NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

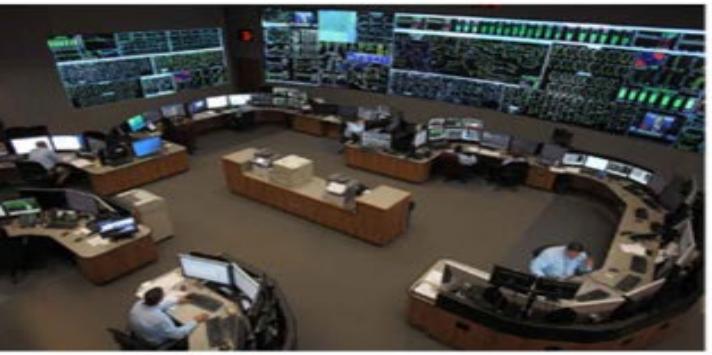
Join: slido.com
#2016-02-D1b

Project 2016-02

Modification to CIP Standards Outreach – Part 2
Draft 1 Posting

CIP SDT Members
March 3, 2021

RELIABILITY | RESILIENCE | SECURITY




Administrative Items

Join: slido.com
#2016-02-D1b

- 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.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. The access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

The CIP Standards Drafting Team

Join: slido.com
#2016-02-D1b

	Name	Entity
Co-chair	Jay Cribb	Southern Company
Co-chair	Matthew Hyatt	Georgia System Operations Corporation
Members	Jake Brown	ERCOT
	Norman Dang	Independent Electricity Systems Operator of Ontario
	Robert Garcia	SPP, Inc.
	Scott Klauminzer	Tacoma Public Utilities
	Sharon Koller	ATC, LLC
	Heather Morgan	EDP Renewables
	Mark Riley	Associated Electric Cooperative, Inc.

Q&A Objectives

- Informal Discussion
  - Via the Slido Q&A feature
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team.

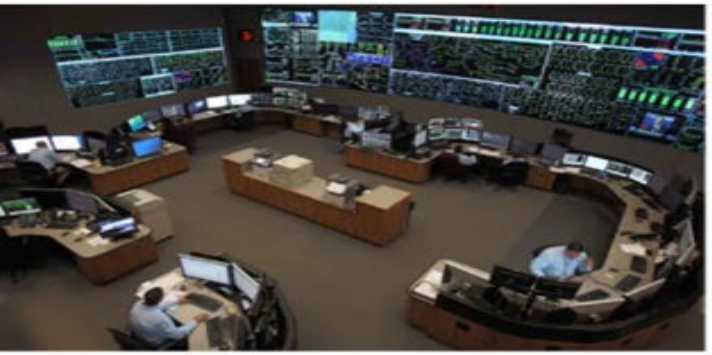
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Providing Feedback

Ask anonymously at anytime!
Vote other's questions up/down
Answer Polls and Surveys

Join at
slido.com
#2016-02-D1b

RELIABILITY | RESILIENCE | SECURITY




Poll Results

Join: slido.com
#2016-02-D1b

1. Help us shape the content for March 3rd. Select the top three topics you would like to hear more about.

195

Webinar Agenda

Join: slido.com
#2016-02-D1b

- Logical Isolation
- Management plane isolation
- Affinity and Logical Isolation for Security Mixed Trust
- Extended ESPs and Encryption Points
- IRA
- Resources
- Q&A

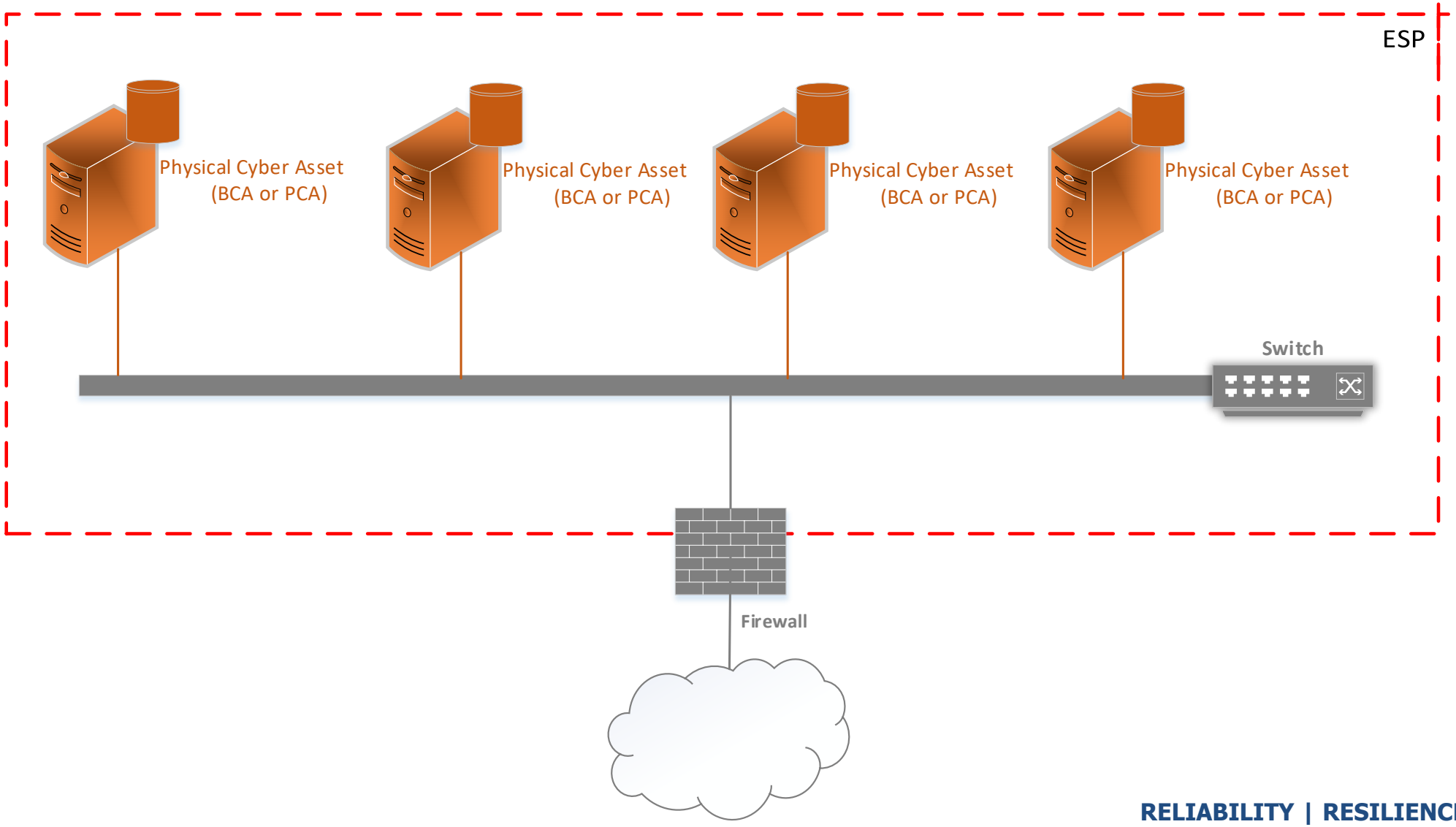
Join: slido.com
#2016-02-D1b

Logical Isolation

A Deeper Dive

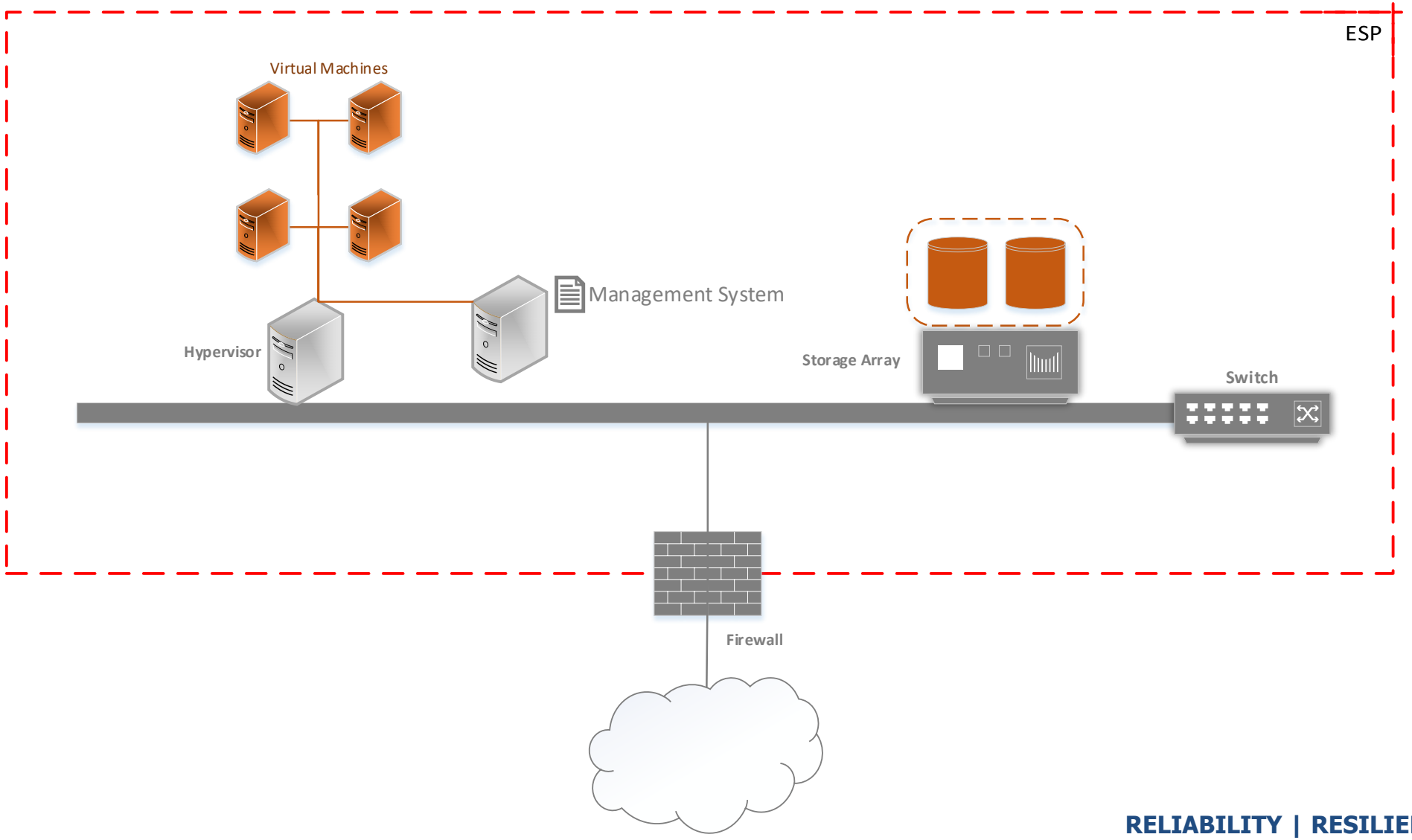
Cyber Assets and CIP-005 Today

Join: slido.com
#2016-02-D1b



Virtualization

Join: slido.com
#2016-02-D1b



Current CIP-005-6

WHAT

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

HOW

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-8 & Logical Isolation

CURRENT

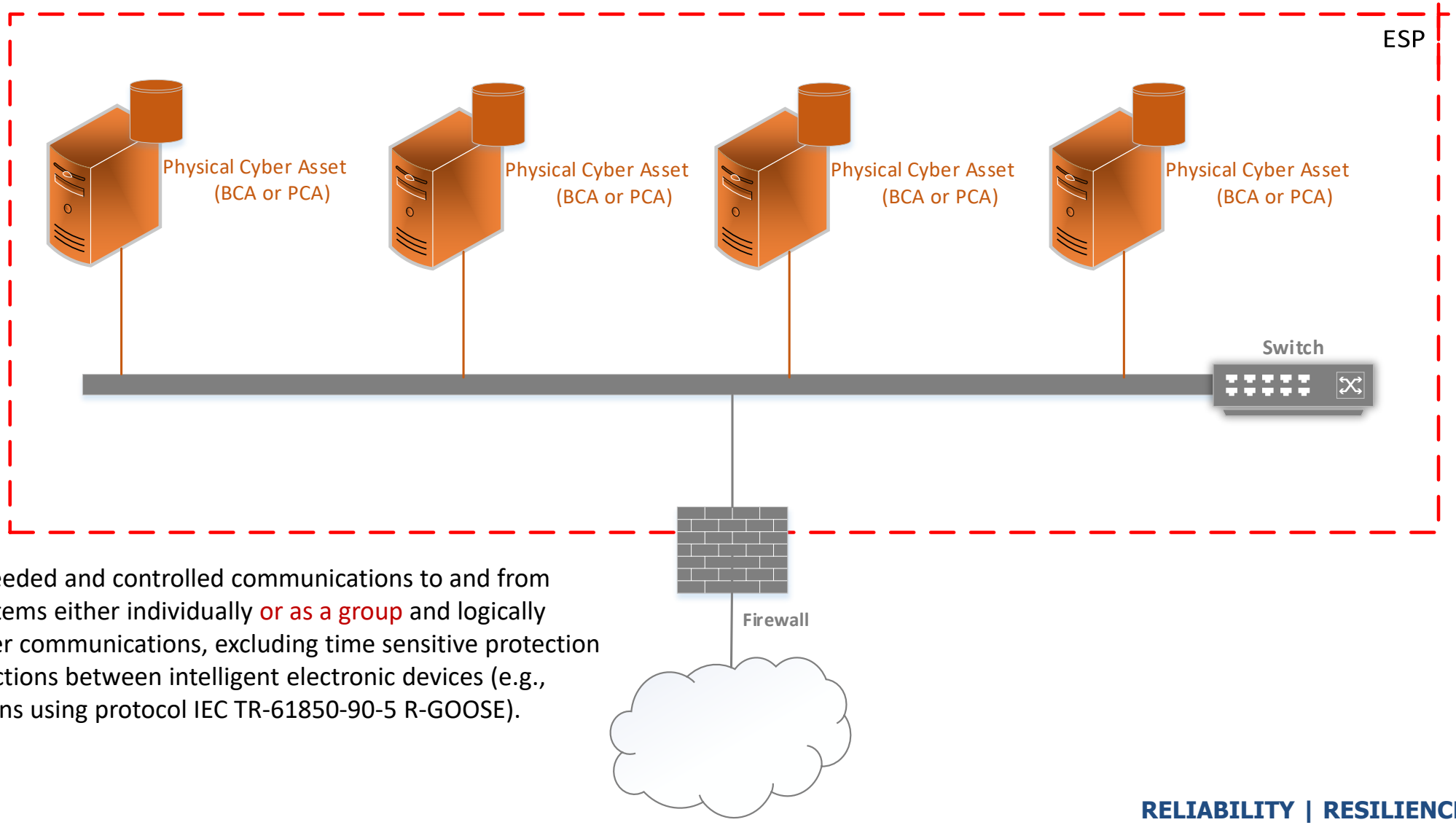
CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.

PROPOSED

CIP-005-8 Table R1 – Logical Isolation			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS connected to a network via a routable protocol and their associated: 1. Protected Cyber Asset (PCA); 2. Physical Access Control Systems (PACS) hosted on SCI; and 3. Electronic Access Control or Monitoring System (EACMS) hosted on SCI Medium Impact BCS connected to a network via a routable protocol and their associated: 1. PCA; 2. PACS hosted on SCI; and 3. EACMS hosted on SCI	Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).	Examples of evidence may include, but is not limited to, documentation that includes the configuration of systems such as: • Network infrastructure configuration or policies (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment); • SCI configuration or policies (hypervisor, fabric, backplane, or SAN configuration); that enforces electronic access control and logical isolation and documents the business need.

Current State Compatibility

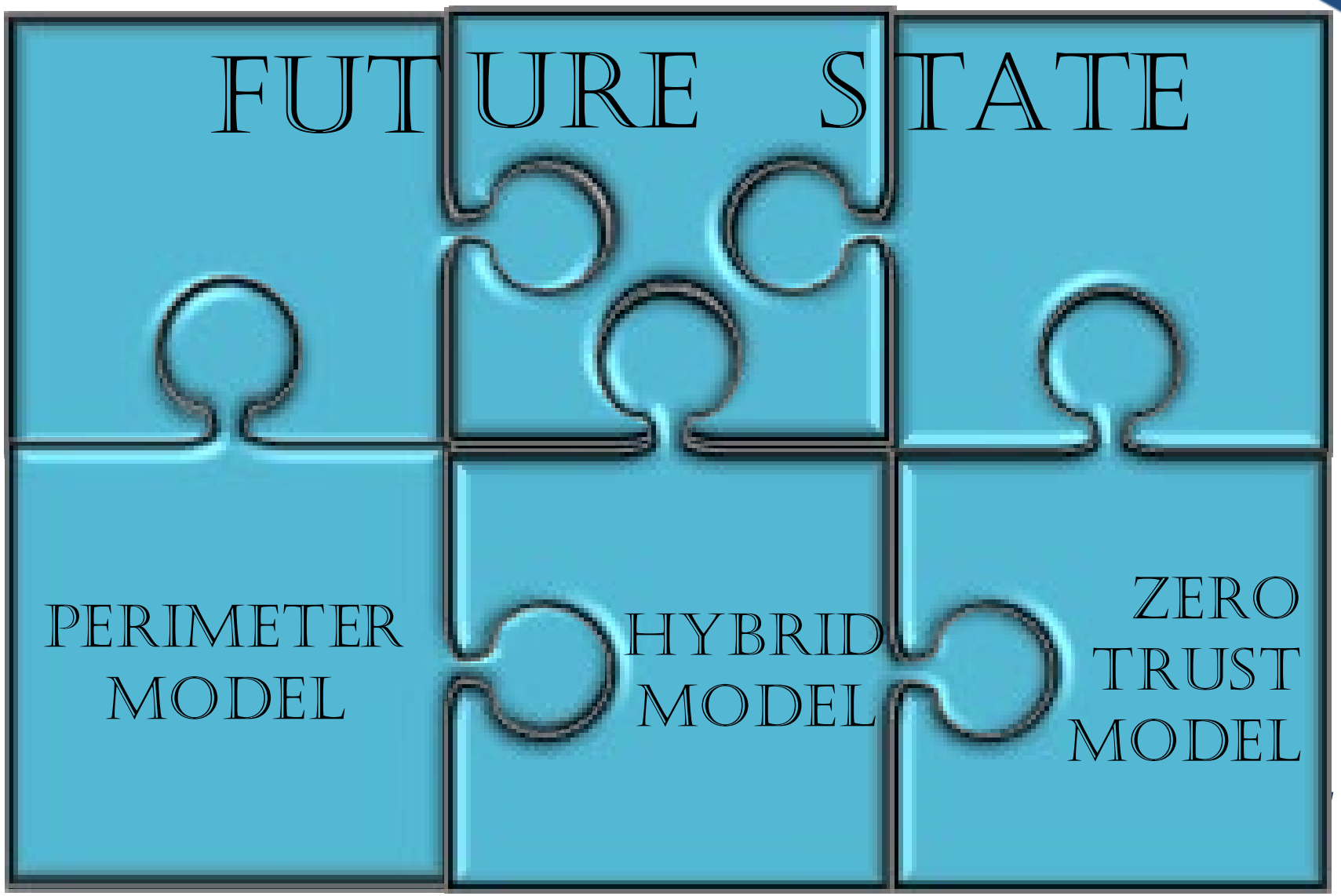
Join: slido.com
#2016-02-D1b



Permit only needed and controlled communications to and from applicable systems either individually or as a group and logically isolate all other communications, excluding time sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Logical Isolation

Join: slido.com
#2016-02-D1b



Join: slido.com
#2016-02-D1b

Questions and Answers

Join: slido.com
#2016-02-D1b

Management Plane Isolation

A Deeper Dive

Management Definitions

Join: slido.com #2016-02-D1b

- **Management System:** *Think: vCenter, Hyper-V Manager*

  "Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules."

- **Management Module:** *Think: iDRAC, iLO, CIMC, etc.*

  "An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system."

- **Management Interface:** *Think: Cisco Console Port, iLO eth port*

  "A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities."

Management System Scope

- So, what is a Management System?

> ***Management System:***
> *"Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying **and** configuring those assets and systems; excluding Management Modules."*

- Management Systems are those systems that do **all** (initialize, deploy, **and** configure)
  - If not all three, it is not a Management System

CIP-005 R1.2 Management Isolation Scope

- What is the scope of Management Plane isolation?

Applicable Systems	Requirements
SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS	Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.

Management Isolation - Why? and How?

Join: slido.com
#2016-02-D1b

Why?

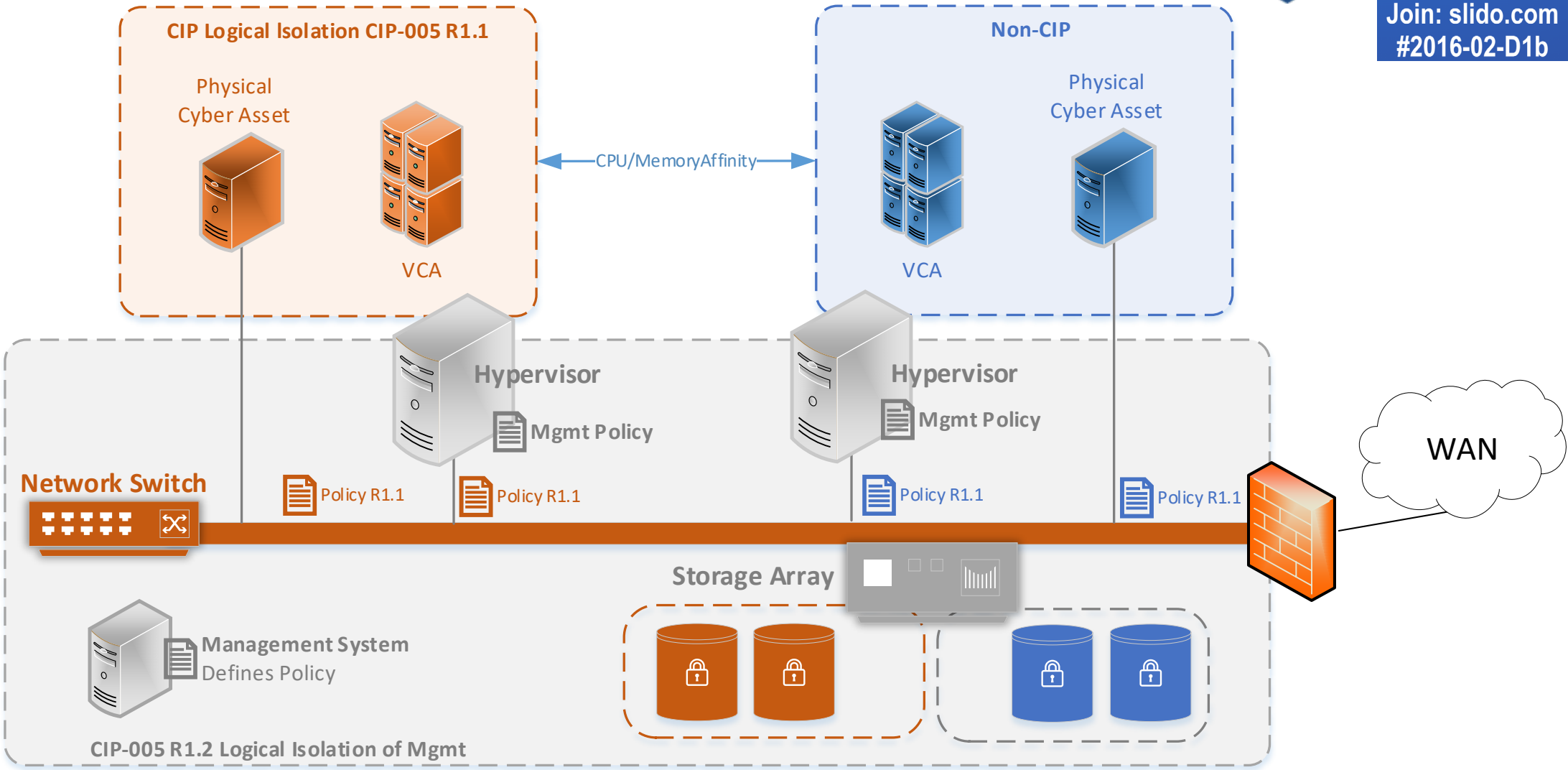
- Cloud tenant isolation control applied to on-prem
  - CIP-005 R1 Part 1.2.1 is affinity control (for mixed trust)
  - CIP-005 R1 Part 1.2.2 is logical isolation
  - CIP-005 R1 Part 1.2.3 denies BCS

How?

- VLAN
- ACL
- Zero-Trust
- Physical…

CIP-005 R1 Part 1.2 Management Isolation

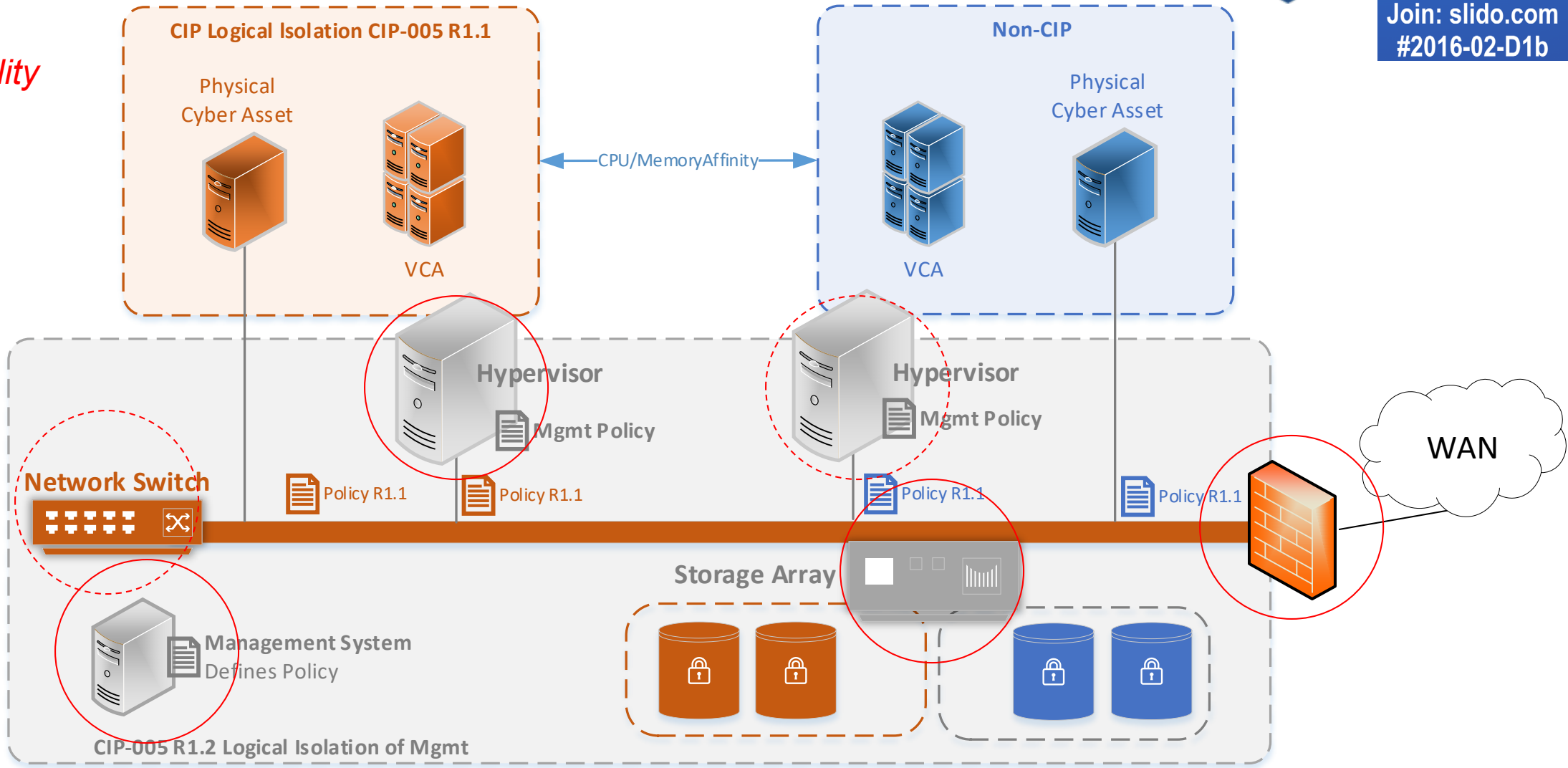
Join: slido.com
#2016-02-D1b



CIP-005 R1 Part 1.2 Management Isolation

Join: slido.com #2016-02-D1b

○ *Indicates Applicability*



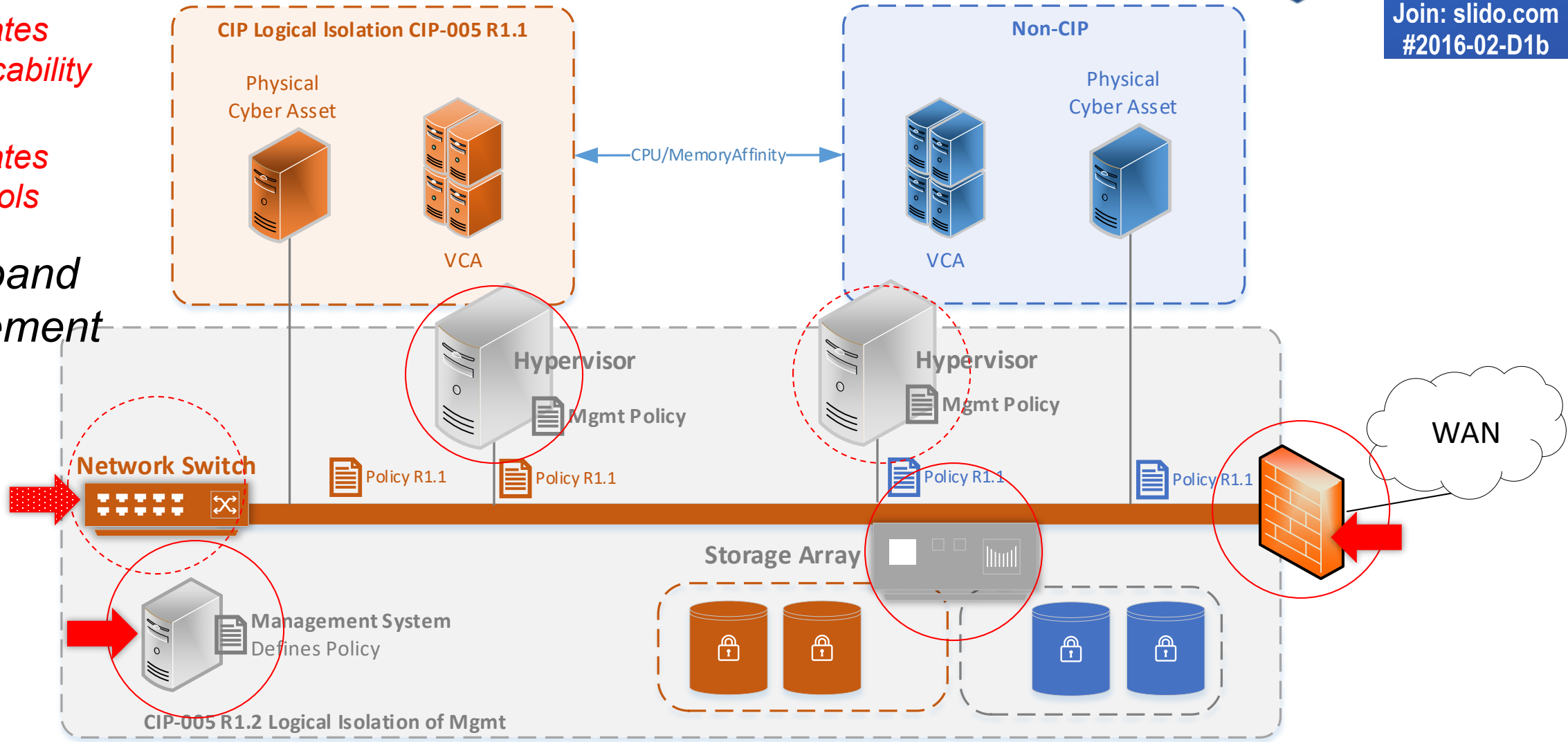
CIP-005 R1 Part 1.2 Management Isolation

Join: slido.com #2016-02-D1b

Indicates Applicability

Indicates Controls

Out-of-band management



Join: slido.com
#2016-02-D1b

Questions and Answers

Join: slido.com
#2016-02-D1b

Affinity and Logical Isolation for securing Mixed Trust

A Deeper Dive

Securing Mixed Trust

Join: slido.com
#2016-02-D1b

What is Mixed-Trust in this context?

- Sharing CPU/memory between differing impact levels
- Sharing storage resources between differing impact levels
- Sharing network Resources between differing impact levels

What are we not considering mixed trust in this context?

- Identity management systems (Active directory, etc)

- **Related Definitions**
  - SCI (Identifies shared compute and storage resources)
  - VCA (Identifies virtual machines)
  - PCA (Used for high watermarking)
- **Related Requirements**
  - CIP-005 R1 Part 1.1 (Permit only needed comms)
  - CIP-005 R1 Part 1.2 (Protect Management)
  - CIP-005 R2 Part 2.6 (Protect Intermediate Systems)

Securing Mixed Trust

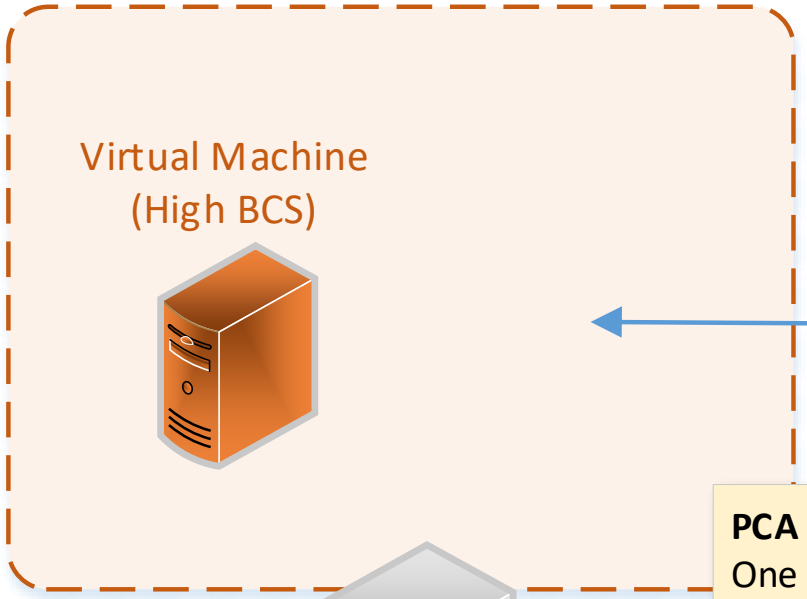
Join: slido.com
#2016-02-D1b

- **Mixed Trust Scenarios**
  - Single Hypervisor
  - Dormant or Staging VM's
  - Cluster of Hypervisors
  - Networks
  - Storage Arrays

Single Hypervisor - Securing Mixed Trust

Join: slido.com
#2016-02-D1b

On a Single Hypervisor scenario, the New VCA meets the definition of a PCA if it is not logically isolated from or shares memory/cpu with a BES Cyber System or



PCA Definition

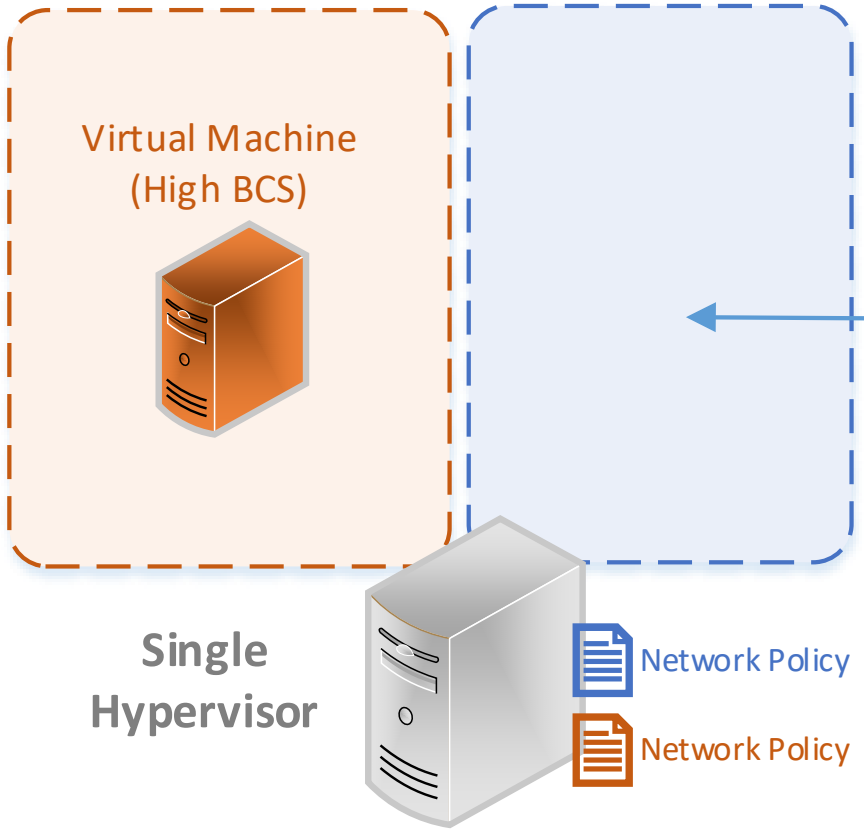
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Single Hypervisor - Securing Mixed Trust

Join: slido.com
#2016-02-D1b



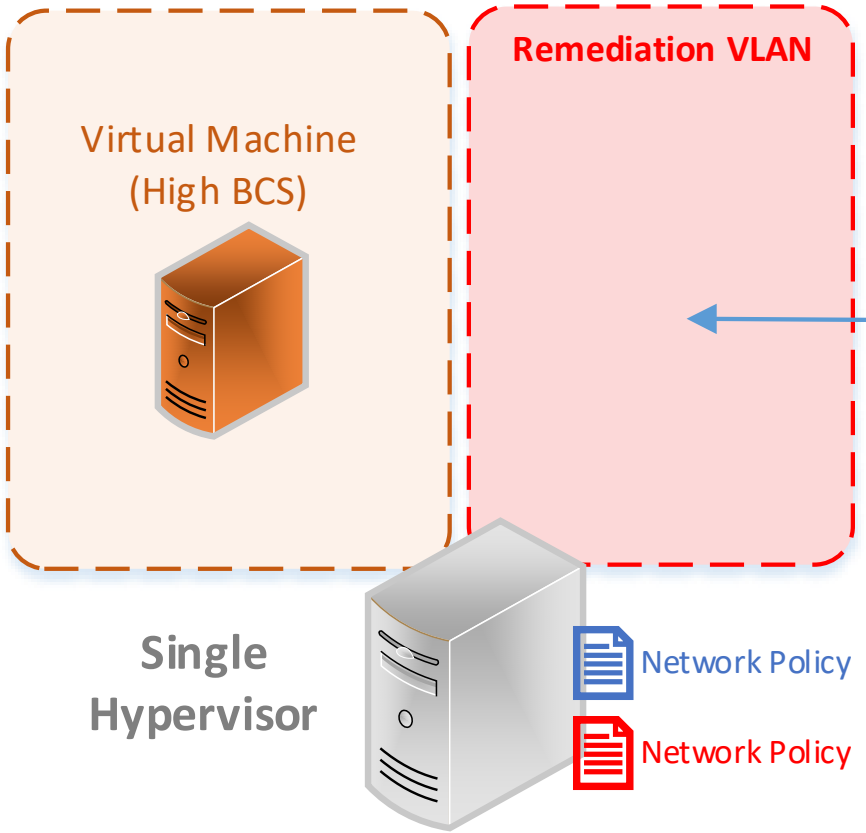
On a Single Hypervisor scenario, the New VCA meets the definition of a PCA if it shares memory/cpu with a BES Cyber System

PCA Definition
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Dormant VM Example – Securing Mixed Trust



PCA Definition

One or more Cyber Assets or Virtual Cyber Assets that:

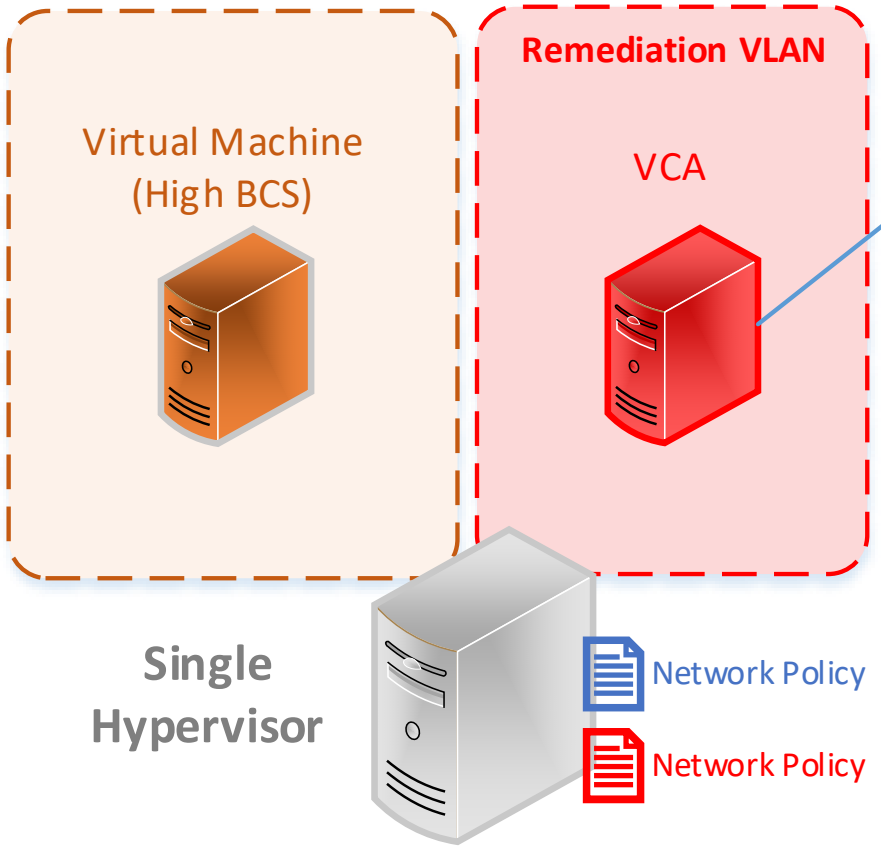
- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding

Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Dormant VM Example – Securing Mixed Trust

Join: slido.com
#2016-02-D1b



VCA is being actively remediated, running scans, ensuring it meets policy before introduction into production network

Has access to patching servers and AV, etc

PCA Definition

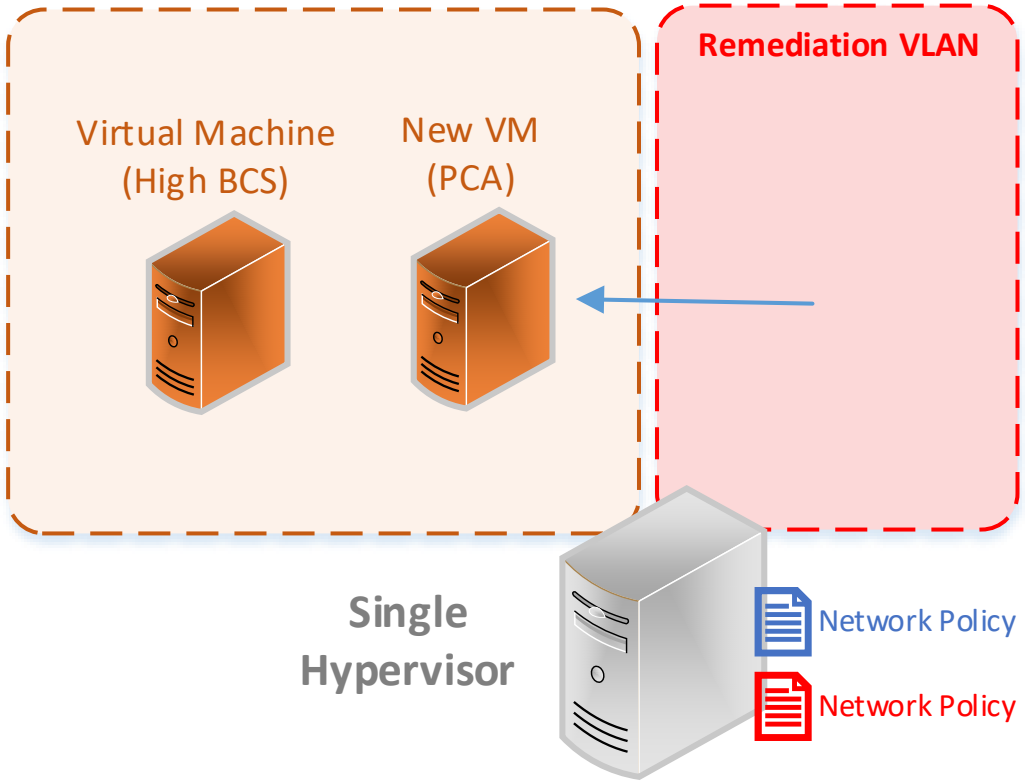
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding

Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Dormant VM Example – Securing Mixed Trust



PCA Definition

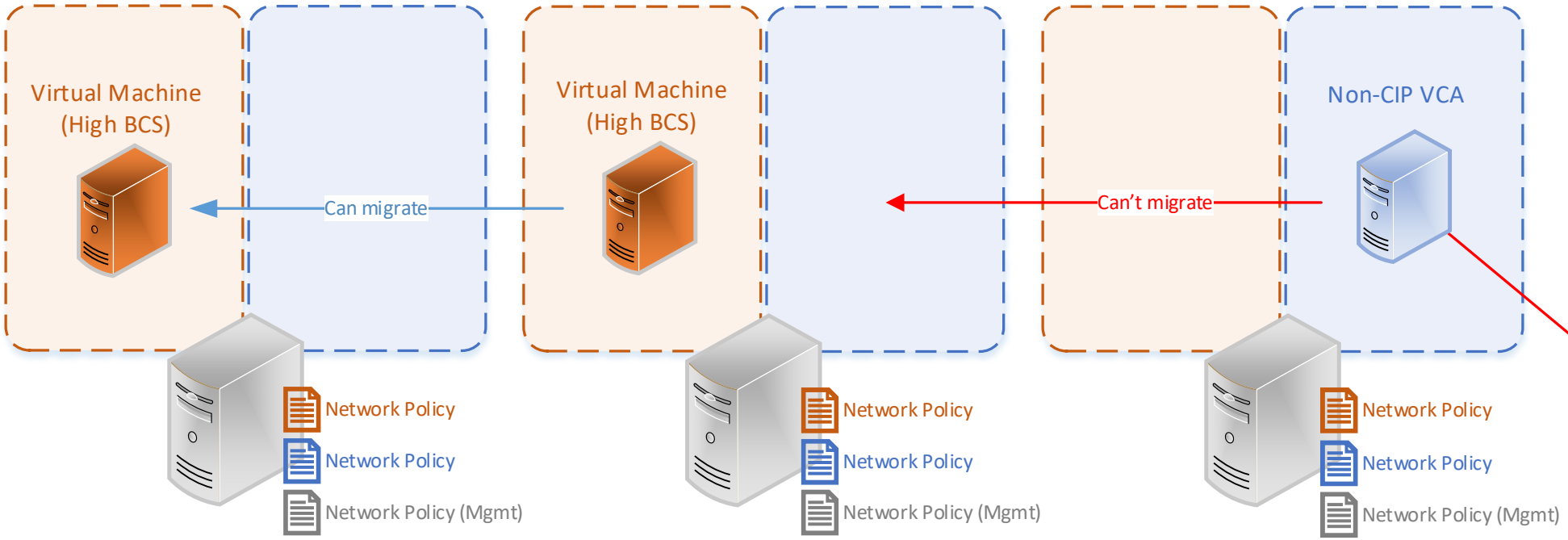
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Hypervisor Cluster - Securing Mixed Trust

Join: slido.com
#2016-02-D1b



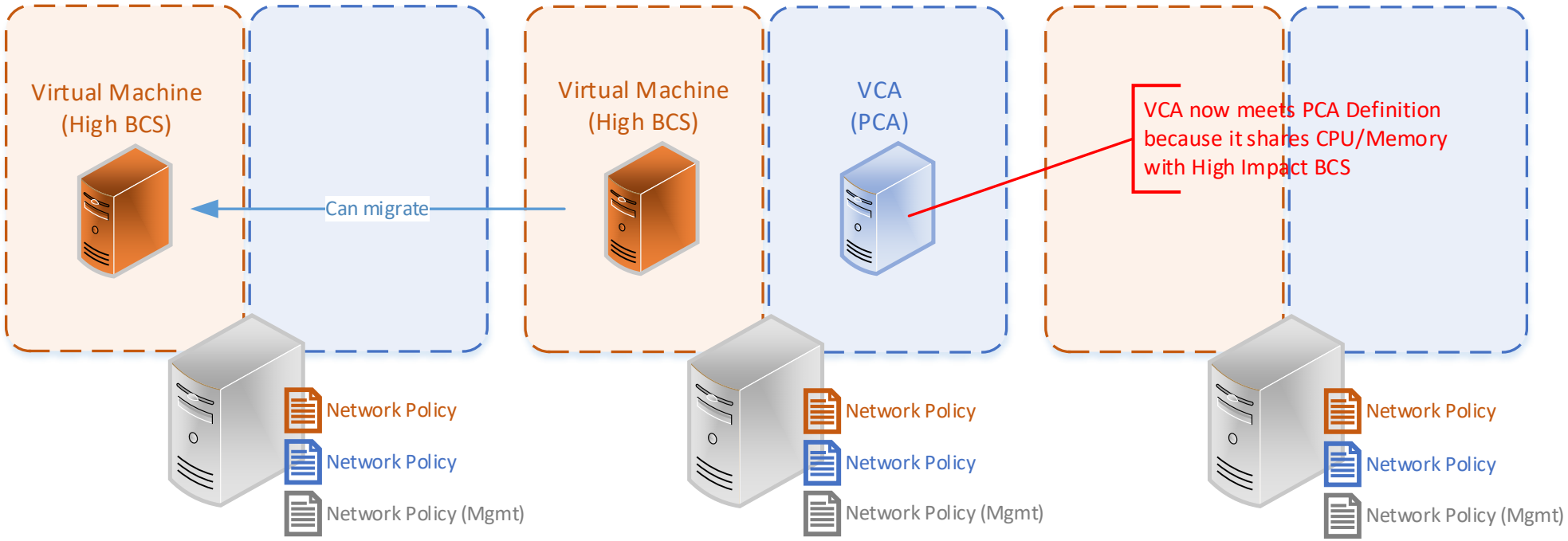
PCA Definition
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Hypervisor Cluster - Securing Mixed Trust

Join: slido.com
#2016-02-D1b

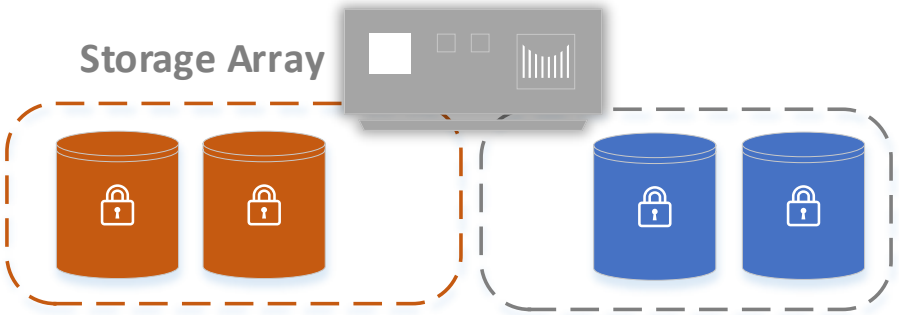


PCA Definition
One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Storage Array Example- Securing Mixed Trust

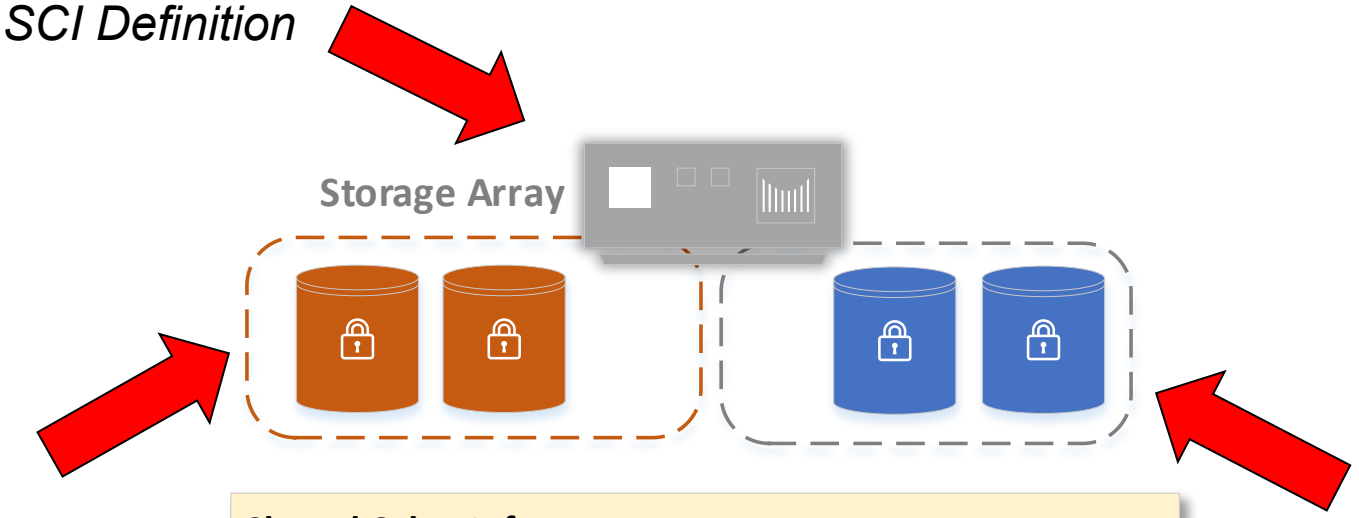


Shared Cyber Infrastructure
One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Storage Array Example- Securing Mixed Trust

Join: slido.com #2016-02-D1b

Meets SCI Definition

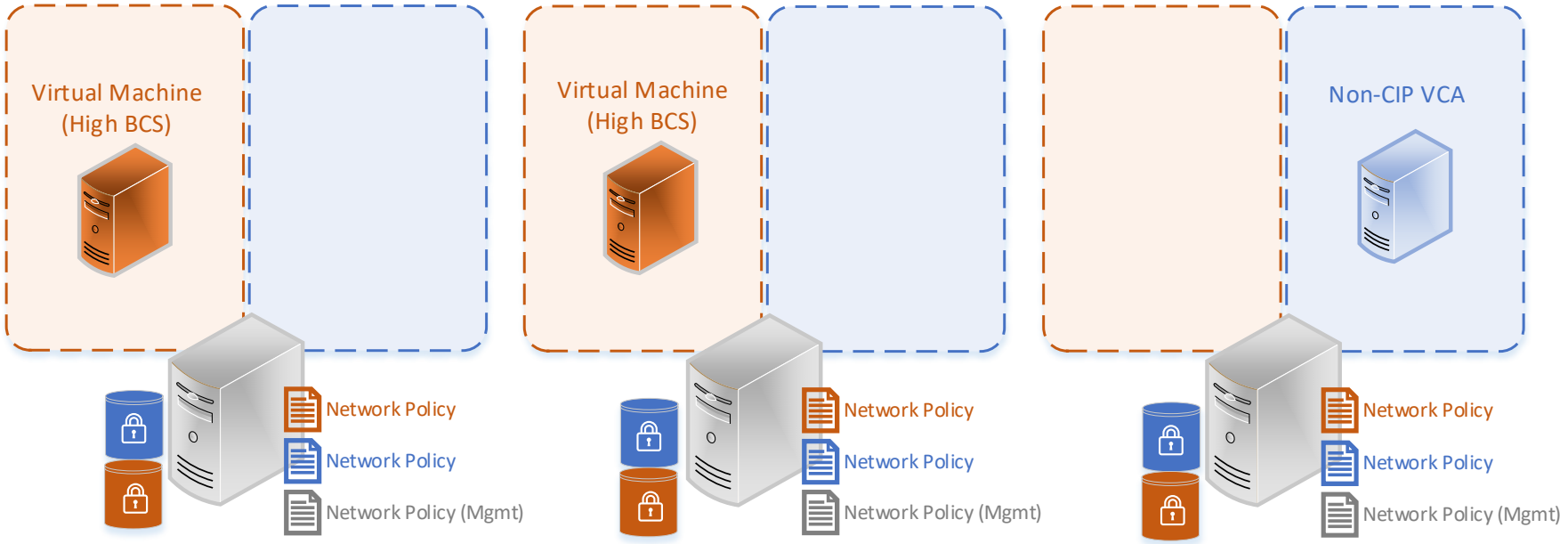


Storage resource shared with BES Cyber System

Storage resource shared with Non-CIP Cyber Asset

Shared Cyber Infrastructure
One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Hyper Converged Storage Example – Securing Mixed Trust



Shared Cyber Infrastructure
One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Meets SCI Definition

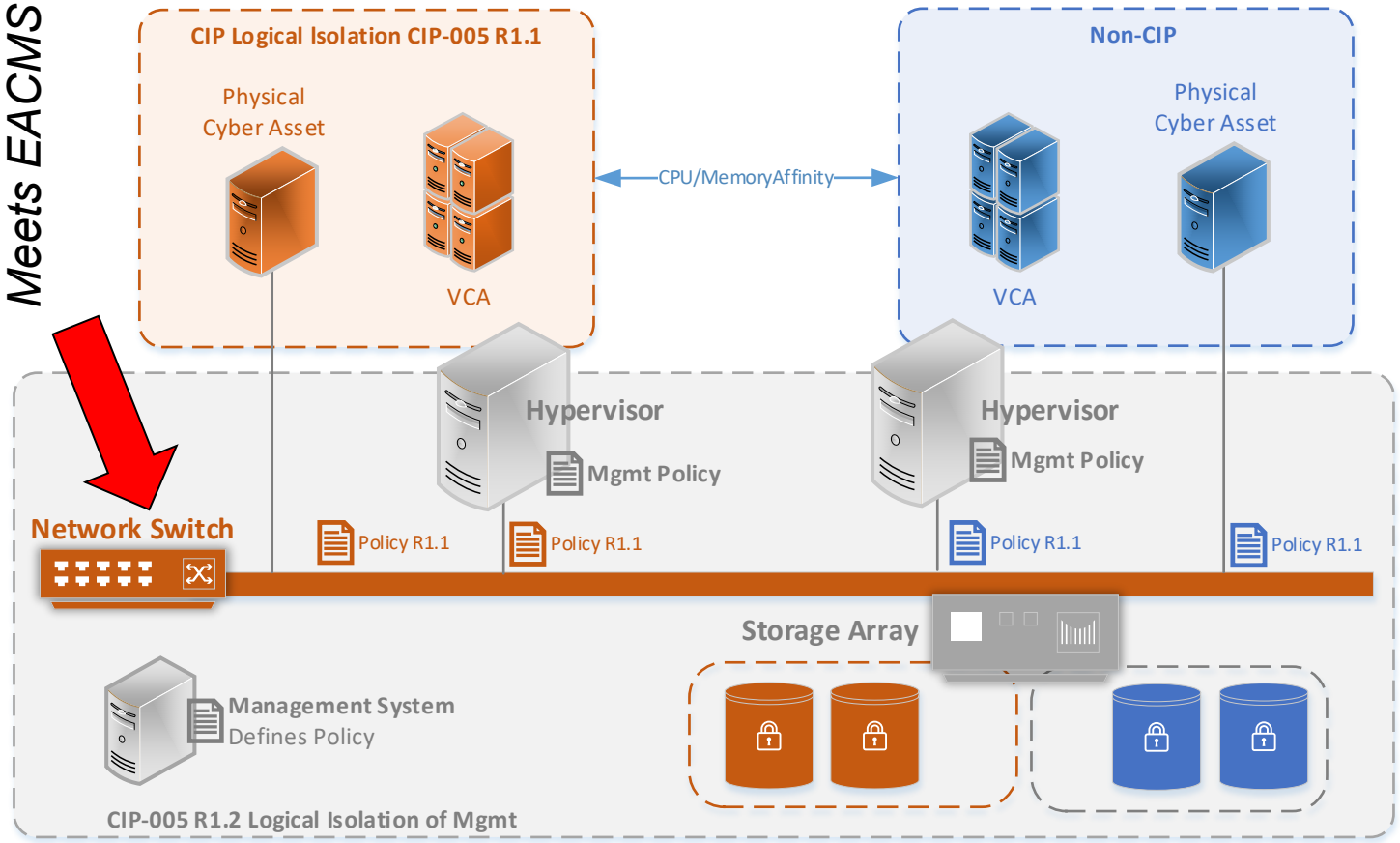
Network Example – Securing Mixed Trust

Join: slido.com
#2016-02-D1b

EACMS
Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation Electronic Security Perimeter(s) ofr BES Cyber Systems. This includes Intermediate Systems.

CIP-005-8 Table R1 – Logical Isolation		
Part	**Applicable Systems**	**Requirements**
1.2	SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS Management Modules of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS EACMS that perform logical isolation for a High Impact BCS EACMS that perform logical isolation for a Medium Impact BCS	Implement for applicable systems as follows: **1.2.1.** Restrict Management Systems to only share CPU and memory with its associated SCI and other Management Systems, per system capability. **1.2.2.** Permit only needed and controlled communications to and from Management Interfaces and Management Systems, logically isolating all other communications. **1.2.3.** Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.

Meets EACMS Definition



Summary - Securing Mixed Trust

Join: slido.com
#2016-02-D1b

Summary – Where is mixed trust allowed?

- ***Single Hypervisor = Not allowed*** *- Can't meet affinity requirements, SCI Def, PCA definition & CIP-005 R1.2*
- ***Dormant VM or staging VM's = Permitted*** *while being actively remediated*
- ***Cluster of Hypervisors = Permitted*** *with proper affinity configuration, Hypervisors meet SCI Def, PCA definition & CIP-005 R1.2*
- ***Storage Array = Permitted****, meets SCI def, no reqs prevent other use*
- ***Networks = Permitted*** *with proper management isolation, CIP-005 R1.2, EACMS performing logical isolation*

Join: slido.com
#2016-02-D1b

Questions and Answers

Join: slido.com
#2016-02-D1b

Extended ESPs & Encryption Points

A Deeper Dive

Extended ESPs (SuperESP)

- What is it?
  - Logical Isolation that extends beyond a Physical Security Perimeter.
- Why?
  - Virtual Machine Migration
  - Multi Site Clustering Mechanisms
- Related Requirements
  - CIP-005 R1 Part 1.3 (Confidentiality and Integrity)

Extended ESPs (SuperESP)

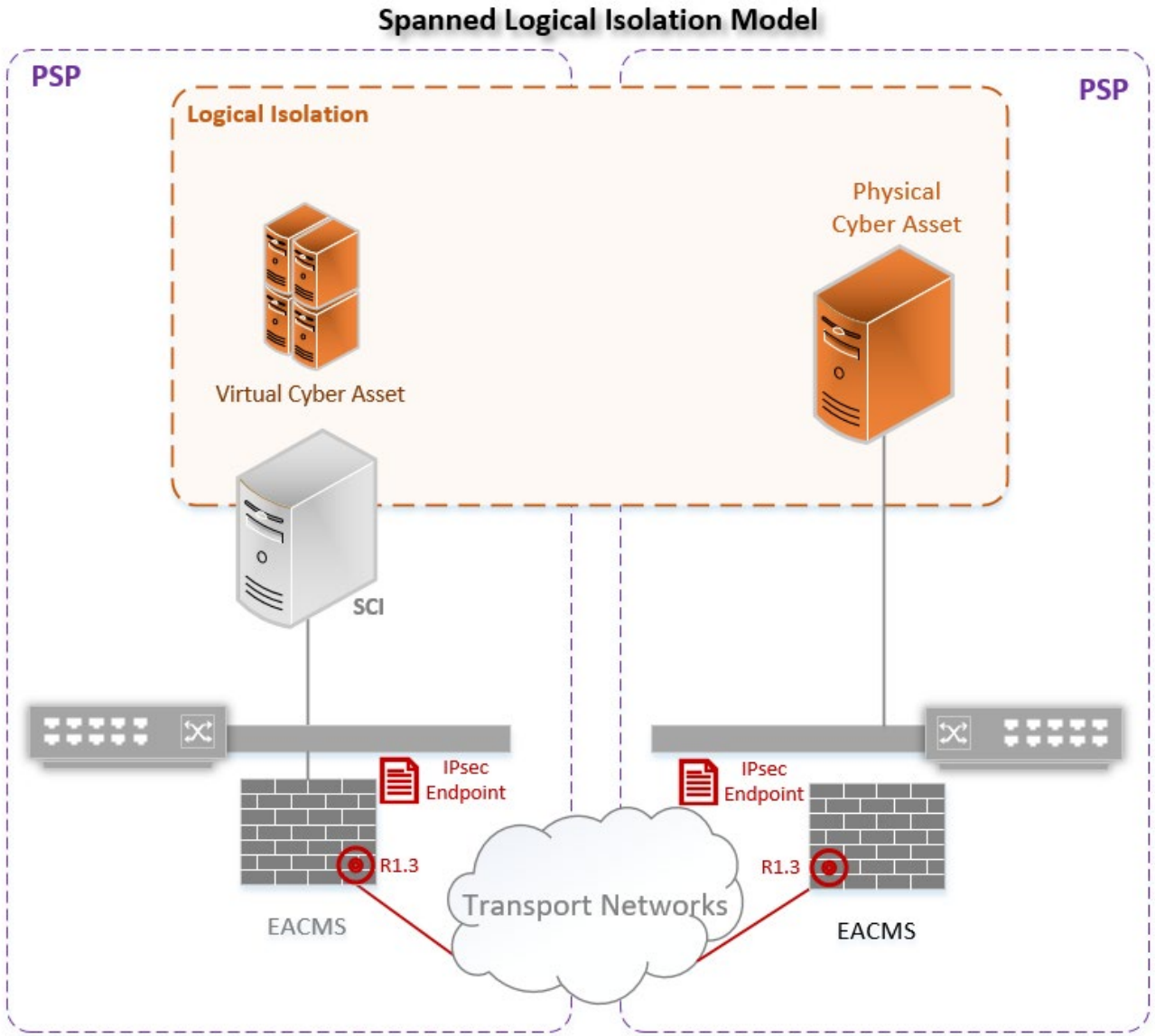
- Confidentiality and Integrity
  - As Seen in CIP-012
    - CIP-005 R1.3 and CIP-012 Differences
  - Confidentiality
    - Encrypt the Data
  - Integrity
    - Authenticate the Data

Extended ESPs (SuperESP)

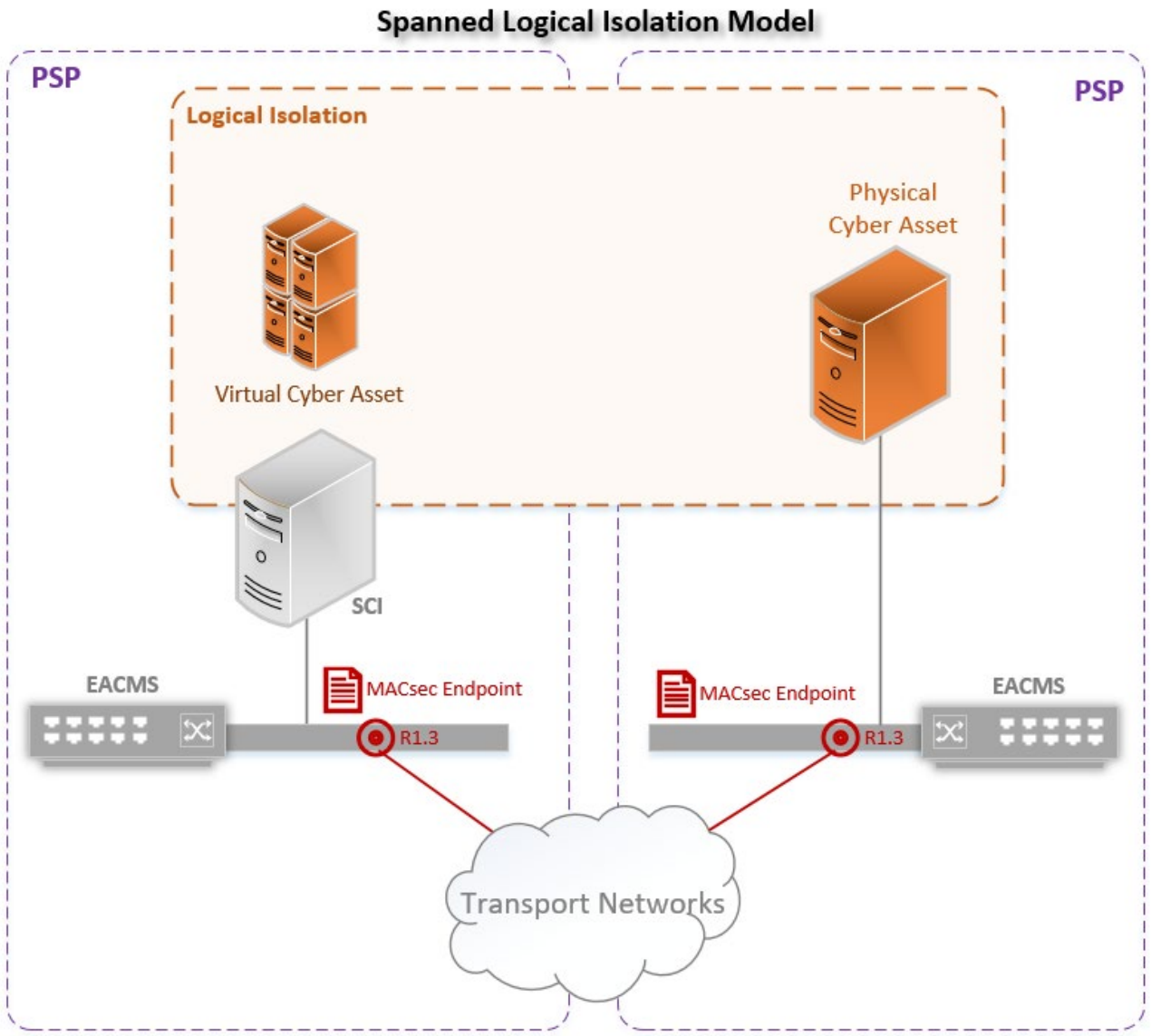
- Example Technologies
  - IPsec
    - Authentication Header(AH)
    - Encapsulating Security Payload(ESP)
  - MACsec
    - Integrated Authentication and Encryption

Extended ESPs (SuperESP)

Join: slido.com
#2016-02-D1b



Extended ESPs (SuperESP)



Join: slido.com
#2016-02-D1b

Questions and Answers

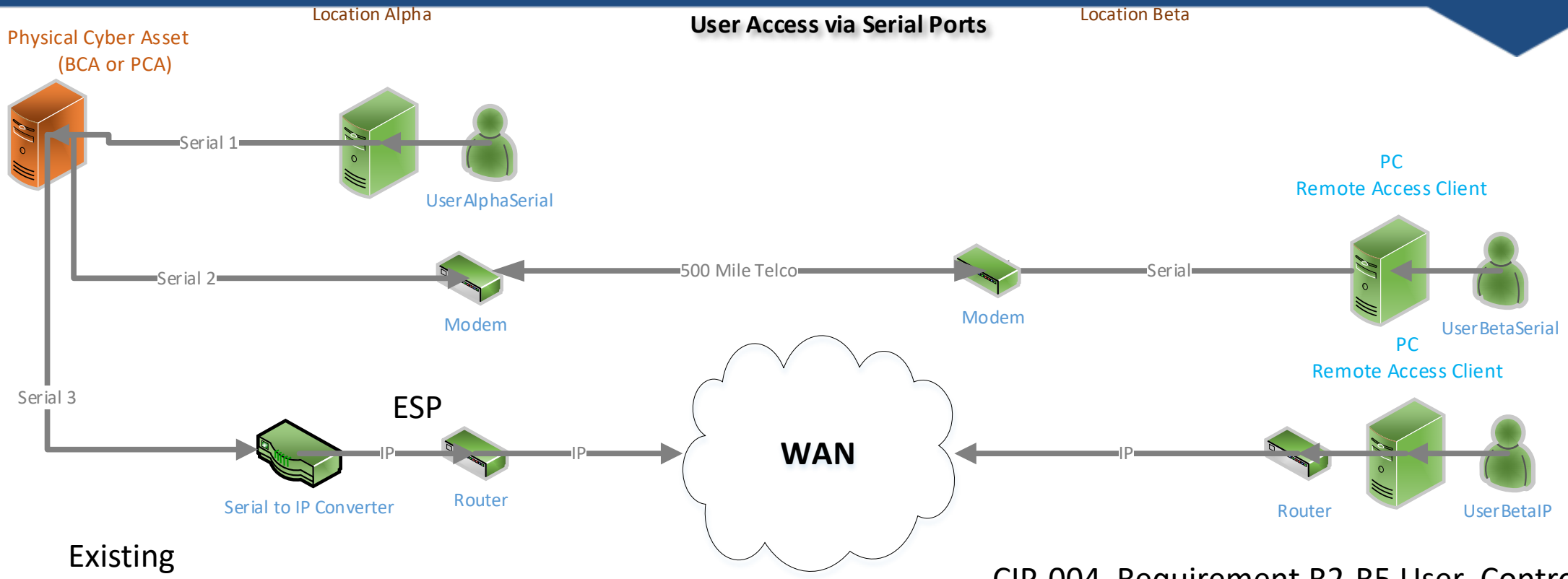
Join: slido.com
#2016-02-D1b

IRA

A Deeper Dive

Interactive Remote Access – Why Change Stuff ?

Join: slido.com
#2016-02-D1b



Existing
ERC = No and therefore IRA = No
CIP-005-7 Requirement R2 Controls Apply ? = No

CIP-004 Requirement R2-R5 User Controls apply? = No

- Serial 2 and 3 represents a gap the existing CIP Standards
- V5TAG asked that this gap be addressed

IRA and Changes CIP-005 Requirement R2

Join: slido.com #2016-02-D1b

V5TAG recommended improving clarity within the concepts and requirements concerning ESP, ERC, and 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

In response, the SDT proposes the following changes:

- Keep ERC as-is with conforming changes in order to not disrupt it’s scoping function.
- Simplify the IRA definition by removing embedded requirements (protocol, location, ownership)
- Change the applicable systems scoping in CIP-005 Requirement R2 where needed from *Medium Impact BES Cyber Systems* ***with ERC*** to *Medium Impact BES Cyber Systems* ***with IRA***

IRA Definition Change

Join: slido.com #2016-02-D1b

Interactive Remote Access (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.	User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed. ~~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.~~

Green

Yellow

Blue

Scoping Change in CIP-005 Requirement R2 Applicability

Join: slido.com #2016-02-D1b

CIP-005-~~6~~7 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact ~~BES Cyber Systems~~BCS and their associated: • PCA Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~Interactive Remote Access (IRA) and their associated: • PCA SCI with IRA hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS~~.~~ Management Modules with IRA of SCI hosting High or Medium Impact BCS or their associated: • PCA; • PACS; or • EACMS	Ensure that ~~authorized~~ IRA is through an Intermediate System. ~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.~~	Examples of evidence may include, but are not limited to, network diagrams~~,~~ ~~or~~ architecture documents, or Management Systems reports that show all IRA is through an Intermediate System.

Green

Yellow

IRA and Changes CIP-005 Requirement R2

Net Effect:

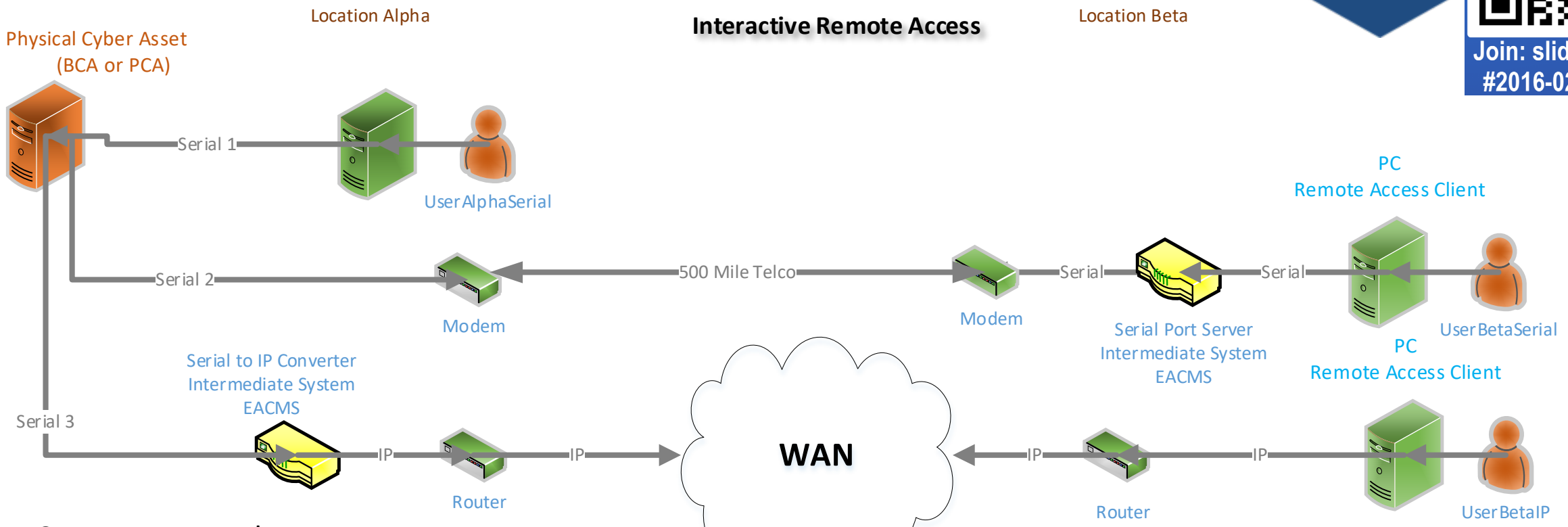
- Scoping change away from “with ERC” to “with IRA” now includes serial connections due to the change in the IRA definition

Side Effect

- Matching controls from CIP-004 Requirements R2 – R5 to cover all instances of user access (including IRA)

Net Effect of SDT Proposed Changes

Join: slido.com #2016-02-D1b



ERC= No , Proposed IRA = Yes
CIP-005-7 R2 Controls Apply ? = Yes for Serials 2 & 3

Proposed CIP-004 R2-R5 User Controls apply? = Yes

- CIP-005 Requirement R2 – applies for Serial Ports 2 and 3
- User controls required from CIP-004 Requirements R2 –R5

Join: slido.com
#2016-02-D1b

Questions and Answers

Resources

Join: slido.com
#2016-02-D1b

- This slide deck and other information relative to the CIP Modifications SDT may be found on the Project 2016-02 Project Page under Related Files:

  http://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx

- The Informational Filing of the North American Electric Reliability Corporation Regarding Standards Development Projects latest filing can be found here:

  https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/CIP%20SDT%20Schedule%20 %20Dec_2020_Informational%20Filing.pdf

- Project 2016-02 Related Files Pages for previous webinar recordings:
  https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx

Resources Continued

Join: slido.com
#2016-02-D1b

- Project 2016-02 Related Files Pages for previous webinar recordings:
  https://www.nerc.com/pa/Stand/Pages/Project-2016-02-Modifications-to-CIP-Standards-RF.aspx
- Specific Recommended Webinars:
  - Draft 1 Posting | Outreach Webinar (Part 1) (LINK)
  - Management Systems (LINK)
  - SuperESP (LINK)
  - Virtual Machines and Containers (LINK)
  - Hypervisor and Storage Systems (LINK)
  - External Routable Connectivity and Interactive Remote Access (LINK)
  - CIP-005 and Zero Trust (LINK)

Join: slido.com
#2016-02-D1b

Questions and Answers