



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Virtualization, Technology Innovation, and NERC CIP

CIP Standard Drafting Team
June 29, 2018

RELIABILITY | ACCOUNTABILITY



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.

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities.

- Virtualization Poll
- V5TAG Transition Issues
- Virtualization Questions
- CIP SDT Course of Action (left/right path)
- Next Steps
- Q&A



- Moving towards a fuller Cyber Systems approach
- Modify requirements to be more objective based and technology neutral
- Backwards Compatibility



- Does your entity use virtualization within the BES Cyber System environment?
 - Yes
 - No
 - Don't know
 - I am just here to listen

- Is your entity having any issues using virtualization under the current CIP Reliability Standards?
 - Yes
 - No
 - Don't know
 - I am just here to listen

- Clarify “programmable”
- “Viewing BCAs too broadly can lead to many thousands of devices in the typical utility becoming an administrative burden for which few if any cyber security controls can actually be applied or where there is limited associated cyber security risk. Vast amounts of effort would be expended for these types of cyber assets to track and document their lack of capability for even the most basic cyber security controls. Viewing BCAs too narrowly could lead to missing consideration of devices that have a sufficient level of cyber capability and risk impact.”

Lesson Learned

CIP Version 5 Transition Program

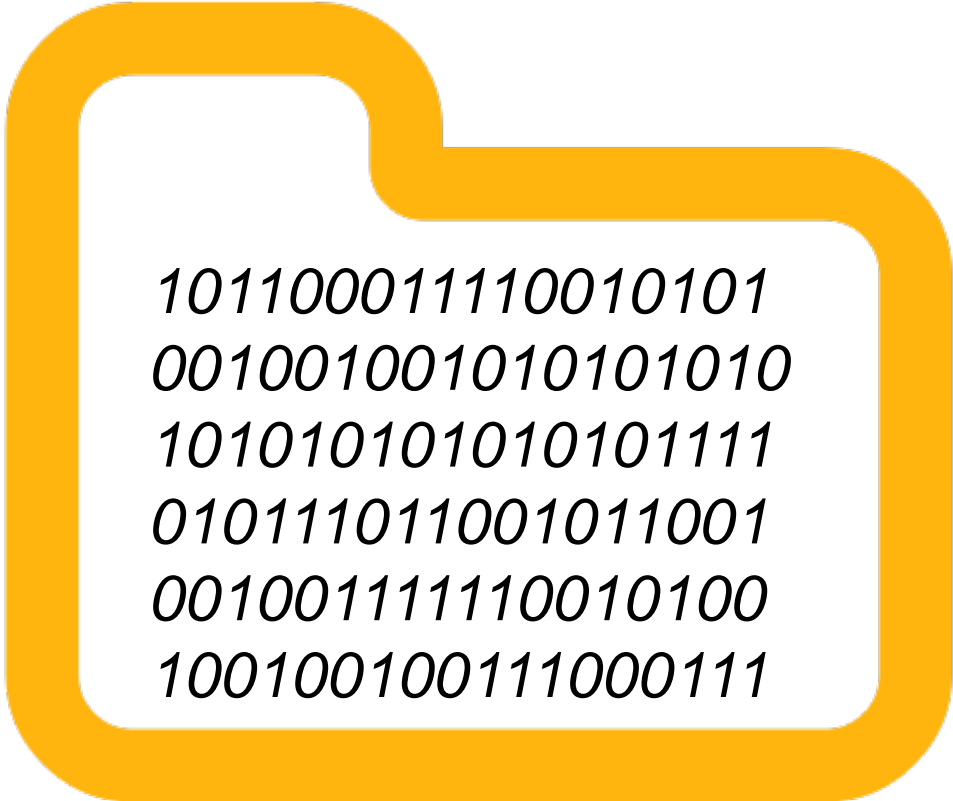
CIP-002-5: BES Cyber Assets

Version: December 7, 2015

Capability: The participants recognized that the CIP standard definitions do not address the level of sophistication or capability of programmable electronic devices nor does it define the term ‘programmable.’ The reliability risk from a cyber perspective posed by a device is often tied to the level of sophistication or capability of that device. Does the device have a level of cyber capability or functionality for which the cyber security controls would be applicable? The risk and potential impact from a compromised operator human-machine interface (HMI) is typically much higher than a single miscalibrated instrument. There are programmable devices that have no concept of a user or authentication, have no ports/services, have no network connectivity, no concept of event logs or alerting, no patches or updates, and are located in areas where physical security perimeters cannot be established. However, the upstream devices to which they connect (e.g., PCs, servers, distributed control system (DCS) controller modules, programmable logic controllers (PLC)) often do have sufficient capability, are clearly Cyber Assets, and were considered as BCAs and afforded CIP protections based on their BES impact categorization.

“The CIP Version 5 standards do not specifically address virtualization. However, because of the increasing use of virtualization in industrial control system environments, questions around treatment of virtualization within the CIP Standards are due for consideration.

The SDT should consider revisions to CIP-005 and the definitions of Cyber Asset and Electronic Access Point that make clear the permitted architecture and address the security risks of network, server and storage virtualization technologies.”



101100011110010101
001001001010101010
101010101010101111
010111011001011001
001001111110010100
100100100111000111

[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

A white, three-dimensional oval plate with a slight shadow underneath. The text is written in a blue, bold, sans-serif font with a halftone dot pattern. The text is arranged in three lines, following the curve of the plate.

Cyber Asset
BES Cyber Asset
Virtualization

- My control system database server is a VM. It exists as a logical construct, stored in a data file in a room of raw computing resources. Is it a BES Cyber Asset or is it just “software or data in those devices”?
- I have an image of a virtual server. Instances of that image are created and destroyed dynamically based on current workload. Are they BCAs? How do I say what the BCAs are in my BCS – I may have BCAs that exist for mere moments.
- What is the hypervisor in the CIP construct? Is it a BCA? An EACMS? Just “software in the device”?
- What can be shared on infrastructure with virtualized BES Cyber Systems? How should it be classified?

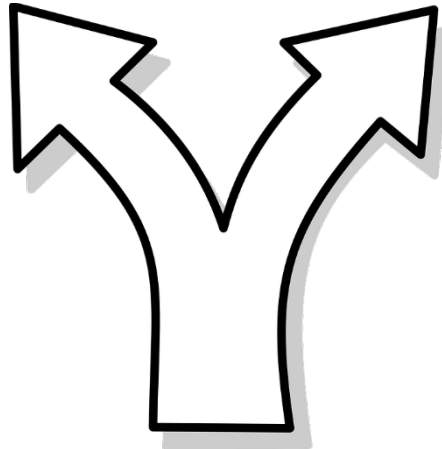
- Is a containerized application a BCA? Or is it just an application? If so, how do the CIP-007 requirements around OS work?
- My EAP is now a *policy* based “firewall” dynamically placed in front of workloads. Access control is now beyond a layer 3 routable protocol level. How do I show compliance with CIP-005?
- Is my SAN part of the same BES Cyber Asset as the virtual machine, is my SAN its own BES Cyber Asset, or is it just a BES Cyber System Information repository since it alone does not perform any BES functions?
- How do I handle sanitization for re-use when storage in my SAN is dynamically allocated amongst multiple cyber systems?



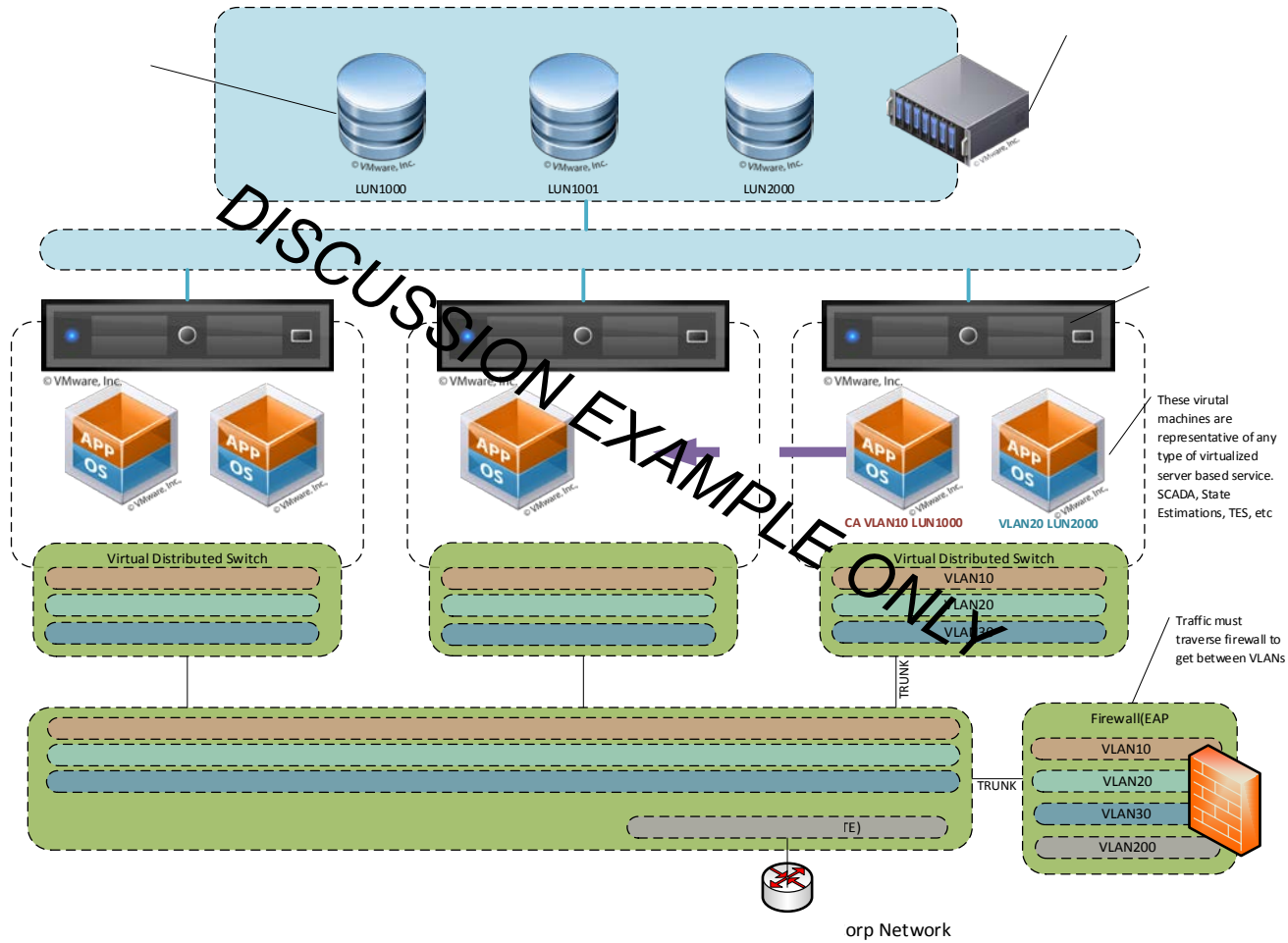
A Fork in the Road

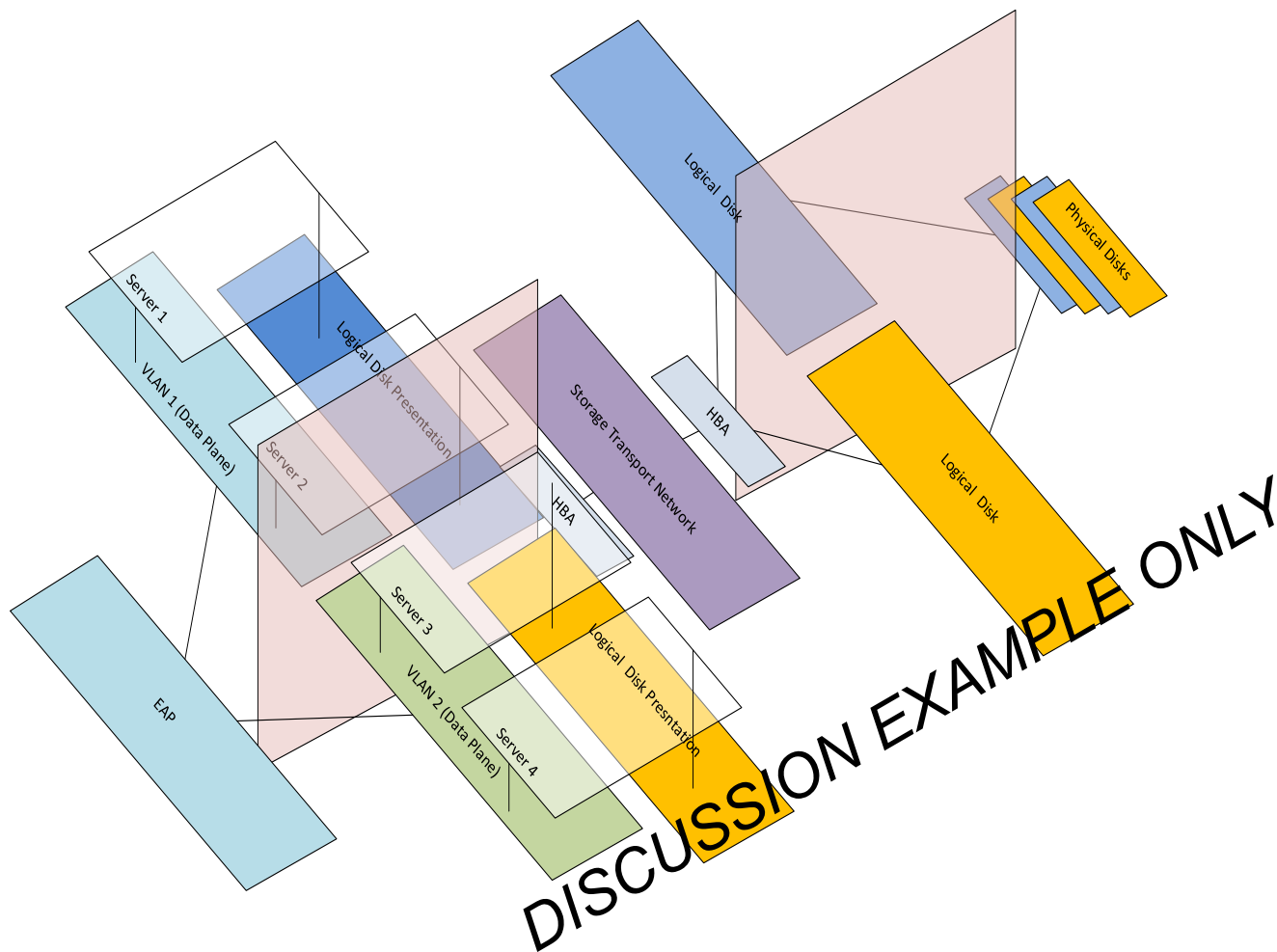


- *Modify existing or create new definitions concerning devices and networking to include virtualization concepts*
- *Create additional technical requirements for securing today's version of virtualization technology.*



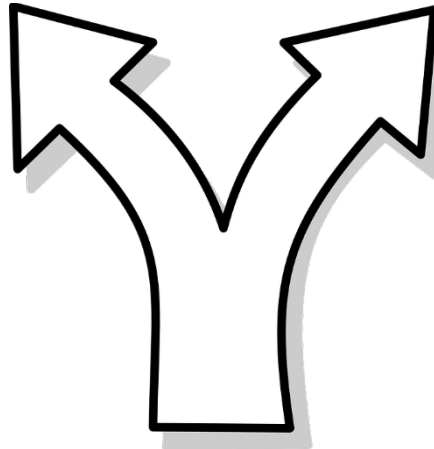
- SDT has worked for over a year on designing virtualization specific language and requirements
 - Electronic Security Zone – to logically isolate systems on shared infrastructure
 - Centralized Management System – to address the risk of virtualization management systems; “fewer, bigger buttons”
- Issues
 - Very complex
 - Today’s technology and products
 - Continues to evolve





- MUCH work on cataloging risk categories unique to virtualization
- Three industry webinars (VMs, storage, networking) in 2017
- March/April 2017
 - Informal Comment form with 10 virtualization/definition questions
- October/November 2017
 - 16 Page informal comment period with 24 virtualization questions
 - Proposed Cyber Asset definition - Each VM is a distinct device
 - Proposed CMS definition
 - Proposed ESZ definition
 - Proposed 5 new requirement parts
 - EACS vs. EACMS and subsequent modifications to BCSI

- *Modify existing or create new definitions concerning devices and networking to include virtualization concepts*
- *Create additional technical requirements for securing today's version of virtualization technology.*
- *More fully embrace the Cyber System concept introduced in Version 5.*
- *Change existing prescriptive technical requirements to be more security objective based and future-proof.*





Backward Compatibility



- CIP is a PROGRAM and the programmatic elements are unchanged.
 - CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011
- CIP has TECHNICAL architecture requirements
 - CIP-005, CIP-007, CIP-010



- Make “BES Cyber System” the foundational object
- Requirements apply at the system level.
 - Implement on system as a whole
 - Implement on components that make sense
 - Allows for dynamic components

- CIP-007-6 R3 Part 3.1

“Deploy method(s) to deter, detect, or prevent malicious code.”

- CIP-007-6 R3 Guidance

“Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes.”

1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.

1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

1.3 Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-6 Table R1 in order to achieve the objective of mitigating the risk posed by unauthorized communications to and from applicable systems. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].

CIP-005-6 Table R1		
Part	Applicable System	Requirements
1.1	<p>High Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Have one or more methods to logically isolate applicable systems either individually or as a group, excluding:</p> <ol style="list-style-type: none"> 1. Communication that has documented inbound and outbound access permissions including the reason for granting access, or 2. Serial connectivity
1.2	<p>High Impact BES Cyber Systems and <u>their</u> associated:</p> <ul style="list-style-type: none"> • PCA <p>Medium Impact BES Cyber Systems at Control Centers and their associated:</p> <ul style="list-style-type: none"> • PCA 	<p>Have one or more methods for detecting known or suspected malicious communications to applicable systems either individually or as a group, excluding serial connectivity.</p>

- Moving towards a fuller Cyber Systems approach
- Modify requirements to be more objective based and technology neutral
- Backwards Compatibility

- Do you support the systems approach concept explained during this WebEx?
 - Yes
 - Yes, but need more information.
 - No (please provide your reasoning in the chat box)
 - I am just here to listen

- Continue to modify requirements within the CIP standards
- Determine measures
- SDT Meetings
 - July 10-12, 2018 (WECC – Salt Lake City, UT)
 - August 7-10, 2018 (NERC – Atlanta, GA)



Questions and Answers