NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Virtualization and Future Technologies

Project 2016-02 Standards Drafting Team: What’s in it for me?

April 2020

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Executive Summary iii

Introduction iv

Background iv

Chapter 1 : Virtualization Benefits Overview 1

Chapter 2 : Clarifications for Permitted Architectures 3

Hypervisors and Storage Systems 3

Virtual Machines 3

Containers 3

Security perimeters that span geographic location (SuperESP) 3

Management 4

Chapter 3 : Additional Capabilities Enabled 5

Zero Trust Architecture 5

Hardware and Software Reduction 5

Network Access Control 5

Automation of Compliance and Evidence Gathering 6

Chapter 4 : Conclusion 7

Executive Summary

What the interconnected power grid does for Bulk Electric System (BES) reliability, virtualization does for the computing infrastructure supporting vital control systems. Individual utilities interconnected their power systems to form a power grid to share spare capacity for meeting demand peaks and surviving contingencies such as generating unit and transmission line outages. Virtualization connects processors, networks, and storage into 'computing grids' that allow our vital systems and applications to meet peak demands and survive outages of individual components.

This is accomplished by abstracting servers, networks, and storage into virtual or logical resources that can be independent of specific underlying hardware such as individual processors, circuits, and disks. A control system and its underlying operating system become a virtual machine and can move to any available hardware. This greatly increases reliability and resiliency of our control systems that support BES reliability.

Virtualization technologies also allow enhanced cyber security controls and the ability to move access controls from the edge of our networks to much deeper inside of them. This is analogous to having generation close to load centers to reduce the susceptibility to outages. These newer security controls allow us to provide tighter security by moving access controls from an outer perimeter closer to the actual code performing reliability tasks.

As the vendors of our systems incorporate more and more virtualization and advanced technology, it is challenging the way we characterize the Critical Infrastructure Protection (CIP) standards' objectives and how we develop technical requirements. Use of virtualization and advanced technology can provide benefits for implementing both operational and security enhancements to a system. The goal is to require technology-enforced controls that meet security objectives as alternatives to the current prescriptive requirements like those requiring a physically structured architecture, without forcing the use of the new technology. The existing standards with their prescriptive language limit the ability to take full advantage of the new technologies. The Project 2016-02 Modifications to CIP Standards Standard Drafting Team (SDT) is modifying existing requirements and drafting new requirements to support virtualization capabilities. This leaves Responsible Entities with the option to maintain a non-virtualized environment and use backward compatibility to preserve current CIP investments and security postures.

This white paper describes the areas that are being addressed by the 2016-02 standards drafting team and attempts to describe the clarifications for existing virtualization architectures and new capabilities that are enabled with the changes.

Introduction

Background

In the history of the CIP standards, industry has seen many versions and changes. Some have been straightforward and almost self-explanatory. Others, complex and time-consuming to implement. Still others have been foundational, like the ‘do-over’ change from Versions 1 – 3 to Version 5. Not surprisingly, the prospect of another set of fairly major changes, this time involving virtualization sparks a great deal of industry concern. It raises valid questions about the timing and the drivers of those changes, and whether or not they are truly necessary. The white paper is designed to provide more detailed answers to those questions from the viewpoint of the SDT.

Recognizing the continuing growth in technology innovation, many entities in the Electricity Sector have implemented virtualization as part of their CIP programs. Many of these same entities, however, have implemented this new technology without taking full advantage of virtualization’s advanced capabilities. There are a number of reasons for this from the constraints of the current CIP architecture to the ongoing ambiguity around how new virtualization technology applies to CIP compliance. Some of those who are implementing virtualization are experiencing a great deal of uncertainty and difficulty around developing implementation strategies that will support compliance and achieve greater reliability and security.

The Version 5 Transition Advisory Group (V5TAG), born out of the Version 5 implementation pilots, determined that the issues around the standards and virtualization needed to be addressed by a drafting team. The Project 2016-02 SDT was assigned the task to clarify the permitted architectures and enable additional capabilities the virtualization technology offers.

The SDT’s purpose of incorporating the virtualization concept into the CIP standards is not to merely augment the current standards. The SDT’s intent is to better position the CIP standards to be applicable to any future technological innovation. Leveraging the abstraction that virtualization provides will allow the industry to more readily adopt new technology and increase security posture. This paper presents the SDT’s case for change to the NERC CIP standards that is needed to allow for the innovative security techniques and new concepts brought about by virtualization.

Chapter 1: Virtualization Benefits Overview

In many ways, virtualization does for our critical applications what the interconnected power grid does for reliability of the bulk power system.

First, it allows for increased reliability in the same way the interconnected power grid does. Imagine if the power system were made up entirely of non-interconnected islands with one generating plant and radial transmission lines. Any failure of any one component and reliability suffers. Likewise, in the traditional non-virtualized scenario of dedicated servers and networks, if a component fails the application fails with it. In this model, reliability is increased primarily through investing in redundant assets, increasing costs.

However, if those islands are connected together into a synchronous power grid with many interties, reliability is greatly increased because the criticality of any single asset is greatly decreased. If a generating unit trips (a hardware server fails), the load is met from the spare capacity at another plant (the virtual server moves to another functioning hardware server). If a transmission line breaker opens (a network switch fails), power is rerouted through the grid (a virtual network delivers data by using other network hardware paths available to it).

Virtualization also reduces costs by providing reliability without large amounts of redundant assets. It's analogous to a Reserve Sharing Group where a group of utilities pool their reserve capacity in order to mitigate contingencies instead of every utility building high degrees of redundant capacity. In the same way, virtualization allows the computer hardware resources (servers, networks, storage) to be grouped and their excess capacity shared among different systems. Now the total of all excess capacity is not tied to individual servers or network circuits but is pooled and available to any virtual server that needs it due to a peak load or a contingency. It prevents having to size every individual server to meet its peak load and then have that capacity unused 99% of the time while another server next to it is starving for resources to meet its current demand. With virtualization, it operates more like the power grid; sharing capacity and obtaining a higher utilization of existing assets. The same reasons behind the creation of grid Interconnections are the same reasons behind virtualization; to handle peak loads and failures of individual components while maintaining reliability of service at a reasonable price. Virtualization provides a 'computing grid' for vital control systems.

In the power grid the sharing of resources and routing of power around failed components and keeping things straight between individual utilities and their customers requires oversight and coordination. In the grid, that role is fulfilled by Balancing Authorities and Reliability Coordinators using Energy Management Systems. In virtualization, that role is fulfilled by the “hypervisor”; the EMS of virtualized infrastructure. It is the main component that performs these same functions for all the individual resources (servers, disks, networks) it manages. It manages the allocation (dispatch) of resources, the moving of virtual servers around failed processors and networks to functioning hardware, and maintains the separation between different virtual machines from each other and itself.

In addition to resiliency from hardware or circuit failures, virtualization also provides the same from software failures. Since virtualization abstracts machines (servers and workstations) to a software 'image' that can run anywhere, virtual servers become simply image files that can be copied. If a software problem develops due to a change, or a patch, or from tampering or a breach, the entire virtual server is simply an image and can be restored to a previous state with a file copy, decreasing recovery time drastically over a physical server rebuild.

All of these concepts together provides the same effect to our computing grid as it does to our power grid: a reduction in both the frequency and the duration of outages at a reasonable cost.

Finally, virtualization can provide numerous security benefits. At a high level, the virtualization of network security functions is analogous to siting generation close to the load centers, in that it allows network security functions to be located ever closer to what they are trying to protect – the applications or services provided by the infrastructure – and thus protect them at a much more granular level. delete or replace before publication.

Chapter 2: Clarifications for Permitted Architectures

Virtualization brings benefits to reliability and resiliency of our BES Cyber Systems. It also brings challenges with determining how some of the newer concepts fit within the framework of the NERC CIP standards. The proposed changes are focused on providing clarification to the following areas for existing virtualization architectures being used today.

- Hypervisors and Storage Systems
- Virtual Machines
- Containers
- Security perimeters that span geographic locations (SuperESP)
- Management

Each of these topics will be covered in the following sections.

Hypervisors and Storage Systems

A hypervisor is a piece of software that divides a physical machine into smaller virtual machines. Storage systems act very similarly except that the resources it shares are consumed by some other device outside of itself. Since the main purpose of hypervisors and storage systems is to share their resources with some other physical or virtual device, the proposed changes have created new a term called "Shared Cyber Infrastructure" (SCI) to provide clarity on how to protect them effectively.

Virtual Machines

Virtual machines are a piece of software that emulates a physical machine. The proposed changes have created a new term called "Virtual Cyber Asset" (VCA) to describe them for the purpose of more accurately applying requirements. Changes have also been made to accommodate some of the specific characteristics of virtual machines that are created on demand, parent/child images, virtual machines that are disabled or turned off (known as dormant VM's), special appliances used to extend functionality (known as helper VM's), etc. The new updates give the industry assurance that they are properly describing the virtualized infrastructure.

Containers

Containers are a piece of software that bundle applications together to make a single function. Unlike virtual machines they do not typically emulate a physical machine. The proposed changes have created a new term called "Self-Contained Applications" (SCA) to describe them for the purpose of more accurately applying requirements as well as to accommodate the management systems and automation associated with containerized applications so that they are properly described in compliance programs.

Security perimeters that span geographic location (SuperESP)

Many redundancy strategies for datacenters include the use of spanned networks (one where an IP address can stay the same at both sites) for the purposes of simplifying the configurations of systems that need to be protected.

The proposed changes implement new requirements that specifically address the confidentiality and integrity risks of spanning security perimeters between geographic locations. With these changes in place, there is clarity on how to properly implementing spanned networks across datacenters.

Management

In the current CIP standards, there are no specific terms to address management interfaces for systems and the proposed changes implement new requirements and definitions that clarify the permitted architectures and address the risks posed by management systems. The following three definitions help describe the types properly so that they can be adequately protected.

- Management Systems (such as systems that centrally manage assets or infrastructure)
- Management Interfaces (such as interfaces used to configure systems, commonly used by Management Systems)
- Management Modules (such as ILO, IDRAC, embedded management devices)

Chapter 3: Additional Capabilities Enabled

Virtualization brings new technology and capabilities to support BES Cyber Systems. This section will cover some of the areas that are enabled by the proposed changes to the CIP standards.

- Zero Trust Architecture
- Hardware and Software Reduction
- Network Access Control
- Automation of Compliance and Evidence Gathering

Each of these topics will be covered in the following sections.

Zero Trust Architecture

There are some new and growing security strategies for networks with the primary one known as "zero trust" architecture. It brings a fundamental change to networking from an implicit trust inside a perimeter to zero trust. The basic premise of this model is there is no implicit trust granted to systems based on their physical or network location because there is no trust of any network. Every network is treated as untrustworthy and data flows are permitted on a case-by-case basis, denying all other traffic by default. This model no longer relies on network information to make decisions as it has access to information about the applications themselves. The additional context allows the entire system to permit based on signed certificates, groups, user accounts, etc. instead of relying on IP and port information. This model is generally considered a much stronger security posture and is described in detail in NIST SP 800-207.

Presently the standard is focused on creating specifically a perimeter-based model for security (commonly known as ESP). The proposed changes to the CIP standards move towards an objective approach that allow zero trust and other models of security while leaving the existing ESP model as a fully compliant option.

Hardware and Software Reduction

Presently the standards focus primarily on physical isolation and do not specifically address virtualizing infrastructure on shared common hardware platforms. The proposed changes introduce the concept of logical isolation to allow the sharing of software or hardware. The proposed changes introduce new requirements and clarity for when hardware or software is shared between differing impact BES Cyber Systems as well as non-CIP Cyber Assets. Another example would be having multiple logical networks on a single network switch that are logically isolated from one another.

Network Access Control

There are some relatively new technologies available that aim to ensure that devices are scanned, patched, and secured prior to connecting to a production network. Network access control strategies (such as 802.1x or Remediation VLANs) allow devices to at the time of network connection be automatically isolated until they meet a set of criteria defined by a software policy.

The current focus of the CIP standards is to ensure that devices are scanned/patched prior to connecting. The changes to the standards allow the device to be connected but automatically isolated while it is being scanned and patched prior to being allowed on the network.

Automation of Compliance and Evidence Gathering

Most commercial virtualization technology was built on the premise that it would be used in large scale deployments. As a result, most of the technology includes automation that can be leveraged to both enforce compliance posture and perform regular evidence gathering tasks. Because of the clarifications provided throughout the standards, entities can use these automation platforms to ensure their environments remain compliant and secure.

Chapter 4: Conclusion

Virtualization technology allows for increases in reliability and resiliency, reducing frequency and duration of outages of vital systems and helping systems meet peak demands at reduced cost through the sharing of excess capacity. These technologies were either not contemplated or in their infancy when the foundations of the CIP standards were laid. The updates to the definitions and requirements within the CIP standards are necessary to clarify the compliant architectures and allow the additional capabilities as discussed in this paper. Many of these capabilities allow for increased cyber security, and some allow for more automated security controls where the infrastructure itself enforces controls and the evidence gathering that are often manual today. The Project 2016-02 assets that these changes move the CIP standards further down the road towards keeping the CIP standards relevant to the technology on which our most vital systems depend upon to keep the bulk power system as the reliable system that it is today