NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

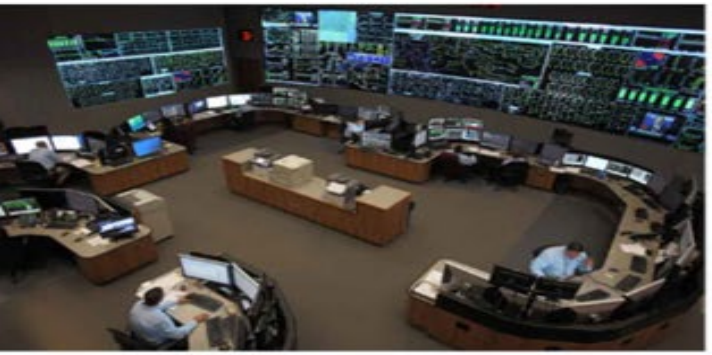
Join: slido.com
#2016-02-D2

Project 2016-02

Modification to CIP Standards Outreach
Draft 2

CIP SDT Members
August 4, 2021

RELIABILITY | RESILIENCE | SECURITY




Administrative Items

Join: slido.com
#2016-02-D2

- 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-D2

	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.

Opening Remarks

Join: slido.com
#2016-02-D2

- **Webinar Purpose:** High level overview of modifications for Project 2016-02 Modification to CIP Standards 45-day initial comment and ballot period (with 1 week extension)
- **Draft 2 Posting Duration:** June 30 – August 31, 2021
  - 45-day comment and ballot period
  - 1 week extension with CIP-004 and CIP-005 repost
  - CIP-002 through CIP-012 and CIP-013 Technical Rationale Posting
- **Standards Affected:** CIP-002 through CIP-011, and CIP-013
  - Standards with substantial changes: CIP-005, CIP-007, and CIP-010
  - Conforming changes: CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, and CIP-013

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

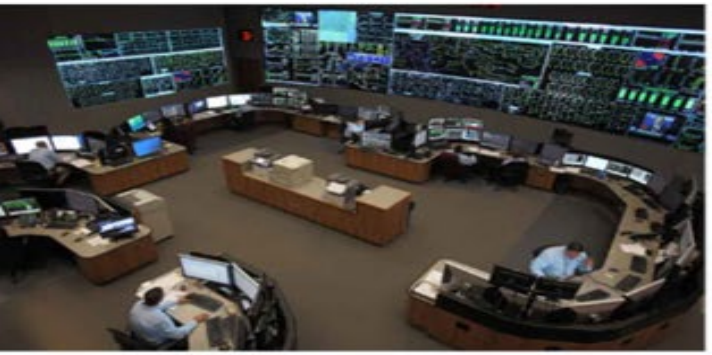
Initial Survey

Providing Feedback

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

Join at Slido.com #2016-02D2

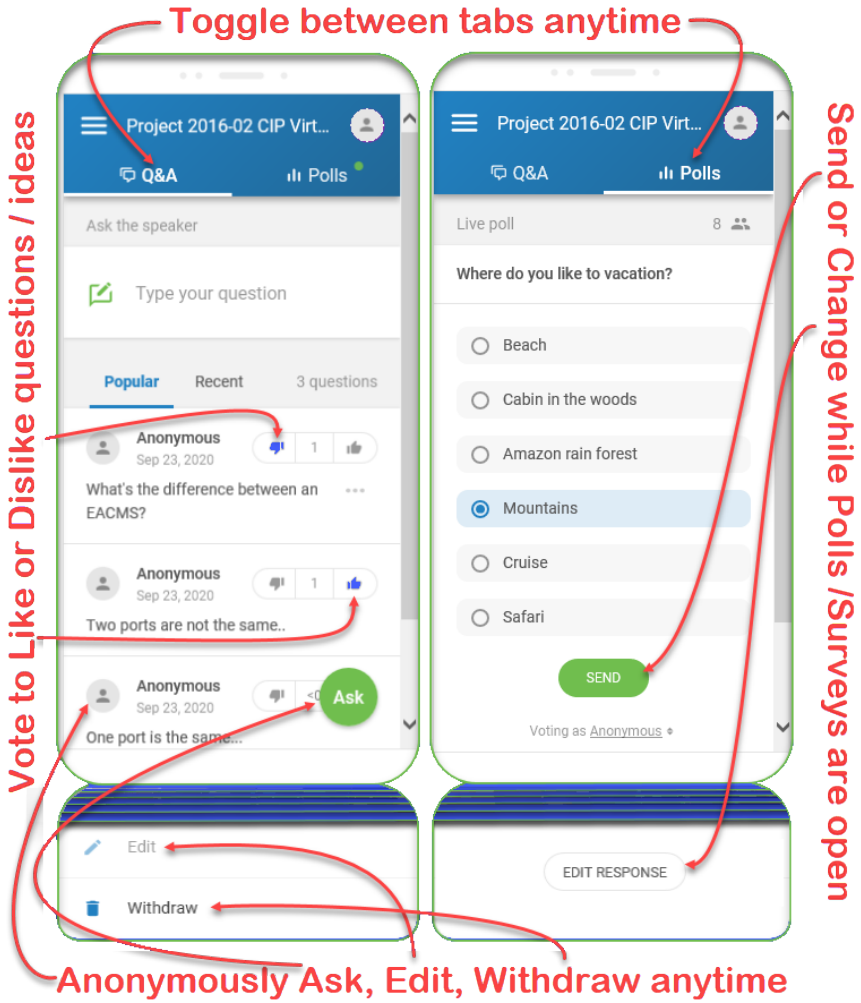
RELIABILITY | RESILIENCE | SECURITY

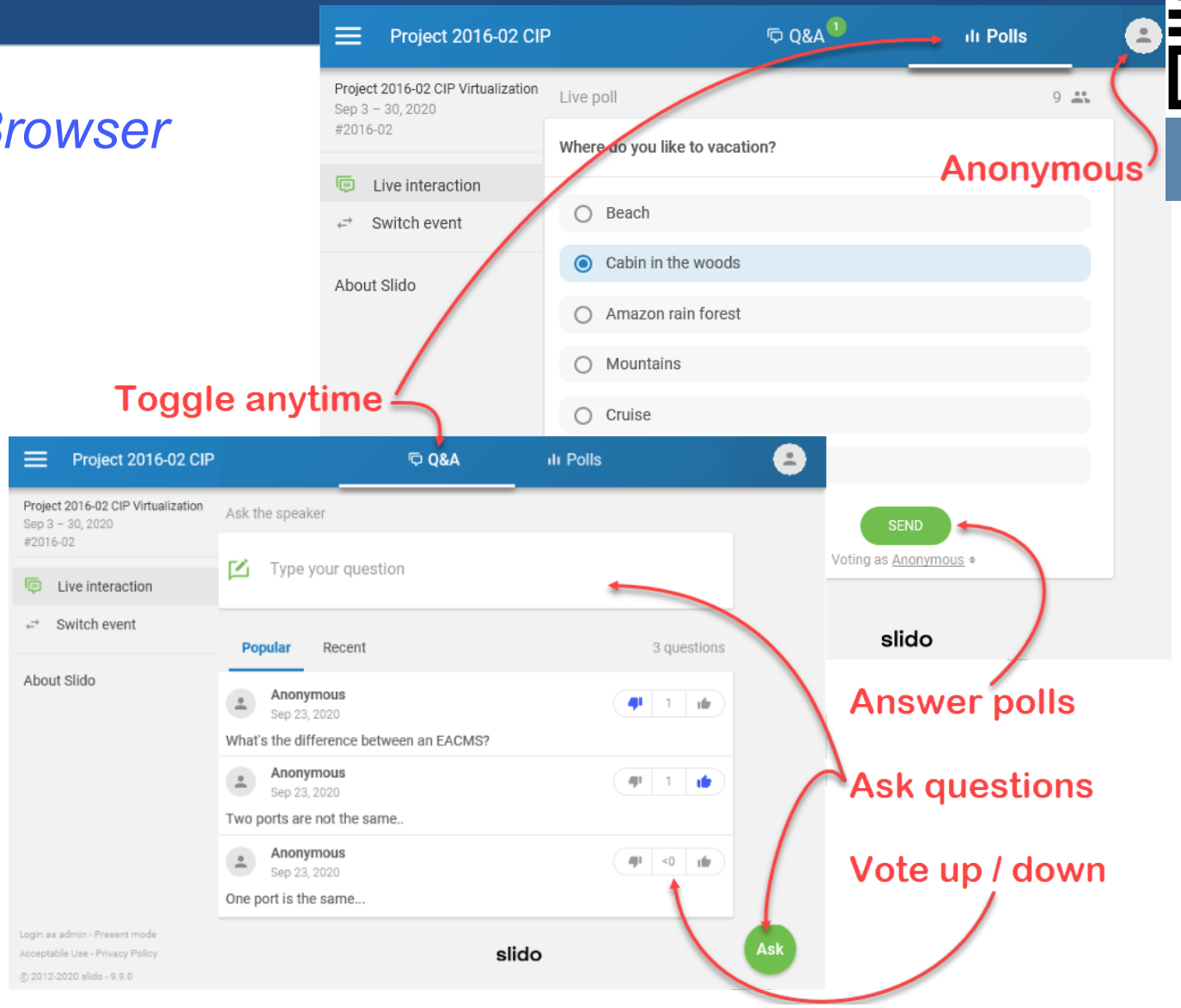



Slido Features and Navigation

Join: slido.com
#2016-02-D2

Use the Mobile App or a Browser





Audience Poll

Join: slido.com
#2016-02-D2

- What role do you have in your organization?
- What type of entity are you?

Scope of Changes from SAR

Join: slido.com
#2016-02-D2

- V5TAG Items
  - Virtualization
    - "The CIP V5 standards do not specifically address virtualization. Because of the increasing use of virtualization in industrial control system environments, V5TAG asked that the SDT consider the CIP V5 standards and the associated definitions regarding permitted architecture and the security risks of virtualization technologies."
  - Clarification of ERC/IRA
    - "V5TAG recommends improving clarity within the concepts and requirements concerning Electronic Security Perimeters (ESP), External Routable Connectivity (ERC), and Interactive Remote Access (IRA) "
- CIP Exceptional Circumstances (CEC)
  - "…the SDT will review and address the CIP V5 requirements for CIP Exceptional Circumstances exceptions."
- Standard Template Conformity
  - Removal of Guidelines and Technical Basis (GTB) and Background sections to Technical Rationale documents.

Introduction

Join: slido.com
#2016-02-D2

- Journey from Draft 1 to Draft 2
  - Draft 1 initial ballot and comment period from Jan 22 - March 22, 2021
  - 91 sets of responses across 133 companies
  - SDT has made several substantial changes
  - Draft 2 posted on June 30th

What We Heard From Draft 1

Join: slido.com
#2016-02-D2

- Simplify Applicability/Simplify for existing virtualized environments
- Logical Isolation definition/ESP Reinstatement
- ERC and IRA – serial only scenarios
- Define Cyber System
- Baselines
- Additional CIP-010 Issues
- System Hardening / Affinity

Draft 2 Redlines and "-Y" Versions

Join: slido.com
#2016-02-D2

- The redlines posted for Draft 2 show the deltas from Draft 1, not from currently enforced or approved versions.
  - Some of the redlines are returning language to currently enforced versions, such as changing all the forms of 'logical isolation' back to ESP.
- CIP-003-Y, CIP-004-Y, and CIP-011-Y posted in Draft 2.
  - Project 2020-03, Supply Chain Low Impact Revisions, is working on CIP-003
  - Project 2019-02, BCSI Access Mgt, passed Final Ballot with CIP-004 and CIP-011 (June 11)

Join: slido.com
#2016-02-D2

Theme 1

Simplify Applicability

Simplify Applicability

Join: slido.com
#2016-02-D2

Applicable Systems
Physical Access Control Systems (PACS) associated with: • High Impact ~~BES Cyber Systems~~BCS~~,~~ ~~or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact ~~BES Cyber Systems~~BCS~~,~~ ~~or~~ • Medium Impact ~~BES Cyber Systems~~BCS with ~~External Routable Connectivity~~ERC • SCI hosting High Impact BCS or their associated EACMS or PCA; or • SCI with ERC hosting Medium Impact BCS or their associated EACMS or PCA SCI hosting PACS associated with High Impact BCS SCI hosting PACS associated with Medium Impact BCS with ERC

Simplification Enablers

Join: slido.com
#2016-02-D2

- Definition changes
  - BES Cyber System (BCS)
  - Shared Cyber Infrastructure (SCI)
  - Management Interface
- CIP-002 changes
- Created flexible SCI scenarios
- “SCI identified independently supporting an Applicable System above”

BES Cyber System Definition

Join: slido.com
#2016-02-D2

BES Cyber System (BCS)

One or more BES Cyber Assets logically grouped by a Responsible Entity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.

Shared Cyber Infrastructure Definition

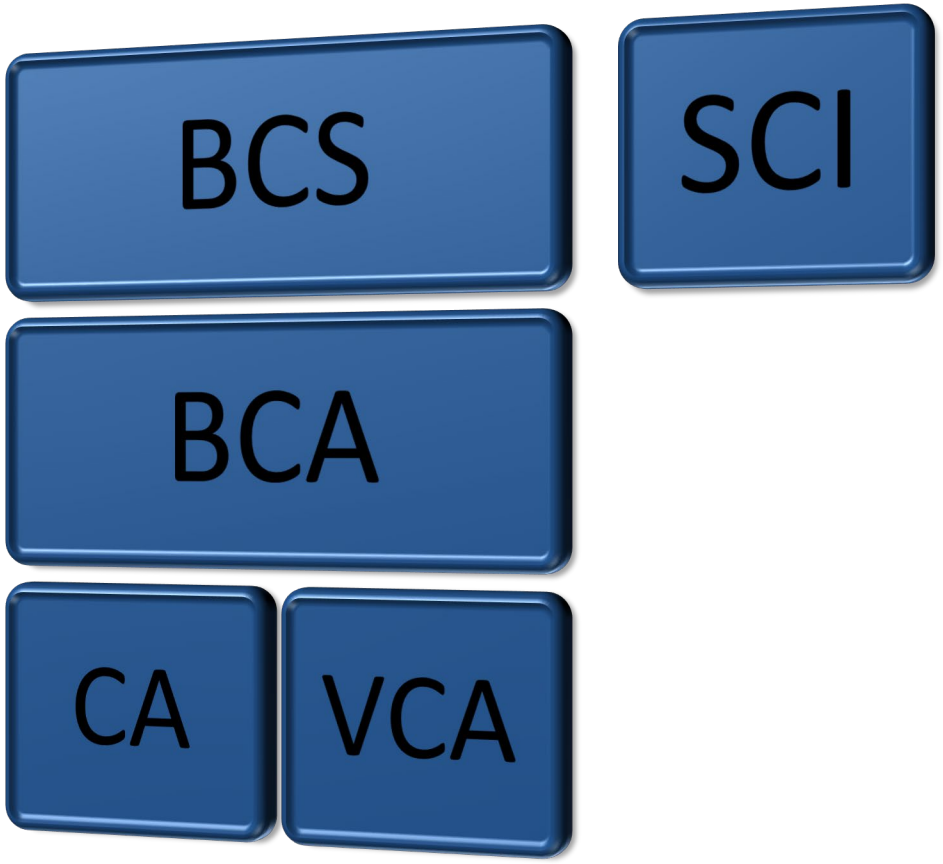
Join: slido.com
#2016-02-D2

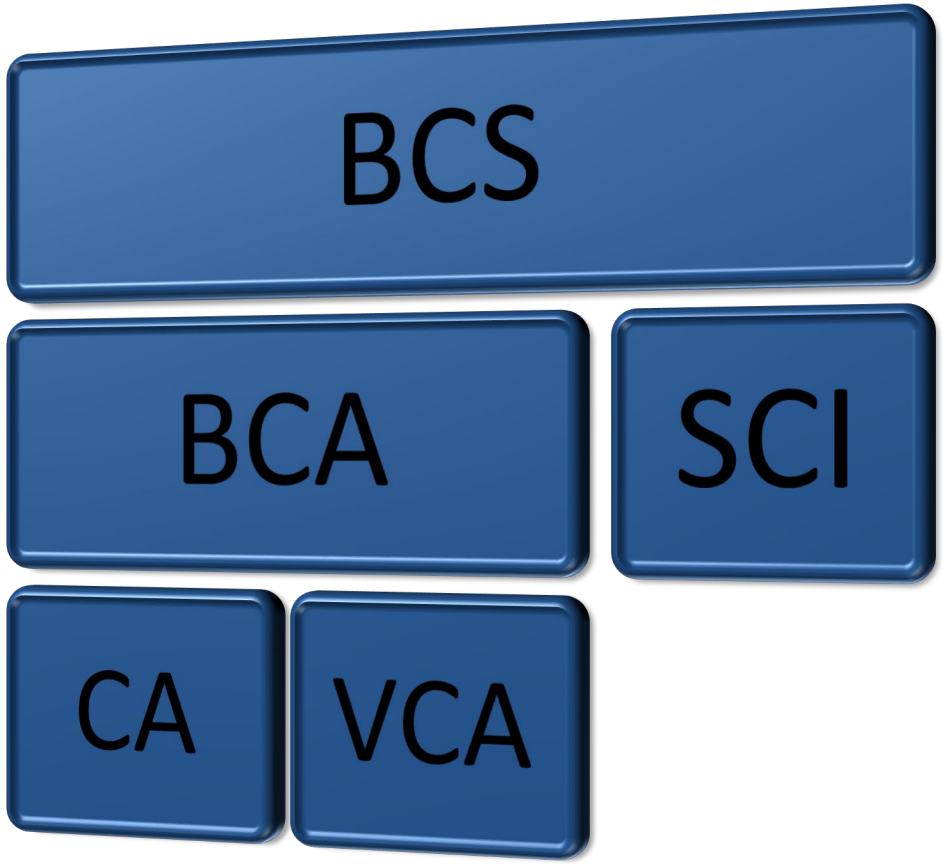
Shared Cyber Infrastructure (SCI)

- One or more programmable electronic devices, including the software and Management Interfaces, that share:
  - CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or
  - storage resources with any part of a BES Cyber System or their associated EACMS or PACS
- Each SCI is either:
  - included in one or more BES Cyber Systems, EACMS, or PACS; or
  - identified independently.
- SCI does not include the supported VCA or CA with which it shares its resources.

Definition Relationship Options

Join: slido.com
#2016-02-D2





CIP-002 Example

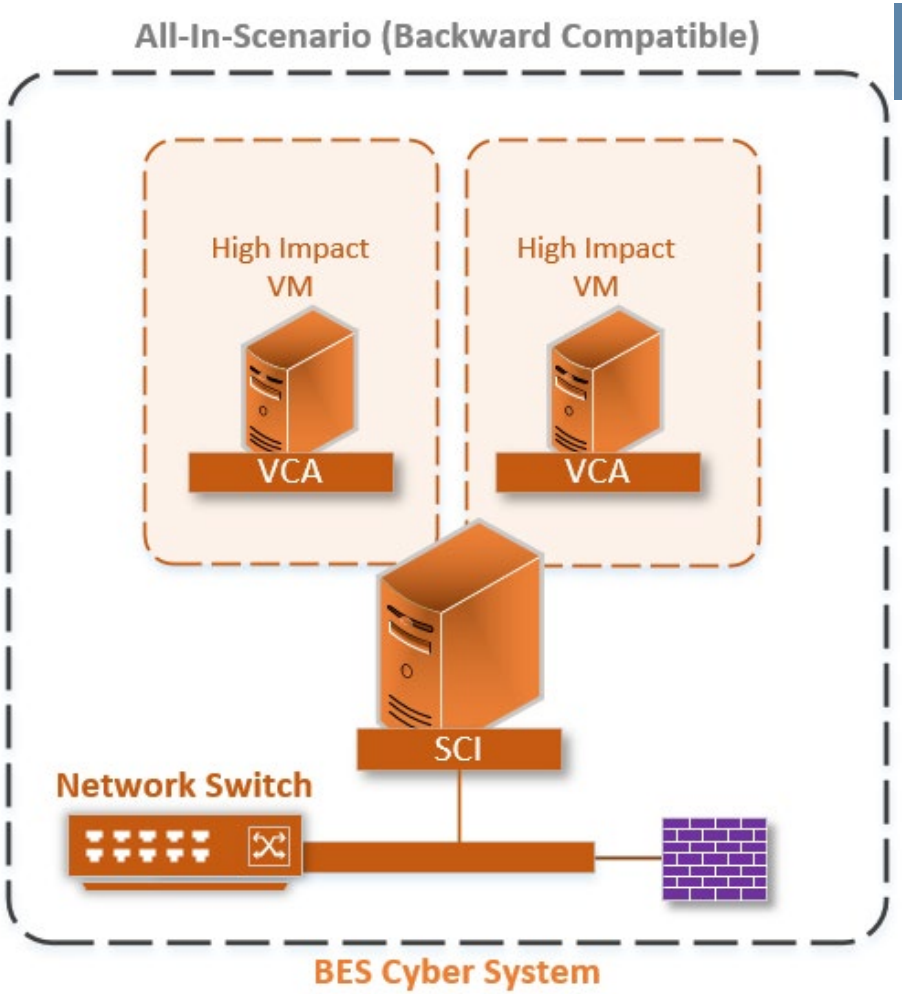
Join: slido.com
#2016-02-D2

- 1.1. Per Attachment 1, Section 1, identify each BES Cyber System as either of the following, if any, at each asset;
  - A high impact BCS including any supporting SCI as part of the BCS; or
  - A high impact BCS and independent SCI supporting any part of the high impact BCS or its associated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS) or Protected Cyber Assets (PCAs).

"All-In" Scenario

Join: slido.com
#2016-02-D2

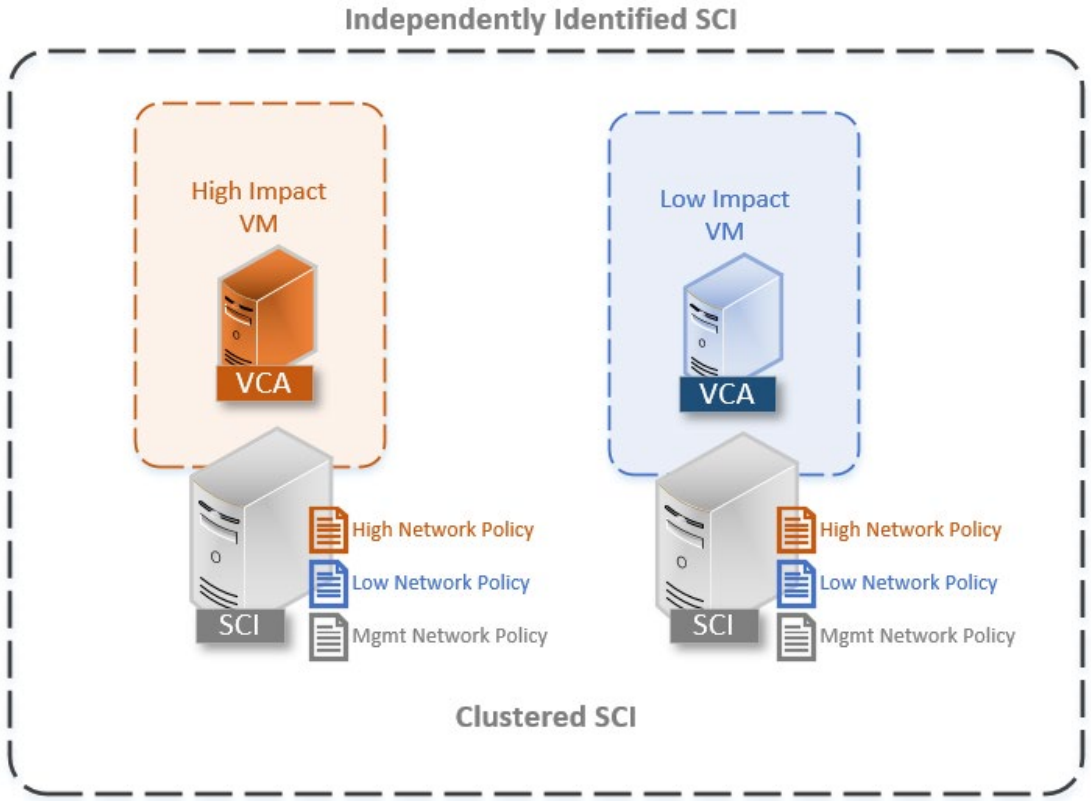
- The SCI is part of the BCS
- Probably what you're doing today
- Why choose this? SIMPLIFICATION



"Identified Independently" Scenario

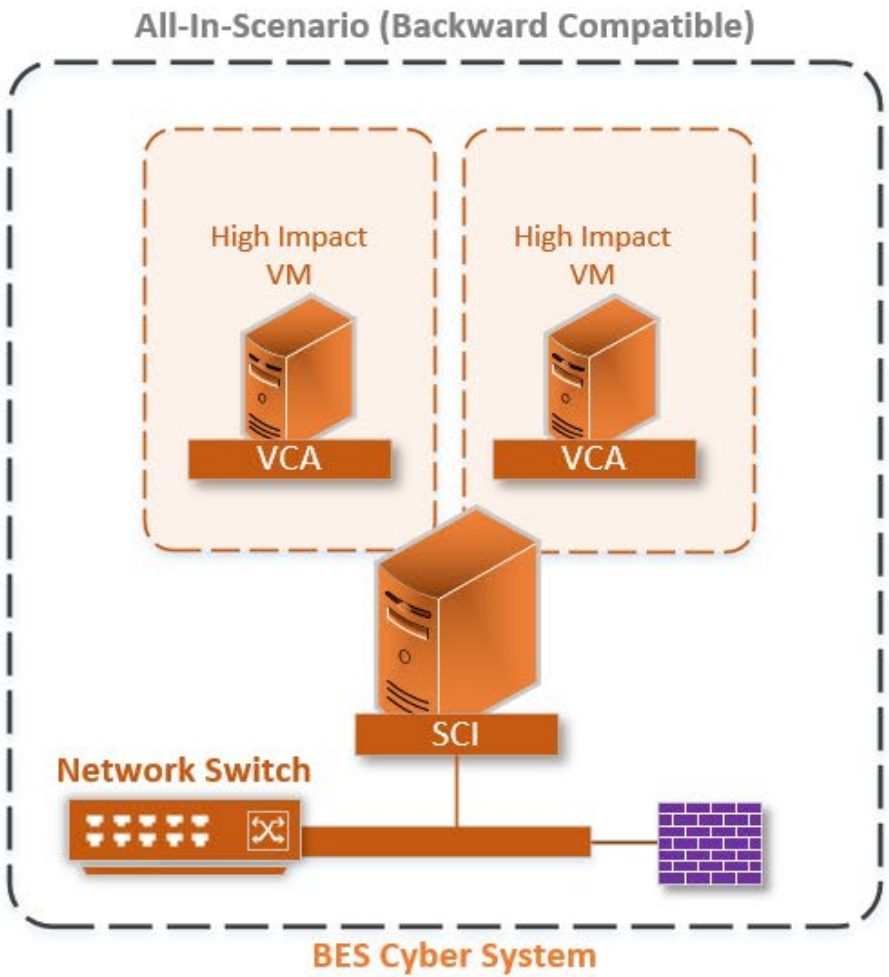
Join: slido.com
#2016-02-D2

- SCI is NOT part of the BCS, but its own independently identified entity
- Hosted BCS identified separately
- Why choose this? FLEXIBILITY

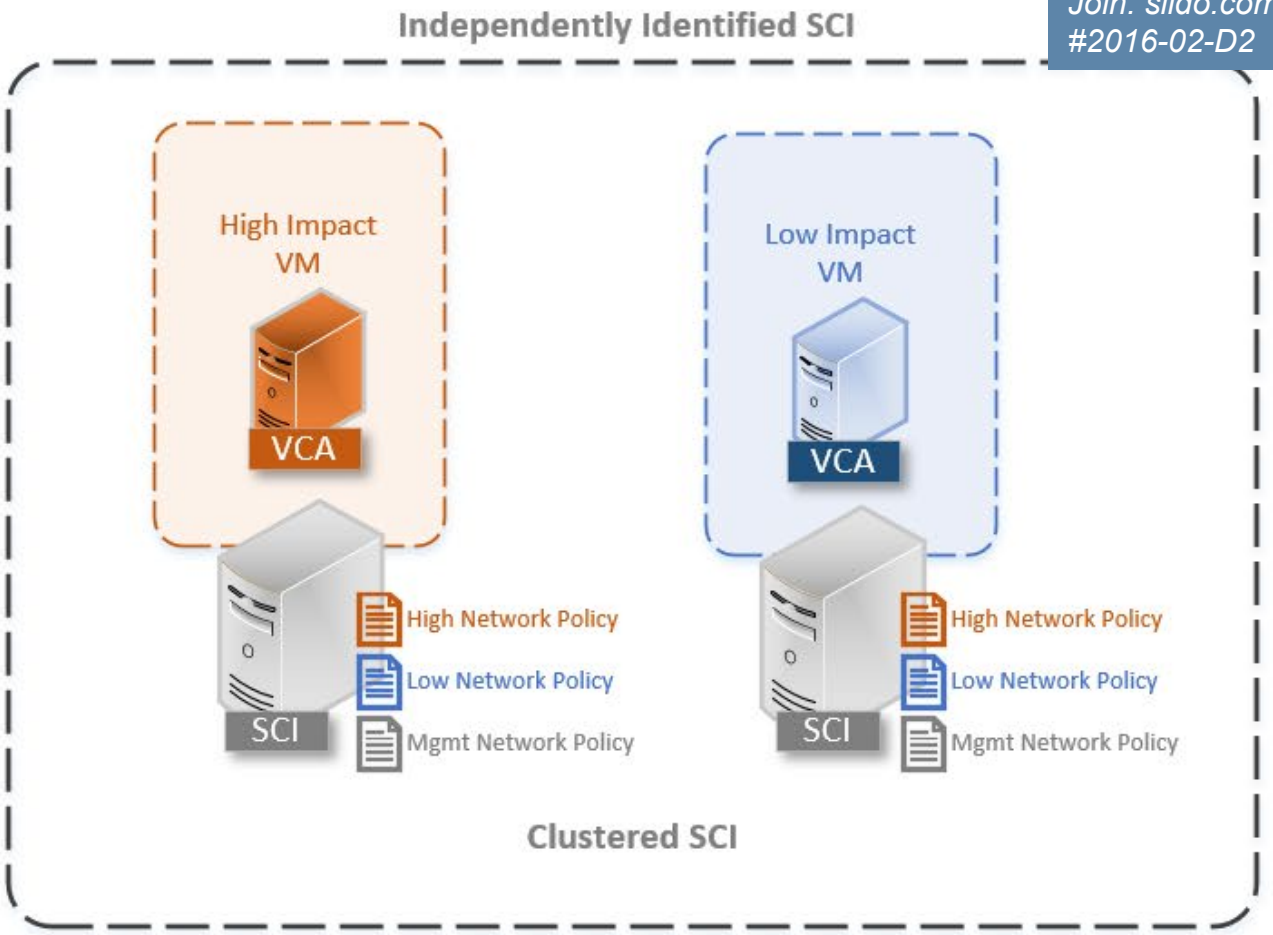


Flexible Scenarios

Join: slido.com
#2016-02-D2



OR



Management Interface

Join: slido.com
#2016-02-D2

- A user interface, logical interface, or dedicated physical port that is used to:
  - Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or
  - Provide lights-out management capabilities; or
  - Configure an Electronic Security Perimeter;

excluding physical user interfaces (e.g., power switch, touch panel, etc.)

Management Interface Example Usage

Join: slido.com
#2016-02-D2

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	
1.2	SCI identified independently supporting an Applicable System from Part 1.1. EACMS that enforces an ESP for the Applicable Systems in Part 1.1.	Permit only needed and controlled communications to and from Management Interfaces, and deny all other communications.	Exam but ar that ir syster and E •

CIP-005-8 Table R1 – ~~Electronic Security Perimeter(s)Logical Isolation~~			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	SCI identified independently ~~hosting~~supporting an Applicable System from Part 1.1. ~~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 enforces an ESP for the Applicable Systems in Part 1.1. ~~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~~deny all other communications. ~~1.2.3. Deny communications from BCS and their associated PCAs to the Management Interfaces and Management Systems, per system capability.~~	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems that enforce access control and ESP~~logical isolation~~ such as: • Logical~~ly isolated out-of-band~~ network infrastructure configuration (ACL, VLAN, VXLAN, MPLS, VRF, multi-context, or multi-tenant environment). • Physically isolated out-of-band network for dedicated Management Interfaces, or~~Management Modules, or Management Systems~~ • SCI configuration or policies showing the isolation of the management plane resources (hypervisor, fabric, back-plane, or SAN configuration).

Join: slido.com
#2016-02-D2

Theme 2

Logical Isolation Definition / Reinstate ESP

Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

- Draft #1 Feedback for Theme 2 – What we heard!
  - Logical Isolation needs to be defined, not well known enough in the industry.
  - Bring back the ESP, this concept is well understood.
  - Too much change - removing the ESP definition causes a lot of unnecessary change and confusion.
  - Firewalls in a host operating system are not equivalent to more advanced firewalls in virtualized environments. Host-based firewalls that only protect the asset they reside on shouldn't be good enough.

Join: slido.com #2016-02-D2

- SDT Response - Changes from Draft 1 to Draft 2
  - Undefined “logical isolation” term has been removed from all of the standards.
  - In order to maintain backward compatibility, we have re-instated a *new version* of the ESP definition.
  - The *new version* of the ESP definition concept relies on EACMS instead of the EAP to preserve backward and forward compatibility with perimeter-based models as well as zero trust methodology.
  - Updated EAP definition is now an example of a policy enforcement point and is only referenced in measures.
  - Clarifications provided for host-based firewalls have been added.

Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

Definition	Approved	2016-02 Draft 2 Proposed
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.

Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

Definition	Approved	2016-02 Draft 2 Proposed
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	A policy enforcement point or a Cyber Asset interface that allows routable communication to and from the BES Cyber System within an Electronic Security Perimeter.

Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as:

- Electronic Access Point (EAP) configuration or policies;
- Network infrastructure

Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

Definition	Approved	2016-02 Draft 2 Proposed
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.

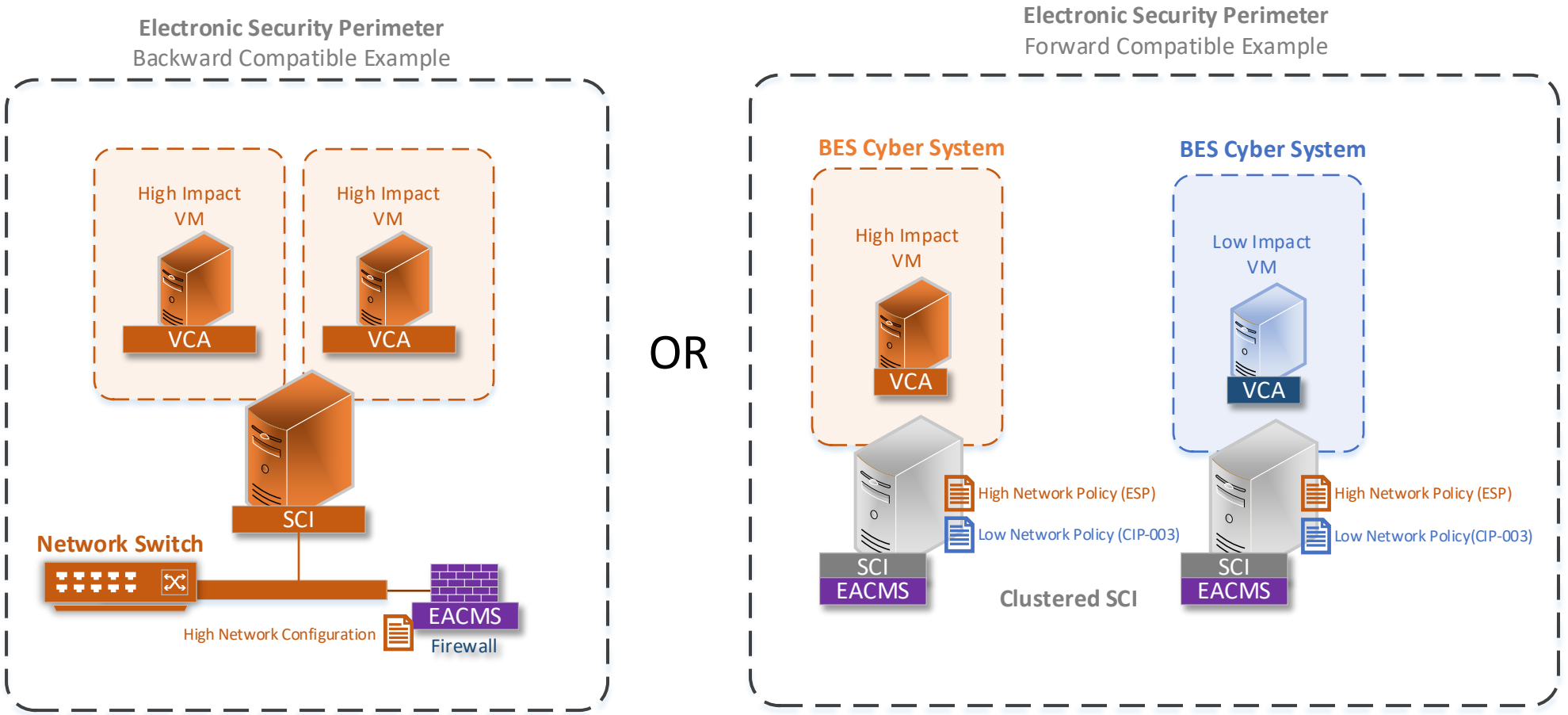
Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

CIP-005-8 Table R1 – Electronic Security Perimeter(s)			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BCS and their associated Protected Cyber Asset (PCA) Medium Impact BCS and their associated PCA	Applicable Systems connected to a network via a routable protocol must be protected by an ESP that permits only needed communications and denies all other communications, excluding time-sensitive protection or control functions between intelligent electronic devices. Host-based firewalls that only protect the host on which they reside are not a sufficient control to meet this requirement.	Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as: • Electronic Access Point (EAP) configuration or policies; • 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 ESP and documents the business need.

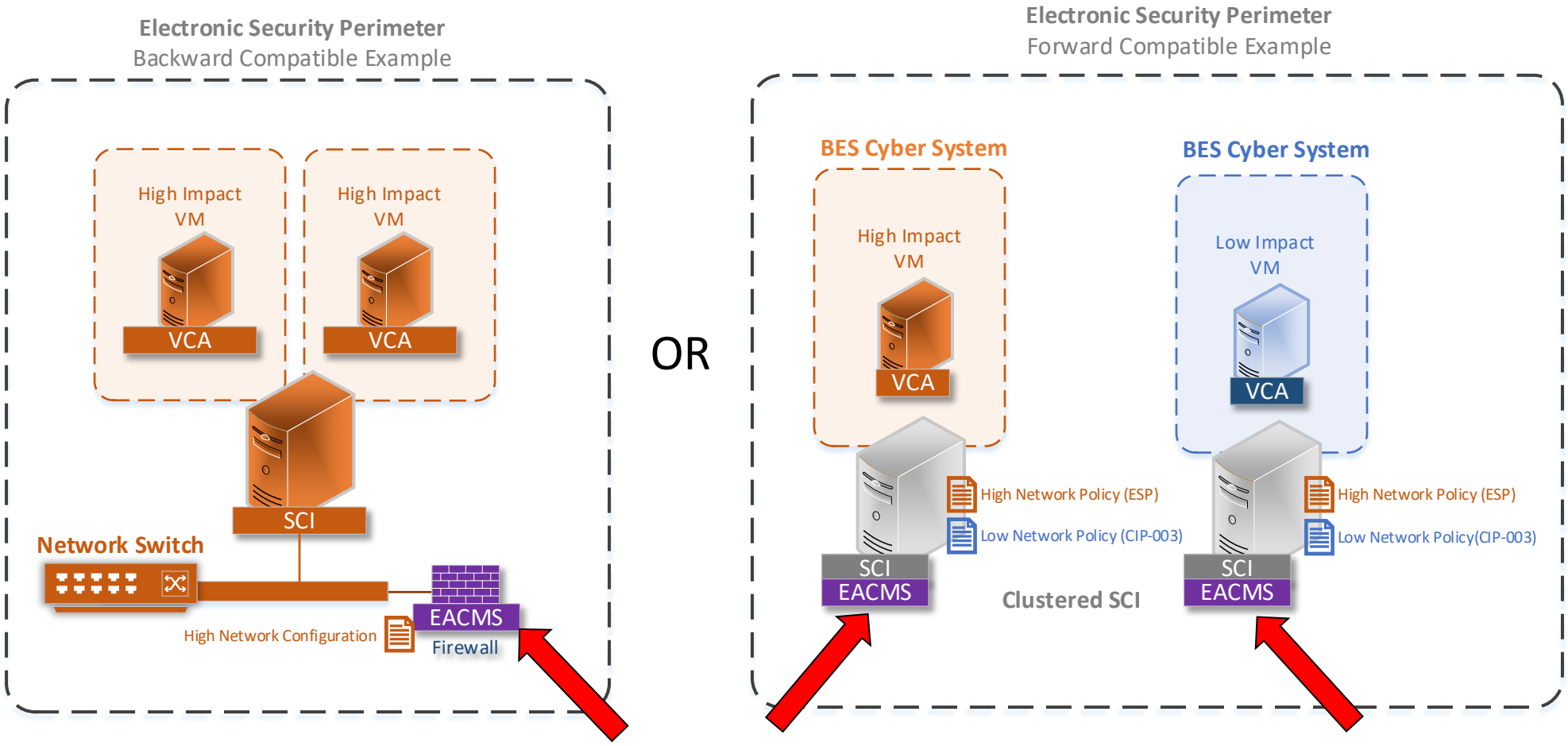
Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2



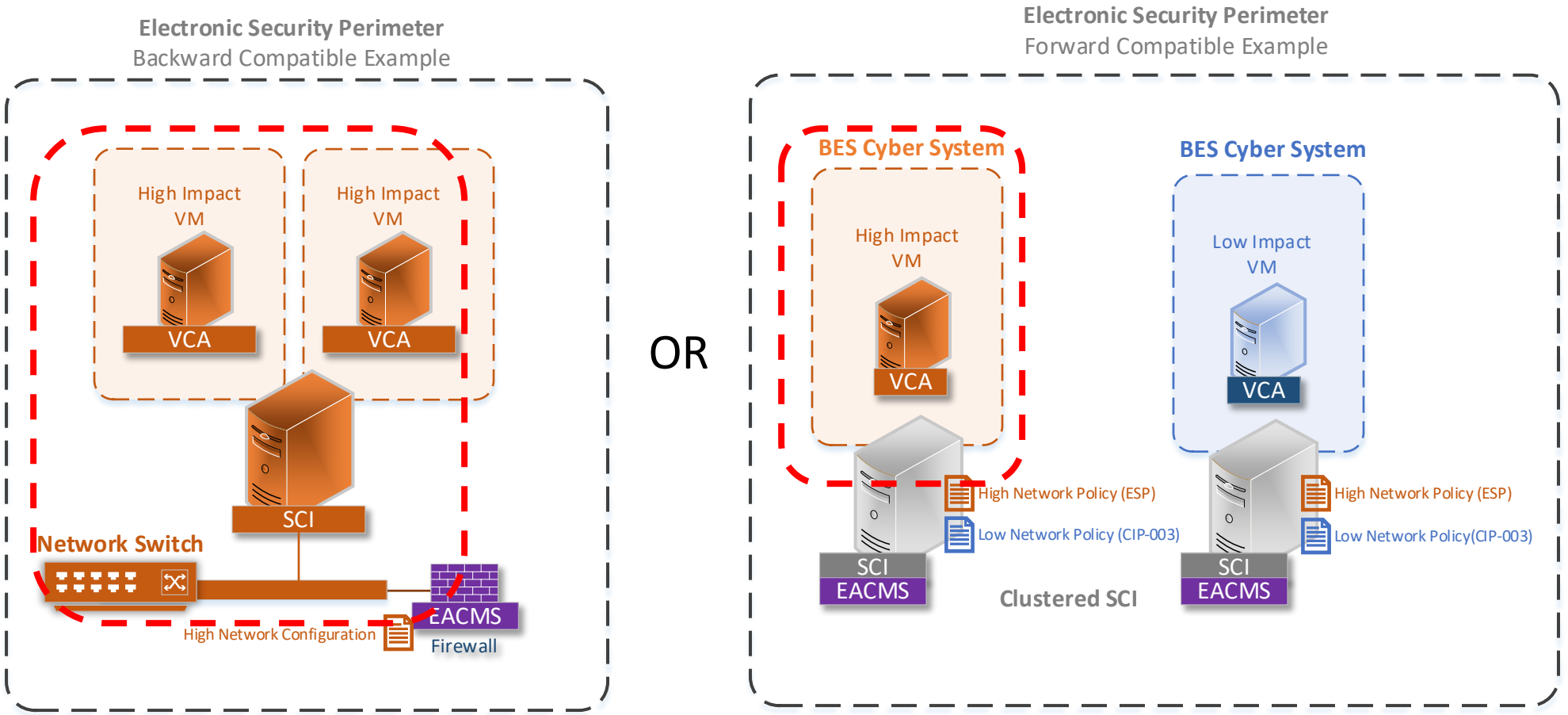
Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2



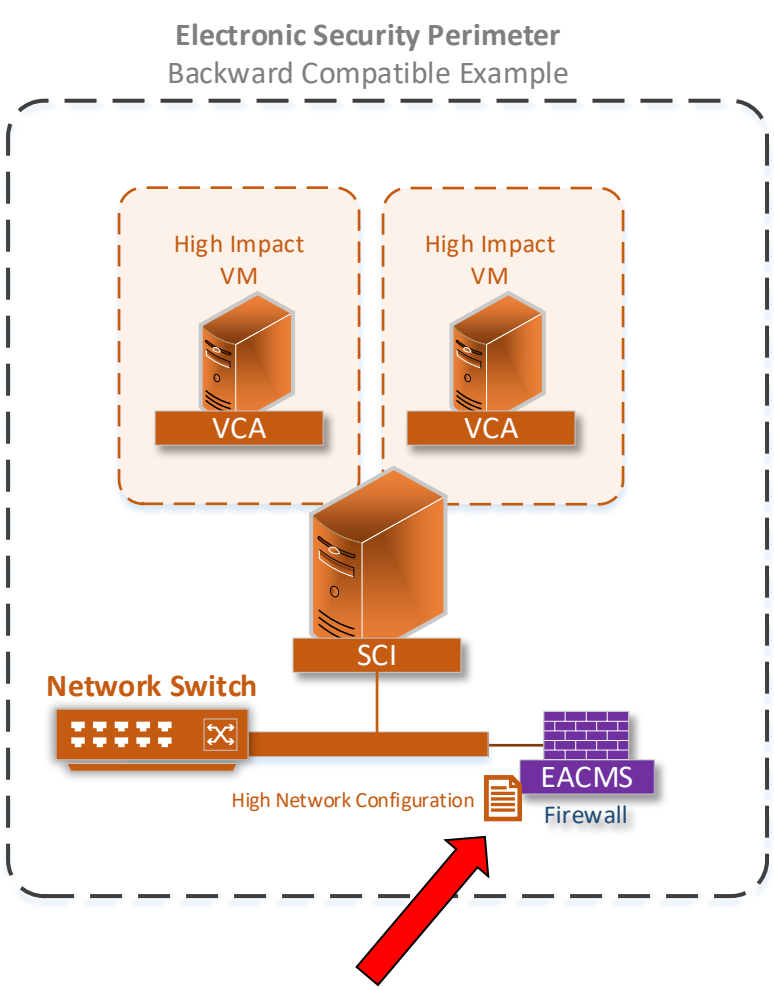
Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

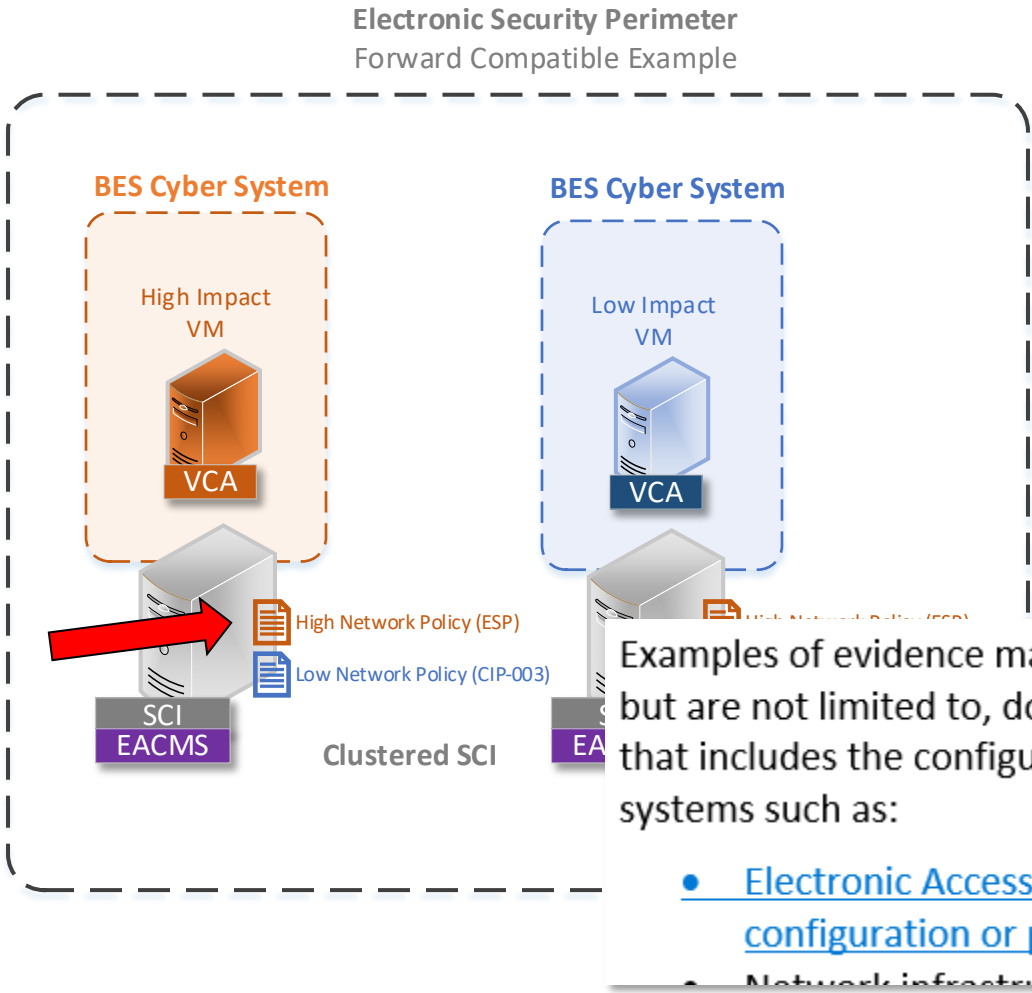


Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2



OR

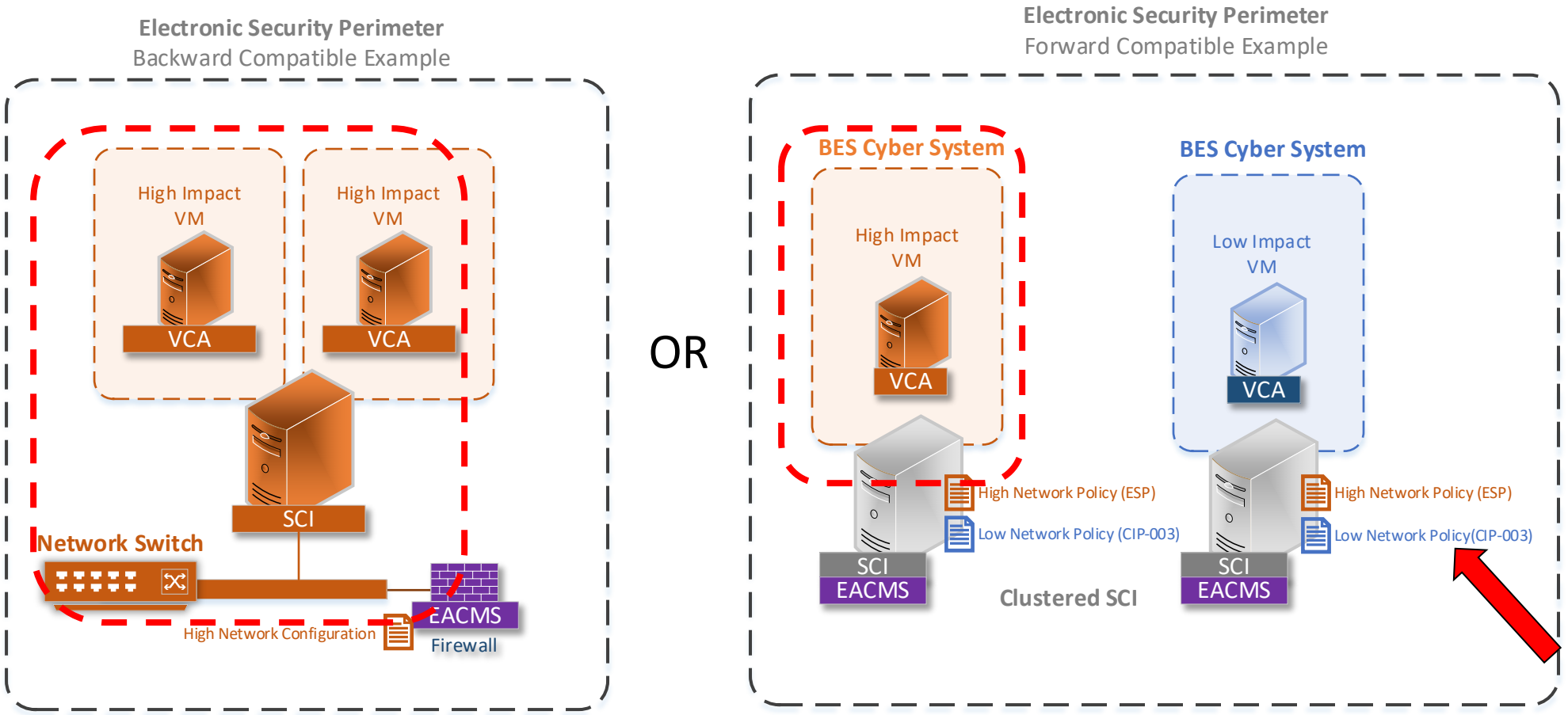


Examples of evidence may include, but are not limited to, documentation that includes the configuration of systems such as:

- Electronic Access Point (EAP) configuration or policies;
- Network infrastructure

Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2



Theme 2 – Def Logical Isolation / Reinstate the ESP

Join: slido.com
#2016-02-D2

- Theme 2 Take-aways
  - The ESP has been reinstated to simplify the draft and to maintain **forward** and **backward** compatibility.
  - ESP, EAP, and EACMS definitions updated to address feedback and continue to allow forward and backward compatibility with fewer changes.
  - Clarifications provided for host-based firewalls have been added to address security concerns.
  - ESP is now a real “electronic security perimeter” and not a “network perimeter”
  - The amount of change in required to achieve the same goals in draft 2 are significantly reduced from draft 1.

Join: slido.com
#2016-02-D2

Theme 3

External Routable Connectivity / Interactive Remote Access

External Routable Connectivity

Join: slido.com
#2016-02-D2

- In Draft 1, the ERC wording was updated to reflect the removal of ESP

- With the reinstatement of the ESP definition, the majority of the approved language could be restored, however …….

The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System ~~that is outside of its associated Electronic Security Perimeter~~ via a bi-directional routable protocol connection.

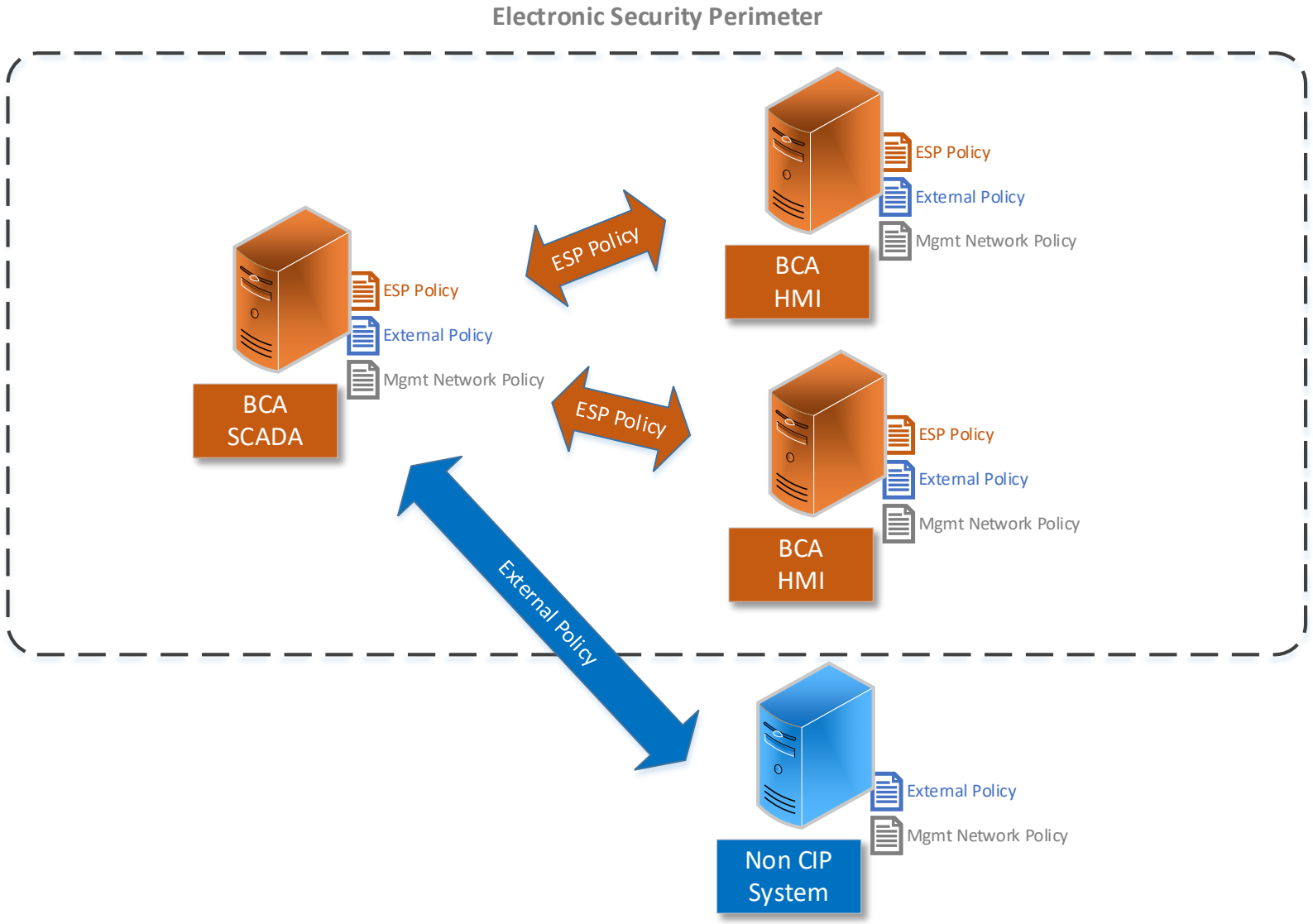
External Routable Connectivity

Join: slido.com
#2016-02-D2

- Old definition ?…
  - *The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.*
- The definition of ESP was expanded to incorporate zero trust environments where all network connectivity is controlled by configuration or policies
- In a zero trust environment, an entity may have many policies that govern network connectivity to a BES Cyber System
- The entity must define the subset of those network connectivity policies that form the Electronic Security Perimeter for that BCS

External Routable Connectivity

Join: slido.com
#2016-02-D2



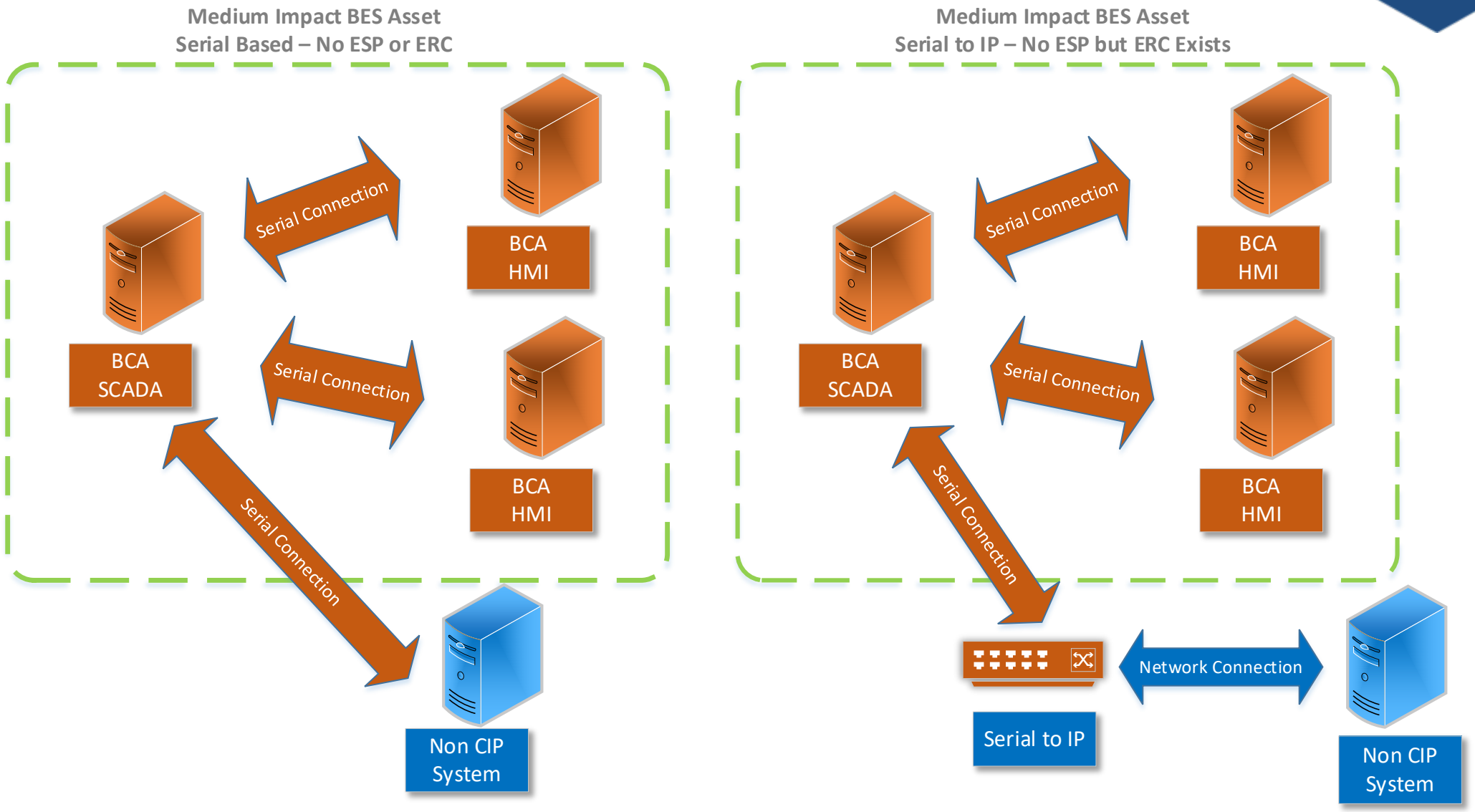
External Routable Connectivity

Join: slido.com
#2016-02-D2

- Problem – Serial based systems don't have an ESP, however serial/IP conversion could allow uncontrolled network access
- The SDT looked at how the ERC scoping mechanism was being used in the other requirements and determined that the risk being addressed was network connectivity from outside the entity's asset
- Asset is already used as a scoping mechanism for low impact BES
- *Solution*
  - *The ability* ***to communicate to a CIP System using*** ~~*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*~~ ***from outside the asset containing the CIP System.***

External Routable Connectivity

Join: slido.com
#2016-02-D2



Interactive Remote Access

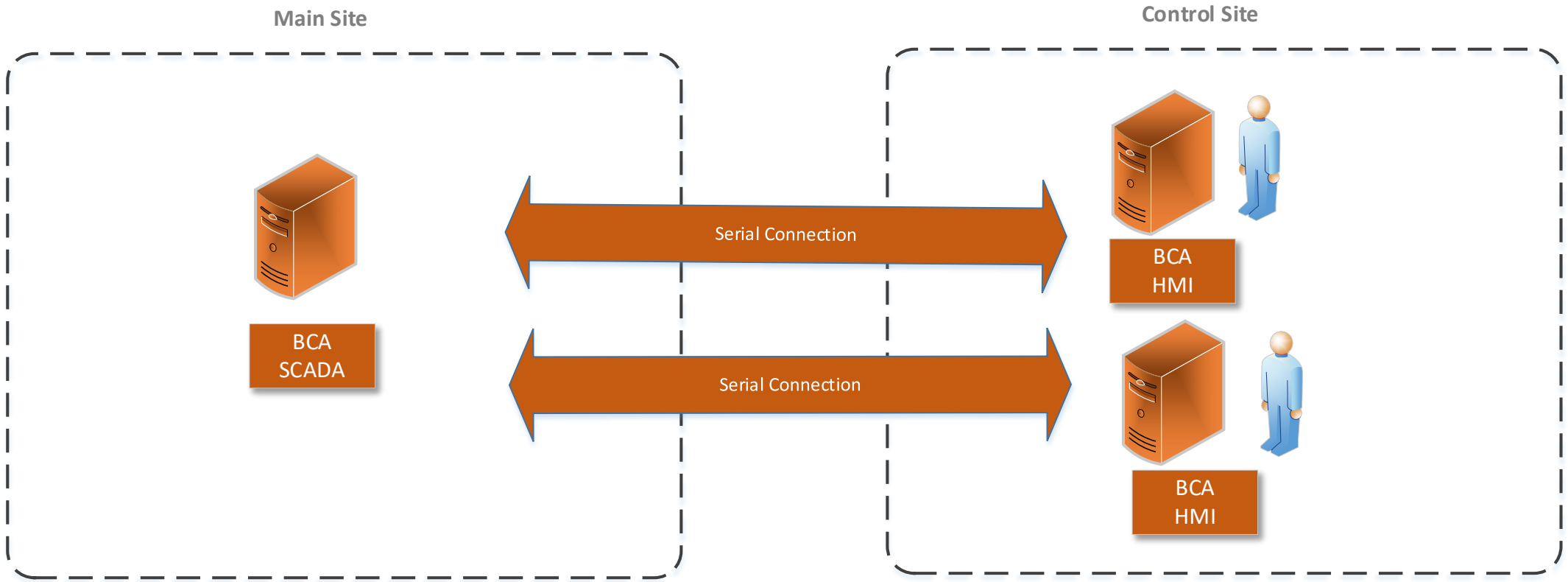
Join: slido.com
#2016-02-D2

- In Draft 1, the wording was updated to only describe “what it is” and remove the other language (for inclusion into the requirements proper)
  - 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~~.

Interactive Remote Access

Join: slido.com
#2016-02-D2

- Problems…… In the case of an entirely serial based SCADA system, operator HMI consoles would fall within that IRA definition, however no CIP-005 R2 controls can be applied and what is a "remote access client"?



Interactive Remote Access

Join: slido.com
#2016-02-D2

- The SDT determined that the IRA risks that needed to be addressed were serial to IP conversion (where CIP-005 R2 type controls could be effectively applied) as well as access to the control of the SCI configuration and the ESP
- For Draft 2, the following needed to be addressed
  - ESP - reinstated
  - serial to IP conversion
  - Access to Management Interfaces that control SCI
  - Access to Management Interfaces that control the ESP

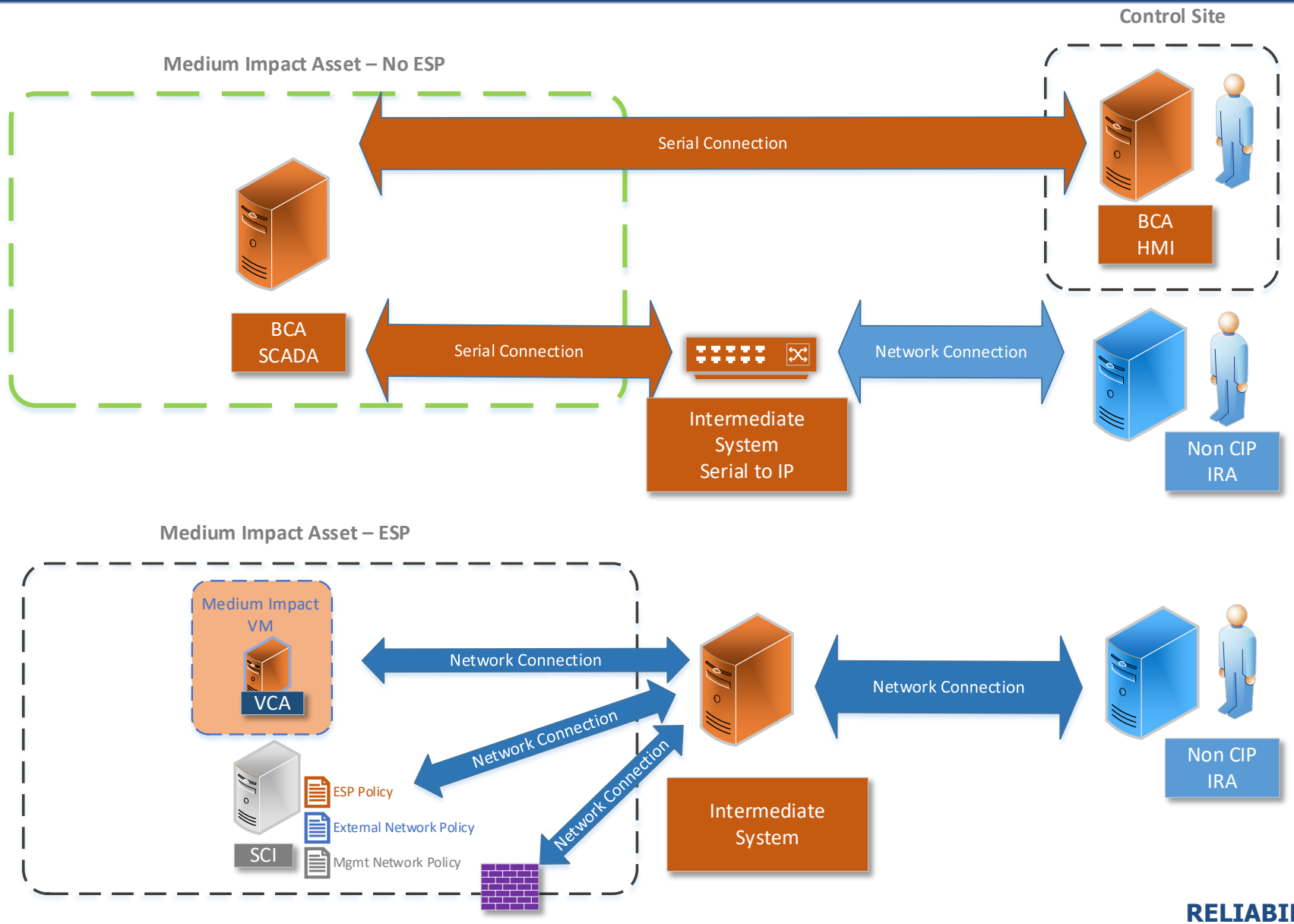
Interactive Remote Access

Join: slido.com
#2016-02-D2

- User-initiated real-time access by a person ~~employing a remote access client~~ from outside of the Responsible Entity's Electronic Security Perimeters (ESP) using a routable protocol:
  - to a Cyber System within an ESP;
  - through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter;
  - to Management Interfaces of Shared Cyber Infrastructure; or
  - to Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP.

Interactive Remote Access

Join: slido.com
#2016-02-D2



Join: slido.com
#2016-02-D2

Theme 4
Use of Cyber System and CIP System

Cyber System

Join: slido.com
#2016-02-D2

- "Cyber Asset" is used in many requirements though out the standards.
- In order to maintain backwards compatibility, the SDT chose to add the definition of "Virtual Cyber Asset".
- For ease of interpretation, "cyber system" was used in Draft 1 in place "Cyber Asset, Virtual Cyber Asset or Shared Cyber Infrastructure"
- For Draft 2, the SDT has accepted the request to formally define "Cyber System" as
  - A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

CIP System

Join: slido.com
#2016-02-D2

- In order to simplify the requirement language ,the SDT chose to add the definition of “CIP System” in Draft 2 as follows:
  - A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.
- This simplification also allows the use of “non-CIP System” in the requirements
- “CIP System” is used in the ERC definition
- “non-CIP System” is used in CIP-007-7-Requirement R1.3 and CIP-010-5 Requirement R1.2.2

Join: slido.com
#2016-02-D2

Theme 5

Baselines

Baselines & CIP-010

Join: slido.com
#2016-02-D2

- Industry comments on security objective served by Baseline
  - SDT chose to include baseline in Measures to provide reference
  - Objective of R1 remains the same

Join: slido.com
#2016-02-D2

Additional CIP-010 issues addressed:

TCAs

Disk Images & Security Patches

Prior to…

TCAs - VCA on a TCA?

Join: slido.com
#2016-02-D2

What if my TCA has a VM to run an old piece of software, since the TCA Definition now includes VCAs.

Clarified in the TCA Definition:

“Virtual machines hosted on a physical TCA can be treated as software on that physical TCA.”

It’s software

Attachment 1 Sections 1.2, 1.3 & 2.2 refer to:

- controls to maintain the known good state…

Join: slido.com
#2016-02-D2

Change Authorization…

Disk Images & Security Patches!

Change Authorization – Disk Images & Security Patches

Join: slido.com
#2016-02-D2

CIP-010-5 Table R1 – Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems (BCS) and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BCS and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI identified independently supporting an Applicable System above	Authorize changes to: 1.1.1. Operating system(s) (OS); or firmware where no independent OS exists; or images used to derive operating systems; or firmware; 1.1.2. Commercially available or open-source application software, including application containers; 1.1.3. Custom software installed, including-applications containers; and 1.1.4. Any logical network accessible ports (or services if unable to determine ports). ~~1.1.5. Any security pathes applied~~	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change. • Documentation of authorization for cyber security patch implementation.

Join: slido.com
#2016-02-D2

Prior to:

adding.. to a production environment

-> logically Connecting

-> Becoming…

Prior to… Response to comments

Join: slido.com
#2016-02-D2

CIP-010-5 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BCS and their associated: 1. EACMS; and 2. PCA SCI identified independently supporting an Applicable System above	Prior to becoming a new Applicable System, perform an active vulnerability assessment of the new Applicable System, except for: • like replacements of the same type of Cyber System with a configuration of the previous or other existing Cyber System; or • CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to: • The output of any tools used to perform the assessment, or • Reports from automated assessment and remediation mechanisms (remediation VLANs, quarantine systems, 802.1x mechanisms that assess and remediate, etc.) that documents the date of the assessment performed prior to becoming a new Applicable System .

Join: slido.com
#2016-02-D2

System Hardening

&

Host Affinity

System Hardening

Join: slido.com
#2016-02-D2

CIP-007-7 Table R1–System Hardening			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	SCI identified independently supporting: • High Impact BCS and their associated: 1. EACMS 2. PACS; and 3. PCA • Medium Impact BCS with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prevent the sharing of the CPU and memory of Management Interfaces of SCI with non-CIP Systems.	Examples of evidence may include, but is not limited to, documentation of the configuration showing that the CPU and memory cannot be shared with non-CIP Systems.

Host Affinity

Join: slido.com
#2016-02-D2

However… did NOT alter CIP-005 R2 Part 2.6 in response to Comments

Options suggested were to allow sharing CPU and memory of Intermediate Systems with:

- BCS, or
- non-CIP Systems

The security risk associated in these scenarios is too great.

NOTE: Left in CIP-005 R2 for Intermediate System consistency (but could easily fit within CIP-007 R1)

Implementation Plan

Join: slido.com
#2016-02-D2

- 24 month implementation plan with provisions for early adoption.
- Early adoption – Entity and Regional Agreement to implement
  - Permits Registered Entities to work directly with their Region(s) to identify a date in advance of the 24 months to be compliant with the virtualization-enabled standards.
  - Responsible Entities must continue to comply with current enforceable CIP Standards and Definitions until that agreed upon Early Adoption date.

Resources

Join: slido.com
#2016-02-D1a

- 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-D2

- 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:
  - 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-D2

Questions and Answers