NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Virtual Machines and Containers

Project 2016-02 Modifications to the CIP Standards

CIP SDT Members
June 11, 2020

RELIABILITY | RESILIENCE | SECURITY




NERC Antitrust

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. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

NERC Public Disclaimer

Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Questions

Please use the Q&A feature in WebEx to ask any relevant questions during the presentation. We will be holding questions until the end of the presentation.

Disclaimer

Virtualization changes to CIP standards are to ***ENABLE*** *new methods/models*

NOT

REQUIRE *Them*

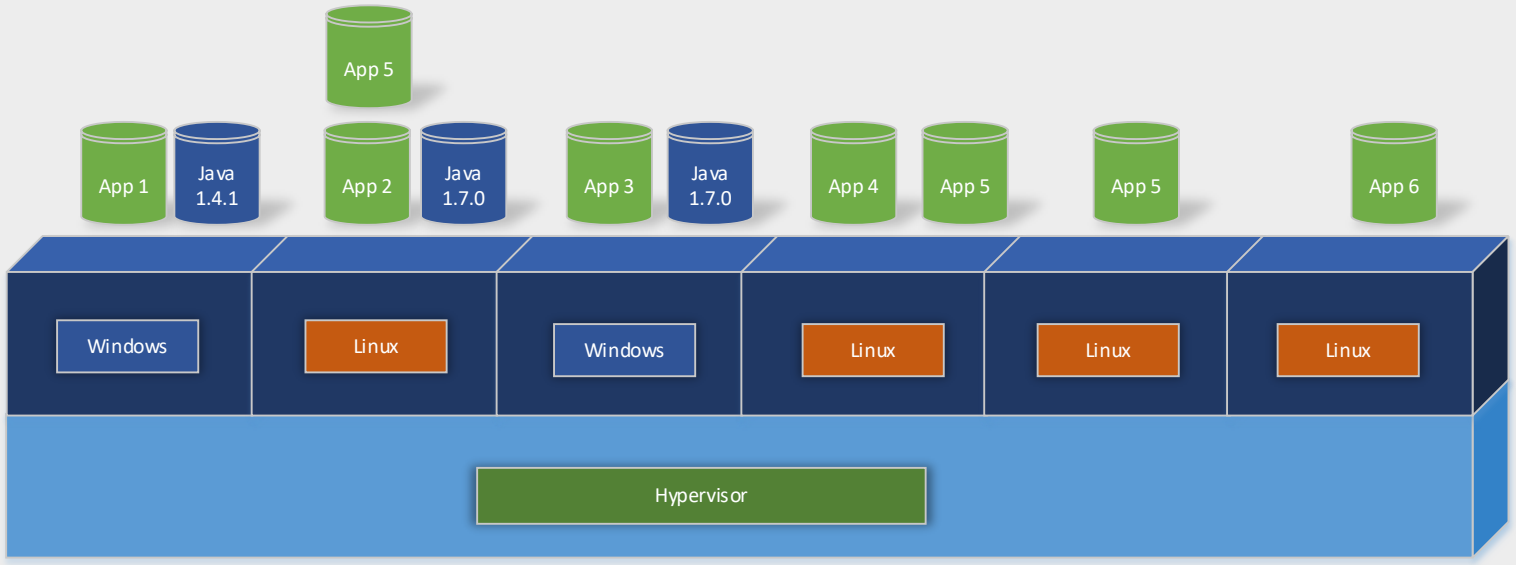
Agenda

- Virtual Machines (VM)
  - What is a VM
  - Capabilities of a VM
  - Challenges for CIP Compliance
  - Changes Made
- Containers
  - What is a container
  - Capabilities of containers
  - Challenges for CIP Compliance
  - Changes Made
- Q&A

What is a Virtual Machine?

- A software representation of a physical device consisting of virtualized hardware, operating system (guest OS), and applications.
- VMs can be:
  - Permanent
  - On-Demand
  - Active or dormant
  - Have Parent – Child Relationships
  - Virtual appliance

What is a Virtual Machine?



Virtualization Software Stack

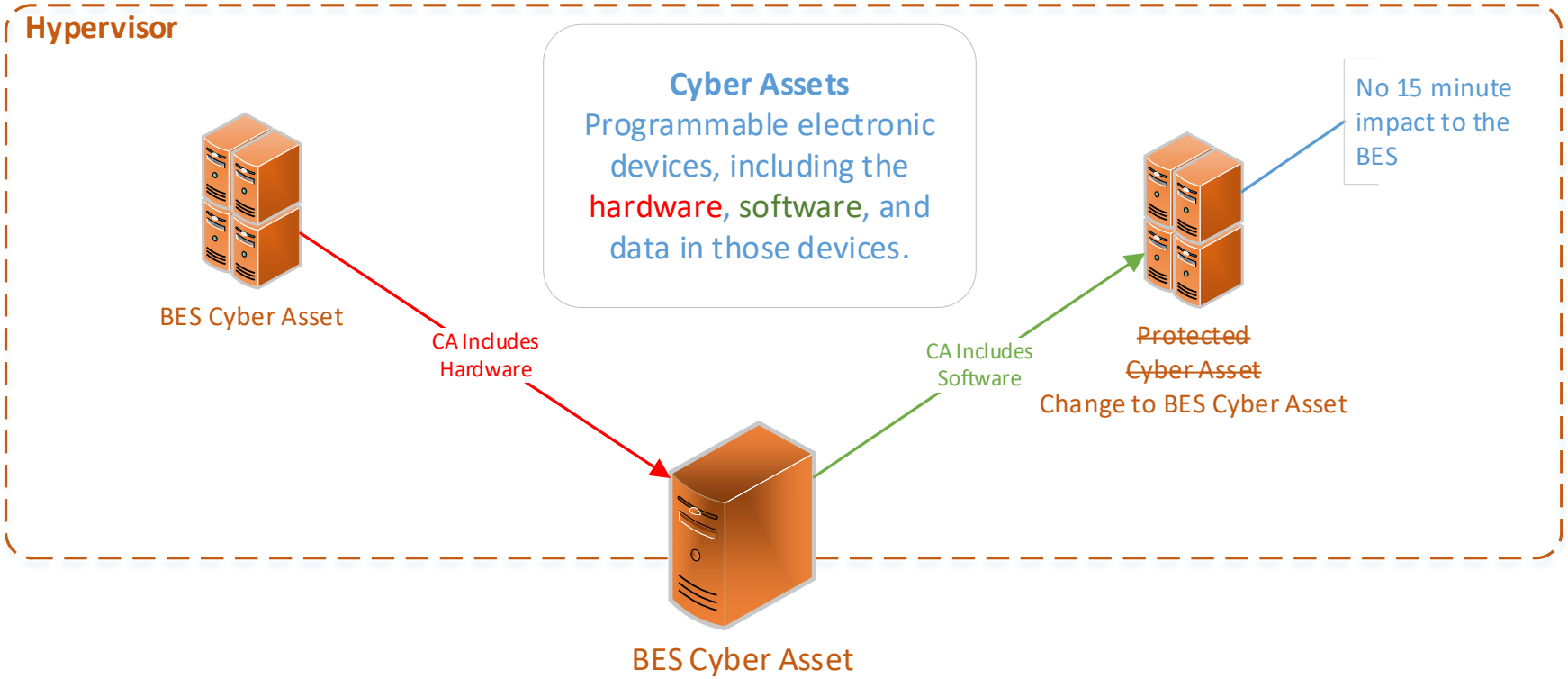
Capabilities of a Virtual Machine

- Virtual Machine Capabilities:
  - Can Increase Efficiency and Decrease Cost
  - Can Enhance Security
  - Disaster Recovery – Can Increase Availability and Decrease downtime
  - Can Allow for Software Mobility
  - Separation of the hardware/software Lifecycle

Virtual Machine Challenges

- Some of the challenges for CIP Compliance:
  - Definitional Construct
  - Security Gaps

Challenges for Virtual Machines



Virtual Machine Changes

- Some of the changes made to support Virtual Machines

  *New Definition Created

Virtual Cyber Asset (VCA): A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure. *(Subject of a future webinar)*

Virtual Machine Changes

- Some of the changes made to support Virtual Machines

  **Updated PCA Definition*

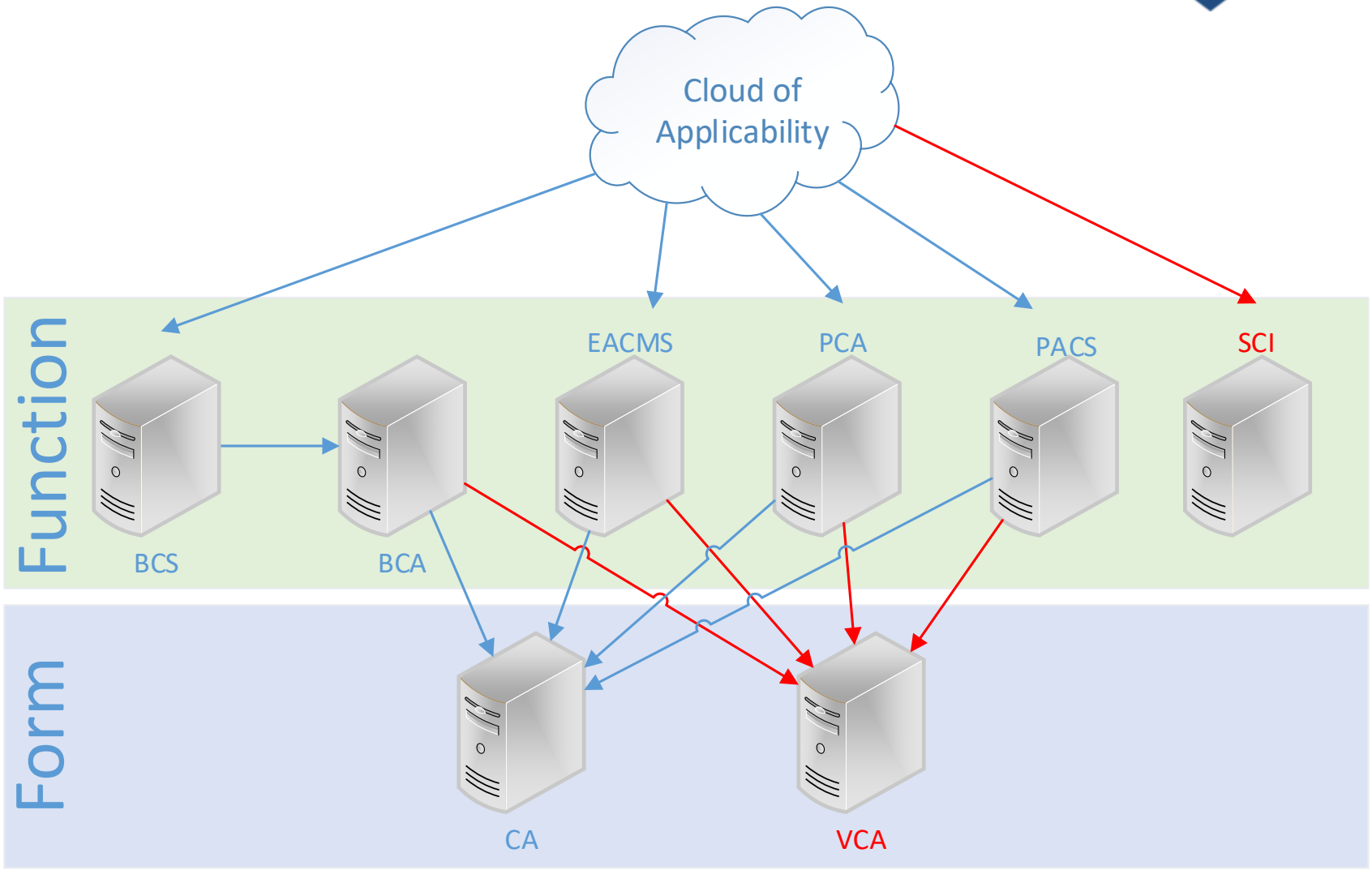
Protected Cyber Asset (PCA) *Cyber Assets or Virtual Cyber Assets that:*

Are not logically isolated from a BES Cyber System; or

Share compute resources (CPU or memory) with a BES Cyber System,

excluding logically isolated cyber assets or virtual cyber assets that are being actively remediated prior to introduction to the production environment.

Virtual Machine Changes



Virtual Machine Changes

- Raising to the System Level
  - Handling of dormant VMs
  - Handling of ephemeral VM's (ones that come and go)
  - Handling of snapshots
  - Handling of new virtual machines

Virtual Machine Changes

- Changes to CIP-007 Example
  - Changes in requirement language from asset to system.

CIP-007-76 Table R4 – Security Event Monitoring		
Part	**Applicable Systems**	**Requirements**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and ~~3.~~ PCA ~~4.~~3. Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Log security events, per system capability, ~~at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Aasset level (per Cyber Aasset capability)~~ for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, ats a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.

Virtual Machine Changes

- Changes to CIP-010 R1 Part 1.3 Example
  - Reference to list in Part 1.1; Baselines removed, replaced with objective

1.~~3~~5	High Impact BES Cyber Systems.	~~Where technically feasible, f~~For each change to the items listed in Part 1.1 ~~that deviates from the existing baseline configuration~~, per system capability: 1.3.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects and differences with the production environment ~~, that models the baseline configuration~~ to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

Virtual Machine Changes

- Changes to CIP-010 R3 Part 3.2 Example

3.2	High Impact BES Cyber Systems. SCI hosting High Impact BCS. Management Modules of SCI hosting High Impact BCS.	~~Where technically feasible, a~~At least once every 36 calendar months, per system capability: 3.2.1. Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects~~,~~ ~~that models the~~and differences with the production environment ~~baseline configuration of the BES Cyber System in a production environment~~; and 3.2.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

Virtual Machine Changes

- Changes to CIP-010 R3 Part 3.3 Example

3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA SCI hosting High Impact BES Cyber Systems or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High Impact BCS or their associated EACMS, or PCA.	Perform an active vulnerability assessment prior to logically connecting an additional applicable Virtual Cyber Asset, Cyber Asset, or Shared Cyber Infrastructure to ~~an other~~a production ~~BES Cyber System~~ environment ~~applicable system~~, per system capability, ~~Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset,~~ except for CIP Exceptional Circumstances and ~~like replace~~deployments of the same type ~~of Cyber Asset~~ with a previously assessed ~~baseline~~ configuration. The production environment does not include devices being actively remediated and logically isolated.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset, Virtual Cyber Asset, or Shared Cyber Infrastructure) and the output of any tools or Management Systems used to perform the assessment.

What is a Container

- What is a container?
  - It's a form of virtualization
  - Can be used from a process to full applications
  - Containers do generally not contain OS images
  - Are lightweight because they do not run multiple OS's
  - Platforms can be managed/orchestrated by tools such as Kubernetes(similar to vsphere for VM's)
  - Most importantly – It is software.

What is a Container

Virtual Machines vs. Containers

Virtual Machine	Virtual Appliance	Container
Full copy of Operating System	Full copy of Operating System	Minimal Operating System files
Application(s) can be installed	Application(s) pre-installed	Single or part of an application pre-installed
Hypervisor required	Hypervisor required	Hypervisor not required
Memory isolation between VMs	Memory isolation between VMs	Shared memory between containers
Software patched individually	Software patched as a bundle	Software patched as a bundle
VCA	VCA	SCA - software

Capabilities of a Container

- Require Less Overhead
- Increased Portability
- More Consistent Operation (Apps must be normalized)
- Greater Efficiency
- Cleans up application development processes

Challenges for Containers

- Some of the challenges for CIP compliance:
  - Falls somewhere on the continuum of software to operating system
  - Includes OS and additional (i.e. Java) dependencies
  - Immutable package (updated as a whole)
  - Runs on a CA or VCA – as software

Changes for Containers

- Some of the changes made to support Containers
  - New Definition Created; used in requirement language
  - **Self Contained Application (SCA):** Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

Changes for Containers

- CIP-010 R1 Part 1.1 Example of Containers in Requirement Language

1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA. Management Modules of SCI hosting High or Medium Impact BCS or their associated PACS, EACMS, or PCA.	Authorize changes to: **1.1.1.** Operating system(s) or firmware or images used to derive operating systems or firmware; **1.1.2.** Commercially available or open-source application software including Self-Contained Applications ; **1.1.3.** Custom software installed including Self-Contained Applications; **1.1.4.** Logical network connectivity; **1.1.5.** Security patches applied; **1.1.6.** SCI configuration that: 1.1.6.1. Enforces electronic access control that

Virtual Machines and Containers – Wrap up

- Key Take-aways
  - Concepts borrowed from NIST, FEDRAMP, other frameworks.
  - New VCA Definition to describe virtual machines
    - VCA works through function definitions (BCA, EACMS, PACS, etc.)
  - Modified PCA Definition to add affinity and remediation
  - Changes to CIP-007 and CIP-010
    - Raised Cyber Asset references in requirement language to system level
    - Shift from baselines to objective level CIP-010
      - Change needed to support Dormant VMs, Parent images, etc.
    - Changes to order of operations for certain tasks to allow devices to be connected physically but logically isolated to automatically remediate their risks
    - New “Self-Contained Application” Definition
      - To be treated as software, used in requirement language to add clarity

Q&A Objectives

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - 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.

Questions and Answers