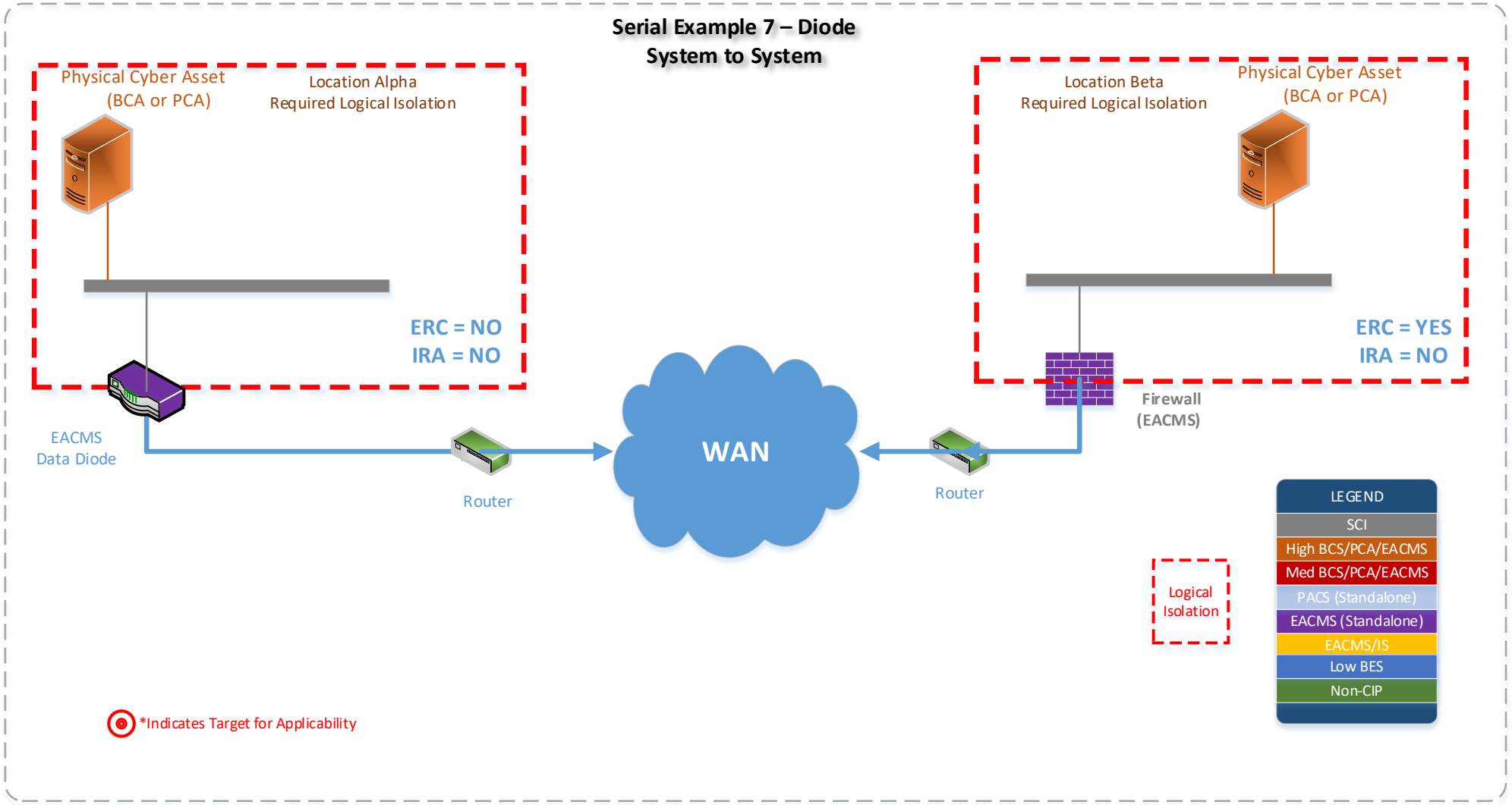
Use Case #5


Serial Example 5 – Remote Serial Data
System to System
Physical Cyber Asset
(BCA or PCA)
Location Alpha
Required Logical Isolation
Serial/ IP Converter
Router
Serial – System to System
No Interactive Remote Access
ERC = NO
IRA = NO
Serial/ IP Converter
Router
WAN
Location Beta
Required Logical Isolation
Physical Cyber Asset
(BCA or PCA)
Serial – System to System
No Interactive Remote Access
ERC = NO
IRA = NO
Logical Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

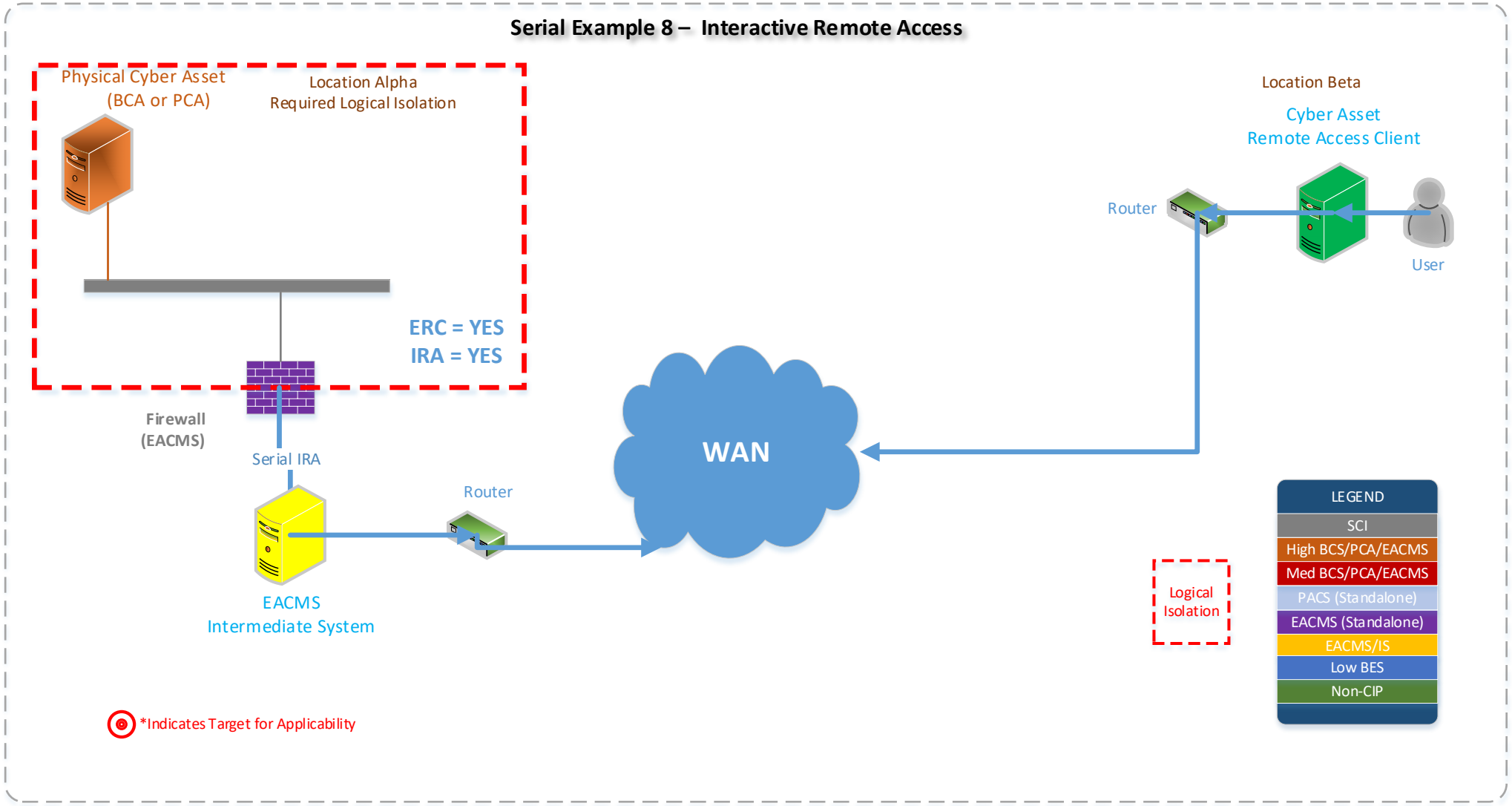
Use Case #6


Serial Example 6 – Serial Interactive Remote Access From another BCS
Location Alpha
Physical Cyber Asset (BCA or PCA)
Serial
Serial/ IP Converter
Router
ERC = NO
IRA = YES, but no R2
Location Beta
Required Logical Isolation
Physical Cyber Asset (BCA or PCA)
User
ERC = YES
IRA = YES, but no R2
Firewall (EACMS)
WAN
Router
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
Logical Isolation
*Indicates Target for Applicability

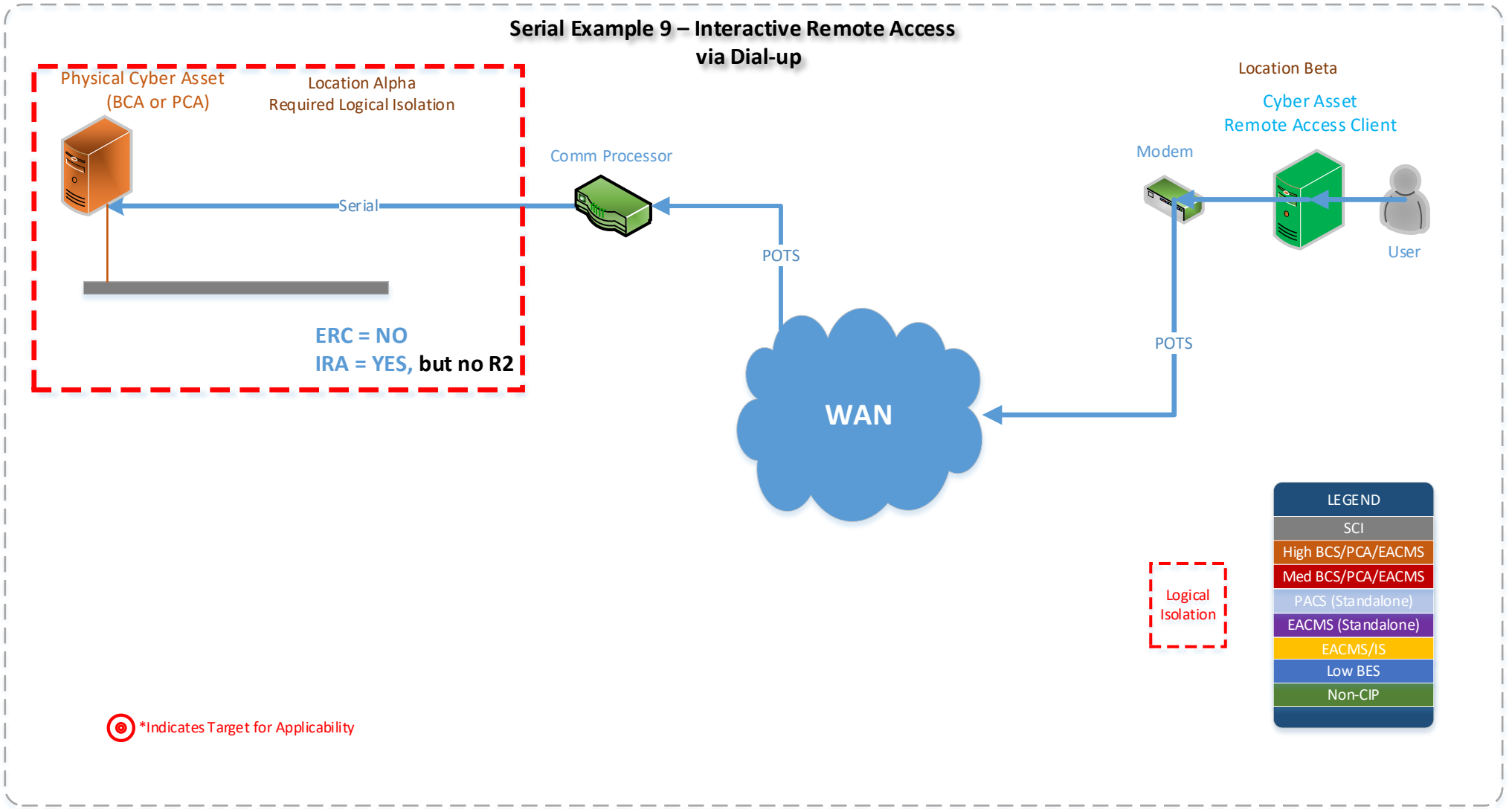
Use Case #7


Serial Example 7 – Diode
System to System
Physical Cyber Asset
(BCA or PCA)
Location Alpha
Required Logical Isolation
ERC = NO
IRA = NO
EACMS
Data Diode
Router
WAN
Router
Location Beta
Required Logical Isolation
Physical Cyber Asset
(BCA or PCA)
ERC = YES
IRA = NO
Firewall
(EACMS)
Logical
Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

Use Case #8


Serial Example 8 – Interactive Remote Access
Physical Cyber Asset
(BCA or PCA)
Location Alpha
Required Logical Isolation
ERC = YES
IRA = YES
Firewall
(EACMS)
Serial IRA
EACMS
Intermediate System
Router
WAN
Location Beta
Cyber Asset
Remote Access Client
Router
User
Logical
Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

Use Case #9


Serial Example 9 – Interactive Remote Access via Dial-up
Physical Cyber Asset (BCA or PCA)
Location Alpha
Required Logical Isolation
Serial
Comm Processor
POTS
WAN
POTS
Location Beta
Cyber Asset
Remote Access Client
Modem
User
ERC = NO
IRA = YES, but no R2
Logical Isolation
LEGEND
SCI
High BCS/PCA/EACMS
Med BCS/PCA/EACMS
PACS (Standalone)
EACMS (Standalone)
EACMS/IS
Low BES
Non-CIP
*Indicates Target for Applicability

Questions