Project 2016-02
CIP Modifications

Webinar on Standard Drafting Team Considerations for the Use of Virtualization in the CIP Environment
July 19, 2017
• Opening Remarks and Introduction of Presenters
• Standard Drafting Team
• Administrative Items
  ▪ Antitrust and Disclaimers
  ▪ Webinar Format
• Storage Virtualization
• Questions and Answers
• 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. Notice of the webinar was posted on the NERC website and 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.
<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-Chair</td>
<td>Christine Hasha</td>
<td>Electric Reliability Council of Texas</td>
</tr>
<tr>
<td>Co-Chair</td>
<td>David Revill</td>
<td>Georgia System Operations Corporation</td>
</tr>
<tr>
<td>Members</td>
<td>Steven Brain</td>
<td>Dominion</td>
</tr>
<tr>
<td></td>
<td>Jay Cribb</td>
<td>Southern Company</td>
</tr>
<tr>
<td></td>
<td>Jennifer Flandermeyer</td>
<td>Kansas City Power and Light</td>
</tr>
<tr>
<td></td>
<td>Tom Foster</td>
<td>PJM Interconnection</td>
</tr>
<tr>
<td></td>
<td>Richard Kinas</td>
<td>Orlando Utilities Commission</td>
</tr>
<tr>
<td></td>
<td>Forrest Krigbaum</td>
<td>Bonneville Power Administration</td>
</tr>
<tr>
<td></td>
<td>Philippe Labrosse</td>
<td>Hydro-Quebec TransEnergie</td>
</tr>
<tr>
<td></td>
<td>Mark Riley</td>
<td>Associated Electric Cooperative, Inc.</td>
</tr>
</tbody>
</table>
Purpose of this presentation:

- To inform and educate industry stakeholders to help them participate in the discussions around virtualization
- To improve feedback on comment forms
- To validate concepts that the SDT has developed with real-world use cases

**Note: The examples and use cases shown here are for discussion purposes only, and are not intended to be guidance for implementing any CIP compliance program**
Virtualization Webinar Recap

• Webinar #1
  ▪ Virtualization Overview
  ▪ Logical Isolation / Management Plane Isolation
  ▪ Introduction of Centralized Management System (CMS)
  ▪ Network Topology

• Webinar #2
  ▪ Hypervisors (Templates, VM Mobility, Resource Scheduler, etc.)
  ▪ Multi-Tenancy (Tenants, Underlay Networks, etc.)
  ▪ Introduced ESZ Concept (Logical Separation)

• Webinar #3
  ▪ Storage
Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection
• **Redundant Array of Independent Disks (RAID)** – a technology used to prevent the loss of data from the failure of an independent disk

• **Storage Processor** – the server built into the storage array for providing access to the shared storage

• **Storage Array** – Generally referred to as the combination of disks and the storage processor

• **Host BUS Adapter (HBA)** – Used to provide servers access to a storage array network

• **Storage Network** – Provides transport between the components of a storage system

• **Storage Area Network** – Collection of HBA, Storage Processors, Storage Arrays and disks
The Personal Computer

- Difficult to share data between users
- Failure results in the total loss of data
• Server Model
  - Easy to share data
  - Single drive failure still results in the total loss of data
• Server w/ RAID
  - Redundancy allows a single drive to fail without the loss of data
  - Wastes 30-50% of storage
  - Servers have a limited number of slots for drives
Server with Direct Attached Storage
- Wastes ~30% of storage
- Each server has drives to manage and maintain
- Server Hardware failure results in total outage to applications
- Applications are installed directly to the physical server
• Redundant Servers with Direct Attached Storage
  - Since the Data exists outside of the servers, multiple servers can be used to support the application
  - Direct Attached Storage Array is now the single point of failure
  - Complex Environment – Experts only
  - Limited Application Support
  - Cabling Distance VERY limited
• Storage Area Network
  ▪ The Storage Area Network is made up of HBA’s, Storage Networks, Storage Processors, and Disks
  ▪ Storage Networks are a separate component from the Storage Array
  ▪ Storage Arrays need a front end to talk to servers across the storage network (commonly called Storage Processors)
  ▪ Addresses the cabling limitations of direct attached storage
  ▪ Provides Redundancy to all components
  ▪ Complex Environment – Experts only
  ▪ Limited Application Support
• Multi-Instance Storage Area Networks
  - Provides Redundancy to all components
  - Supports Multiple Tenants at a physical level
  - Complex Environment – Experts only
  - Limited Application Support
• Storage Area Network w/ Hypervisor
  - Current Technology
  - Complex Backend Environment
  - Applications are moved to virtual machines
  - Applications no longer need to understand the storage infrastructure to be redundant
  - Since the complex hardware environment is abstracted from the users it can be replaced without impacting users.
• Fully Virtualized SAN
  - New Technology <2 years old
  - Backend storage system is simplified dramatically
  - This type of Storage Area Network is entirely software controlled
  - Consistent and simplified hardware profile
  - Significantly reduced software footprint
  - Transition Issues: Some implementations emulate the old constructs that are very complex, Others use simplified models that are very easy to administer
Evolution Wrap-up

- Each Iteration of Storage Technology tried to fix a major problem from the previous generation
- Utilities are generally using multiple iterations of storage technology
- Storage Networks were added later and are separate from the Storage Array
- Hypervisors were built to abstract applications from backend systems
- Datacenter Storage Systems are designed for Multi-Instance environments from the ground up. (Even before Hypervisors were implemented)
Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection
• Server and Storage Virtualization Similarities
  ▪ They both service application workloads for user consumption
  ▪ Both operate invisible to the users
  ▪ Both typically have dedicated management planes and operate out of band from the production systems
  ▪ Both are built from the ground up to service multi-instance environments
  ▪ ESZ's can be applied to logically separate both
The SDT is considering the creation of a construct called an Electronic Security Zone to describe controls used to separate Tenants with logical isolation:

- This concept would be used to separate the management plane from the data plane.
- The concept can be used to create other ESZ’s within an ESP (Such as to isolate outbound communication, or to split a storage array).
- Devices that support multi-tenancy need to use the management ESZ to communicate with their Centralized Management System (CMS).
- Not limited to networking concepts, can be used to model any type of logical control.
ESZ Storage Network Examples

• Electronic Security Zones applied to Storage Arrays
  ▪ Storage Processors
  ▪ Logically Isolated Management Plane

• Electronic Security Zones applied to current/future shared storage networking technologies
  ▪ Fiber Channel
  ▪ iSCSI
  ▪ VSAN(Future)
• Components
  § Management Console
  § Storage Processor
  § Physical Disks
  § Logical Disks
  § Logical Presentations
  § Physical Interfaces
ESZ : Storage Arrays
ESZ: Storage Arrays

Storage Array

- Management Console
- Logical Disk #1: SCADA
- Logical Disk #2: ICCP

Physical Interfaces

- Presentation SCADA
- Presentation ICCP

Storage Processors

Physical Disks

Storage Network
ESZ: Storage Arrays

Storage Array

Management Console

Logical Disk #1 SCADA
Logical Disk #2 ICCP

Presentation SCADA
Presentation ICCP

Storage Processors

Physical Disks

Storage Network
ESZ: Storage Arrays

Storage Array

Management Console

Logical Disk #1 SCADA

Logical Disk #2 ICCP

Presentation SCADA

Presentation ICCP

Physical Interfaces

Storage Processors

Physical Disks

Storage Network
ESZ: Storage Arrays

Diagram showing a storage array with management console, storage processors, physical disks, presentation interfaces, and storage network.
ESZ: Storage Arrays

Hypervisor 1

VM

VM

SCSI

Resource Scheduler

Fiber Channel HBA

Storage Processor

Logical Disk #1

Logical Disk #2

Storage Processors

Fiber Channel HBA

Disks

Fiber Channel Switch

VSAN 10
ESZ: Storage Arrays

Hypervisor 1

VM

Fiber Channel HBA

Resource Scheduler

SCSI

Storage Processor

Logical Disk #1

Logical Disk #2

Storage Processors

Fiber Channel HBA

Disks

Fiber Channel Switch

VSAN 10
ESZ: Storage Arrays

Hypervisor 1

- VM
- Resource Scheduler
- Fiber Channel HBA
- SCSI

Storage Processor

- Logical Disk #1
- Logical Disk #2
- Storage Processors
- Fiber Channel HBA
- Disks

Fiber Channel Switch

VSAN 10
- Fiber Channel Frames are not Ethernet
- They are raw SCSI frames encapsulated in a fiber channel header
- VSAN’s divide switches
- Zones control which HBA’s can talk to each other
ESZ Defined by Device Configurations

- The configuration of the Storage Processor is providing isolation between devices in different ESZ’s.
- The configuration of the hypervisor is providing isolation between devices in different ESZ’s.
- The configuration of the Fiber Channel switch is ensuring that the correct devices are providing access control to logically isolate the ESZ’s.
• ESZ Defined by Device Configurations
  - The configuration of the Storage Processor is providing isolation between devices in different ESZ’s
  - The configuration of the hypervisor is providing isolation between devices in different ESZ’s
  - The configuration of the Ethernet switch is ensuring that the correct devices are providing access control to logically isolate the ESZ’s
ESZ: Fully Virtualized Storage Array
ESZ: Fully Virtualized Storage Array
Applying ESZs to Different Storage Systems

- Applying ESZ’s Wrap-up
  - Electronic Security Zones applied to current/future shared storage networking technologies
    - Storage Processors
    - Fiber Channel
    - iSCSI
    - NFS
    - VSAN (*Future*)
  - The configuration of the devices in the multi-instance environment are responsible for ensuring that ESZ’s remain logically isolated.
Webinar 3 - Storage Summary

Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection
Scaling Storage Networks

- The SDT has asserted in the past few webinars that vendors provide security and resiliency features based on the scale of the environment.
- Smaller scale environments do not offer as many enterprise grade solutions for security and resiliency.
- Examples from 4 Common Storage Vendors*
  - Sizing based on ~40Tb for CIP Environments and >500TB for non-CIP environments
  - Disclaimer: Information was mined from the vendors publicly available information and was not provided by vendors
  - References will be posted at the end of this section
Scaling Storage Networks

• Comparison #1 : Vendor HP

• HP StoreEasy 1550
  ▪ Entry-Level
  ▪ Capacity: 80Tb
  ▪ Encryption: N/A
  ▪ DR: N/A

• HP 3PAR StoreServ 8000
  ▪ Mid-Enterprise Level
  ▪ Capacity: 4000Tb
  ▪ Encryption: Hardware
  ▪ DR: Site-to-Site
  ▪ FIPS/FDE Certified Disks
Scaling Storage Networks

• Comparison #2 : Vendor Dell/EMC

  • Dell Storage PS4210E
    ▪ Entry-Level
    ▪ Capacity: 72Tb
    ▪ Encryption: N/A
    ▪ DR: N/A

  • EMC Unity 500F
    ▪ Mid-Enterprise Level
    ▪ Capacity: 7800Tb
    ▪ Encryption: Hardware
    ▪ DR: Site-to-Site
    ▪ FIPS/FDE Certified Disks
• **Comparison #3 : Vendor NetApp**

  - **NetApp SolidFire SF38410**
    - Entry-Level
    - Capacity: 84Tb
    - Encryption: Software
    - DR: Site-to-Site
  
  - **NetApp AFF A700**
    - Mid-Enterprise Level
    - Capacity: 1800Tb
    - Encryption: Hardware
    - DR: Site-to-Site
    - FIPS/FDE Certified Disks
Comparison #4: Vendor Nimble Storage

- Nimble AF5000
  - Entry-Level
  - Capacity: 167Tb
  - Encryption: Software
  - DR: Site-to-Site

- Nimble AF9000
  - Mid-Enterprise Level
  - Capacity: 2212Tb
  - Encryption: Software
  - DR: Site-to-Site
## Scaling Storage Networks

### Entry Level Solutions (Target ~40Tb Storage)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Solution</th>
<th>Encryption</th>
<th>Max Tb</th>
<th>HW Redundancy</th>
<th>DR</th>
<th>FDE/FIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP</td>
<td>StoreEasy 1550</td>
<td>N/A</td>
<td>80Tb</td>
<td>Partial</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Dell/EMC</td>
<td>Dell Storage PS4210E</td>
<td>N/A</td>
<td>72Tb</td>
<td>Partial</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>NetApp</td>
<td>SolidFire SF38410(x2)</td>
<td>Software</td>
<td>84Tb</td>
<td>Full</td>
<td>Site-to-Site</td>
<td>N/A</td>
</tr>
<tr>
<td>Nimble</td>
<td>Nimble AF5000</td>
<td>Software</td>
<td>167Tb</td>
<td>Partial</td>
<td>Site-to-Site</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Midrange Solutions (Target >500Tb + Growth)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Solution</th>
<th>Encryption</th>
<th>Max Tb</th>
<th>HW Redundancy</th>
<th>DR</th>
<th>FDE/FIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP</td>
<td>HPE 3PAR StoreServ 8000</td>
<td>Hardware</td>
<td>4000Tb</td>
<td>Full</td>
<td>Site-to-Site</td>
<td>Certified</td>
</tr>
<tr>
<td>Dell/EMC</td>
<td>EMC Unity 500F</td>
<td>Hardware</td>
<td>7800Tb</td>
<td>Full</td>
<td>Site-to-Site</td>
<td>Certified</td>
</tr>
<tr>
<td>NetApp</td>
<td>NetApp AFF A700</td>
<td>Hardware</td>
<td>1800Tb</td>
<td>Full</td>
<td>Site-to-Site</td>
<td>Certified</td>
</tr>
<tr>
<td>Nimble</td>
<td>Nimble AF9000</td>
<td>Software</td>
<td>2212Tb</td>
<td>Full</td>
<td>Site-to-Site</td>
<td>N/A</td>
</tr>
</tbody>
</table>
• Scaling Storage Networks Wrap-Up
  ▪ The SDT has asserted in the past few webinars that vendors provide security and resiliency based on the scale of the environment
  ▪ Smaller scale environments do not offer as many enterprise grade solutions for security and resiliency
  ▪ Entry Level Solutions
    o Tend to lack hardware redundancy, have reduce encryption capability, and rely on other software to perform disaster recovery
  ▪ Midrange-Enterprise Solutions
    o Tend to be fully hardware redundant
    o Tend to have built in Site-to-Site disaster recovery capabilities
    o Tend to have better encryption features such as Hardware encryption and support for FIPS certified full disk encryption
  ▪ Since larger storage systems tend to have better security features, sharing infrastructure between CIP and non-CIP assets could in some cases increase the security and reliability of the systems.
Scaling Storage Networks

- **References for Vendor Comparisons**
Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection
• Cyber Asset Definition:
  - A *programmable electronic device (physical or virtual)*, including the hardware, software, and data in the device. *Each virtual machine and host is itself a distinct Cyber Asset.*

• The Storage hardware houses the data and is considered Underlay. Assumes the highest level of security (The CIP definition of Cyber Asset is inclusive of the data)
Data Protection

Storage Array

Management Console

Logical Disk #1 SCADA
Logical Disk #2 ICCP

Presentation SCADA
Presentation ICCP

Physical Interfaces

Storage Processors

Physical Disks

Storage Network
Data Protection

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: NEWAPP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks
Data Protection

ESZ DMZ: NEWAPP

ESZ PROD: SCADA

Physical Disks
• Controls Exist in CIP11
  ▪ Part 1.1 of CIP-011 is related to BCS Information identification and part 1.2 to BCS Information protection and handling procedures
  ▪ As currently drafted—both apply to physical and virtual environments

• CIP-011 Part 2.1 Requirement:
  ▪ Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset Storage Media
CIP-011 Part 2.1 Measure:

- Examples of acceptable evidence include, but are not limited to: Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying;
- Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.
• CIP-011 Part 2.2 Requirement

Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

• CIP-011 Part 2.2 Measure

  ▪ Examples of acceptable evidence include, but are not limited to:

    Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.
Data Protection Wrap-up

- The Cyber Asset Definition is inclusive of data
- There are two main ways to ensure data is destroyed
  - Destroy ALL physical media
  - Encrypt the data with security zone specific keys
- CIP11 has Controls that address the risks associated with information protection
  - The SDT believes the applicability of CIP11 as drafted is inclusive of multi-instance environments
Webinar 3 - Storage Summary

Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection
Questions and Answers