WHITE PAPER

Substation Management Platform Common Design Architecture

CONTENTS

EXECUTIVE SUMMARY

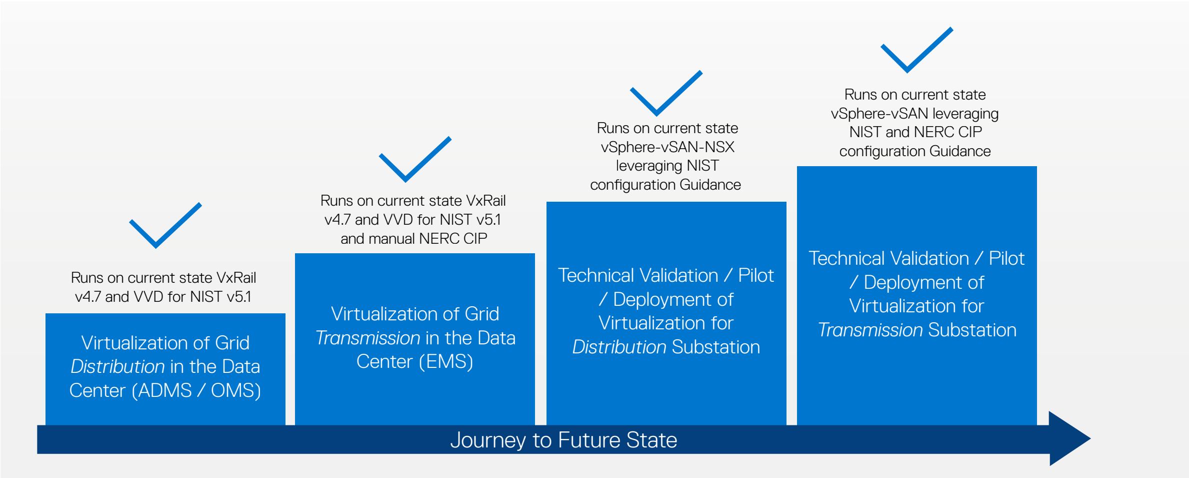
The utility industry is seeing unprecedented change in the utility grid, which is driven by a global transition to renewable energy, faster uptake of Distributed Energy Resources (DERs) and the need to support worldwide sustainability goals. The industry is undergoing an IT (Information Technology)/OT (Operations Technology) convergence to support the migration from a rigid OT-centric model to a more dynamic software defined, data-driven model.

The foundation for this IT/OT convergence is a robust enterprise-grade software-defined data center (SDDC) that can extend from the data center (control center) to the edge (substation), capable of supporting cloud-native and legacy (Window/Linux) x86 applications on a single platform while providing intrinsic security, compliance, and lifecycle management.

The term SDDC or virtual infrastructure describes the separation of physical hardware from the operating system(s) and application(s) leveraging the physical hardware. This layer of abstraction between compute, storage and network hardware gives administrators the advantage of managing pooled resources across the enterprise, allowing IT to be more responsive and agile to organizational and business needs.

The journey to a virtualized Grid Data center (Control Center) and Edge (Substation) can be an incremental process across both Grid Transmission and Distribution Operations in the Data center or at the Edge. Dell Technologies, VMware, and Intel are providing proven solutions to utility providers across four pillars (see Figure 1).

FIGURE 1. Transmission / Distribution Operations & Transmission / Distribution Substation

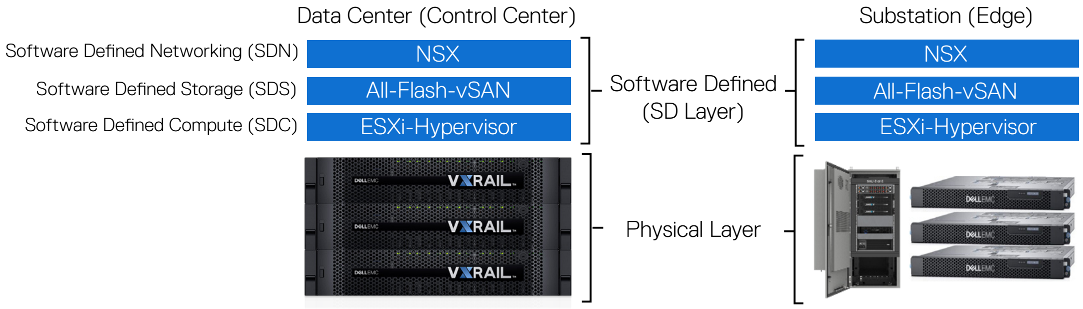

Runs on current state VxRail v4.7 and VVD for NIST v5.1
Virtualization of Grid *Distribution* in the Data Center (ADMS / OMS)
Runs on current state VxRail v4.7 and VVD for NIST v5.1 and manual NERC CIP
Virtualization of Grid *Transmission* in the Data Center (EMS)
Runs on current state vSphere-vSAN-NSX leveraging NIST configuration Guidance
Technical Validation / Pilot / Deployment of Virtualization for *Distribution* Substation
Runs on current state vSphere-vSAN leveraging NIST and NERC CIP configuration Guidance
Technical Validation / Pilot / Deployment of Virtualization for *Transmission* Substation
Journey to Future State

Data center virtualization can be accomplished for both grid transmission and distribution operations. Dell Technologies, VMware, and Intel® are providing utility providers with both non-NERC CIP (Distribution Operations) and NERC CIP (Transmission Operations) regulated environments. The foundation for the data center deployment is a VMware Validated Design (VVD) on the Dell EMC Hyperconverged VxRail infrastructure. The Dell EMC VxRail infrastructure powered by Intel® is specifically designed and built to fully leverage the VVD Blueprint architecture. This can be further enhanced with the VVD for NIST 800-53 Compliance Toolkit as a cybersecurity foundational baseline. With a few additional technology control settings, the environment can be further extended to meet NERC CIP (North American Reliability Corporation Critical Infrastructure Protection) compliance.

The product and services solution sets from Dell Technologies, VMware and Intel have been curated for optimized performance and deployment into the substations and grid data centers. Joint partnerships with the leading utility software vendors who provide both EMS (Energy

Management System) and ADMS (Advanced Distributed Management System) systems have been formed to further validate their specific application portfolios on the Dell Technologies, VMware and Intel infrastructure platforms.

Now, Dell Technologies, VMware, and Intel are turning our attention to the remaining two pillars on the journey to a virtualized grid data center and edge: distribution and transmission substations. The evolution of the substation is in its infancy and the best starting point is an enterprise grade infrastructure that can run at the edge, while using the same tools and retaining the same capabilities as the enterprise grade data center.


Data Center (Control Center)
Substation (Edge)
Software Defined Networking (SDN)
Software Defined Storage (SDS)
Software Defined Compute (SDC)
NSX
All-Flash-vSAN
ESXi-Hypervisor
Software Defined (SD Layer)
NSX
All-Flash-vSAN
ESXi-Hypervisor
VXRAIL
VXRAIL
VXRAIL
Physical Layer
DELLEMC
DELLEMC
DELLEMC

Traditional substation automation systems in electric utility substations are typically costly to maintain and inflexible. These systems do not promote a high degree of grid reliability and system resilience, cyber and physical risk mitigation, operational efficiency, safety, or emergency response and recovery.

With technical advancements in substation automation and IT/OT integration practices, virtualization can simplify substation automation systems and solve current industry challenges while addressing cybersecurity monitoring and response capabilities.

The remainder of this document is focused on the definition of a common design architecture for deployment of a hyperconverged infrastructure platform at the edge (substation) called a Substation Management Platform (SMP). SMP is a new term that is emerging to define a compact hyperconverged infrastructure with the same capabilities/functions as the data center.

OVERVIEW – SUBSTATION MANAGEMENT PLATFORM

The Substation Management Platform is a distributed hyperconverged infrastructure with the same data center enterprise-grade capabilities that fully leverages centralized management. At the core is server virtualization, which is accomplished using software called the hypervisor installed directly on the physical server. The hypervisor abstracts the physical hardware using virtual drivers that emulate the central processing unit (CPU), memory, networking, storage, and other physical devices. Virtual Machines (VMs) are presented with the virtual drivers that enable multiple operating systems to run simultaneously on the same physical hardware. The four core tenants of virtualization are:

- **Partitioning** provides the ability to run multiple operating systems on one physical machine, while dividing system resources between virtual machines.
- **Isolation** ensures fault and security isolation at the hardware level, with advanced resource controls to preserve performance.
- **Encapsulation** means the entire state of the virtual machine can be saved to files. Additionally, the VM can be moved and copied as easily as moving and copying files.
- **Hardware Independence** allows provisioning or migration of any virtual machine to any similar or different physical server.

VIRTUALIZATION BENEFITS INCLUDE:

- Reduced operational costs
- High reliability / fault tolerance
- Increased efficiency, flexibility and responsiveness
- Faster provisioning of applications and resources
- Greater business continuity and disaster recovery
- Simplified/centralized management

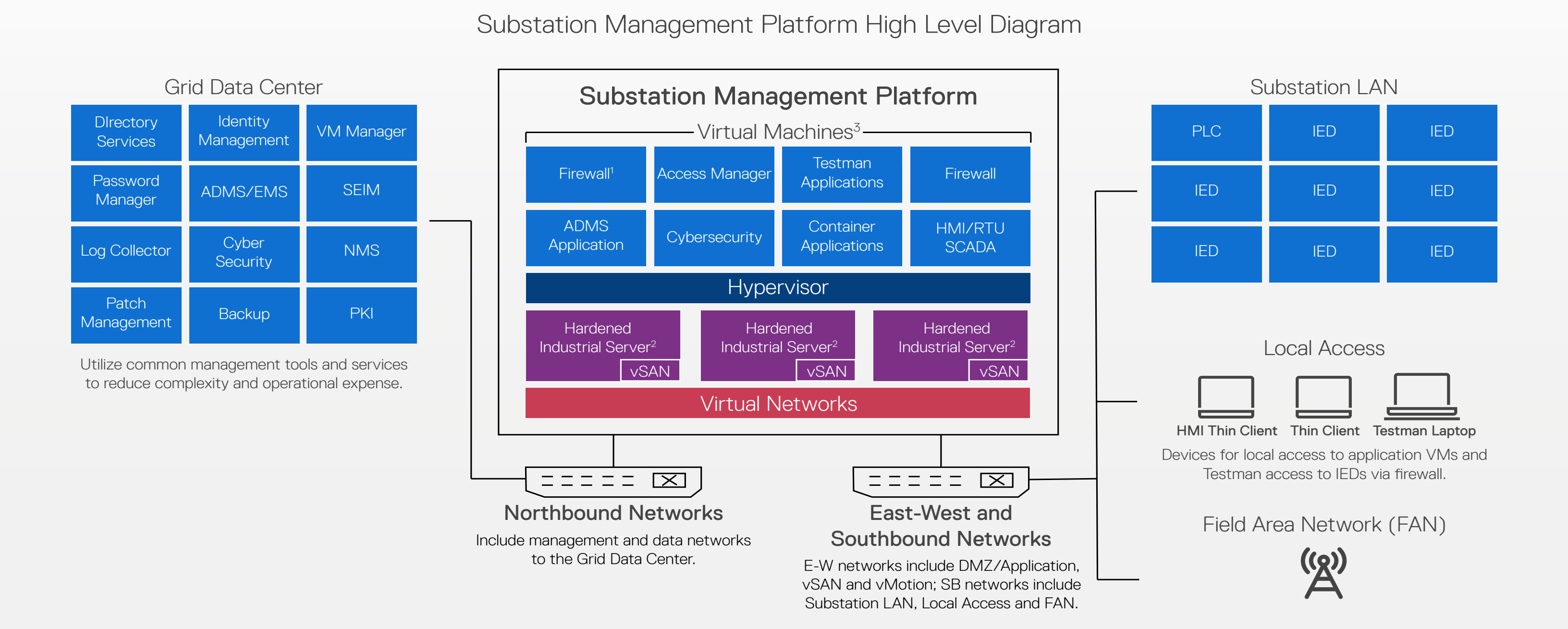
In the following sections, we identify the key considerations and components used for a standard Substation Management Platform, as depicted in Figure 2 - Substation Management Platform High Level Common Design Architecture Diagram.

INFRASTRUCTURE

Server

The chosen servers must be ruggedized, industrially hardened hardware that meet either IEEE 1613 - Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations or IEC 61850-3 - Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations. Both standards call for specific temperature operating ranges. The IEEE standard calls for fan-less devices while the IEC standard does make allowance for the use of fans for cooling. In addition, there are requirements for shock, vibration, Electro-Mechanical Compliance, and others. The server manufacturer must understand and provide certification that the product meets the requirements. For complete understanding of the standard requirements, you may obtain a copy of the standard from the IEEE or IEC webstore.

FIGURE 2. Substation Management Platform High Level Common Design Architecture Diagram


Substation Management Platform High Level Diagram
Grid Data Center
DIrectory Services
Identity Management
VM Manager
Password Manager
ADMS/EMS
SEIM
Log Collector
Cyber Security
NMS
Patch Management
Backup
PKI
Utilize common management tools and services to reduce complexity and operational expense.
Substation Management Platform
Virtual Machines[3]
Firewall[1]
Access Manager
Testman Applications
Firewall
ADMS Application
Cybersecurity
Container Applications
HMI/RTU SCADA
Hypervisor
Hardened Industrial Server[2]
vSAN
Hardened Industrial Server[2]
vSAN
Hardened Industrial Server[2]
vSAN
Virtual Networks
Northbound Networks
Include management and data networks to the Grid Data Center.
East-West and Southbound Networks
E-W networks include DMZ/Application, vSAN and vMotion; SB networks include Substation LAN, Local Access and FAN.
Substation LAN
PLC
IED
IED
IED
IED
IED
IED
IED
IED
Local Access
HMI Thin Client
Thin Client
Testman Laptop
Devices for local access to application VMs and Testman access to IEDs via firewall.
Field Area Network (FAN)

The type of processor, number of cores and amount of memory and storage will vary depending upon the application requirements. A typical 3 node cluster with virtual Human Machine Interface/ Remote Telemetry Unit (HMI/RTU), firewalls, Intelligent Electronic Devices (IED) management application and cybersecurity tools, would require an Intel® Xeon® processor, or equivalent, with a minimum of 8 cores running at ~2 GHz. and a minimum 32 GB RAM.

This common design architecture uses VMware vSphere as the hypervisor. To improve reliability and resiliency, a cluster of three servers is used. Additional nodes can be added to accommodate additional workload. Shared storage is required in a vSphere cluster so that data is available across all nodes of the cluster. There are currently no storage arrays on the market that conform to the environmental standards required in the substation. VMware's Virtual Storage Area Network (vSAN) software is used to accommodate the shared storage requirement. vSAN manages data replication across the server nodes as well as access to the data from each node. Data access and replication are accomplished across a separate, non-routable, VLAN dedicated for vSAN. The system must have a minimum of two SAS or SATA SSD or PCIe flash devices and one SD or SATA DOM device. The SD or SATA DOM device will be used to boot the ESXi host and must be a minimum of 4GB. The SSD or PCIe devices will be used for the cache disk and VM data storage. The cache disk must be at least 10 percent of the size of the data storage disk.

Client

Many electric utilities have a policy that requires personnel who enter the substation to log on to the HMI upon entry into the control building. A virtualized HMI will not have a keyboard and monitor used to log in. To remedy this, the use of a thin client terminal is required. A thin client terminal, such as the Intel-based Dell Wyse 3040, uses the ThinOS operating system firmware and can be managed by a central management utility. Management functions include configuration management and remote firmware updates. For technical support personnel, "Shadow session" functionality can be useful by being able to see what the on-site user is seeing during a support session.

Identity and Access Management

For Identity and Access Management in the SMP, we recommend you use the same tools as used in the data center. The use of active directory and other authentication methods like RSA are supported, and the use of centralized tools reduces complexity and operational overhead.

In the case of a network down situation, the use of a "Break Glass" local ID and password will allow the operator or testman to access the local system. Local IDs are created with the needed access controls. These IDs can be managed by your specific centralized password management system. When needed the user would call into the help desk and request the Break Glass ID and password. The help desk would determine the proper ID upon verification of the user's identity. The checked-out password for the used Break Glass ID would then automatically be changed at the proper interval when the network has been restored.

Network Impacts

Network segmentation is a key practice for cybersecurity. In this design, we separate the communication networks both physically and with the use of VLANs. See Figure 3 Substation Management Platform High Level Network Diagram for a higher-level perspective on the network, and Figure 4 Substation Management Platform Network Diagram for more details. Access to these networks is regulated by the use of firewalls, both in the data center and in the SMP. We propose the use of virtual firewalls running in a highly available (HA) configuration as VMs on the SMP cluster. Since there are a relatively small number of VLANs, the use of the virtual firewall's router function is sufficient and will reduce cost and complexity.

Separate physical switches are recommended to physically separate the northbound WAN traffic from the southbound substation traffic. This is a requirement in a NERC-CIP environment. NERC-CIP-005 requires physical separation and access controls to create the boundary of the Electronic Security Perimeter (ESP). If using a redundant pair of switches, two 1 GB fiber ethernet ports are required for each server node in the SMP cluster on the northbound switches. On the southbound switches either two 10 GB fiber ports or six 1 GB fiber ports are required per server node if using redundant switches. Typically, there will be a minimum of three server nodes in the cluster. In addition, a number of 1 GB ports will be required on the southbound switches to connect the Substation LAN, Thin client devices, transient devices, IPMI ports, and switch management ports.

Northbound Networks

Northbound networks are used for communication from the SMP to the main data center and are on a separate physical switch from the southbound networks. This includes a management network and a general data network. The management network is used to connect to the hypervisor and the firewall management interfaces. These interfaces generally can be configured to use TLS encryption and are limited to these interfaces, so no transport encryption is required. The data network is used for all other communications to and from the SMP. This includes both encrypted and unencrypted data. To protect the privacy and integrity of the unencrypted data, we propose the use of an IPSEC tunnel on this transport network. This IPSEC tunnel can be instantiated between the virtual firewall in the SMP and the firewall in the main data center.

FIGURE 3. Substation Management Platform High Level Network Diagram

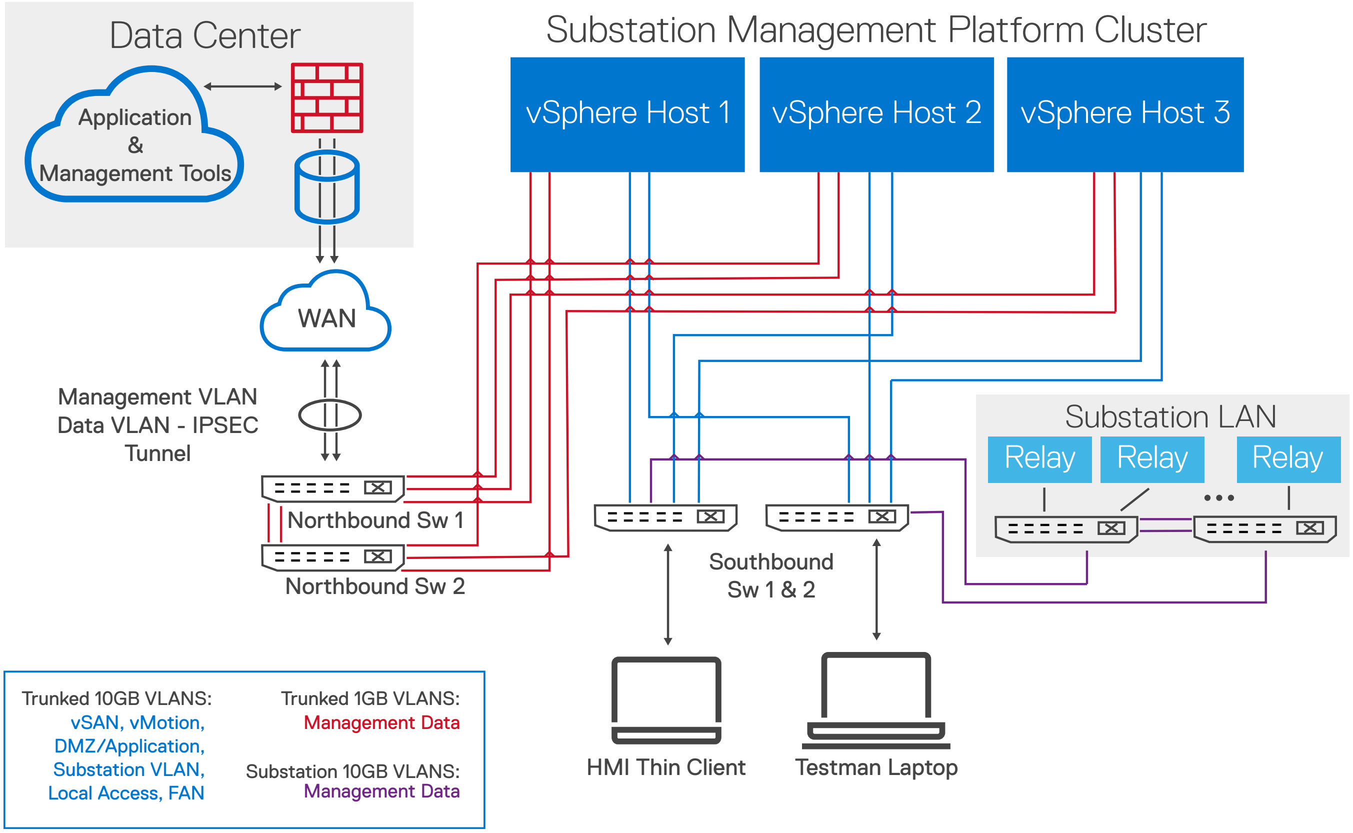
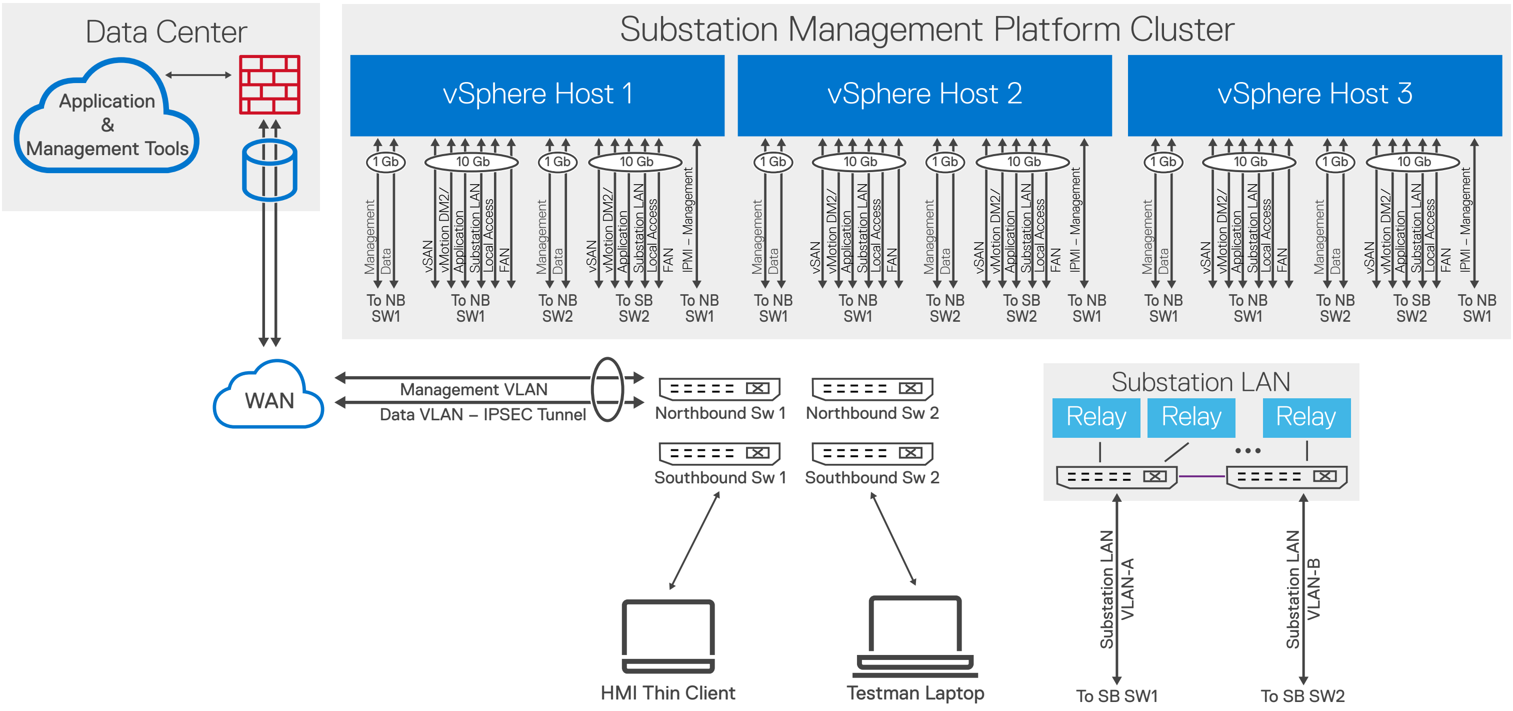


FIGURE 4. Substation Management Platform Network Diagram



Southbound Networks

The southbound networks serve in the SMP and include the following.

- vSAN – This is a non-routable network used to carry storage traffic between the compute nodes.
- vMotion – This is a non-routable network used for the migration of live VM workloads between the compute nodes.
- DMZ/Application – This network is used for application and management VMs. It is considered a DMZ since it will be used as a demarcation point for communications from the data center to the IEDs.
- Substation LAN – This network is used for the IEDs in the substation. This network should only be routable to the DMZ/Application network. Any communications to the IEDs from any other network will then require some form of proxy in the DMZ/Application network.
- Local Access – This network will have the thin client devices and ports for the testman or operator to connect authorized transient devices to the network.
- Local management – This network is used to connect local management interfaces such as IPMI and the substation ethernet switches.
- Field Area Network (FAN) – This optional network can be used to connect to devices beyond the substation fence such as distributed energy resources (DERs), remote fault indicators (RFI), or remote intelligent switches (RIS).

Firewall

This architecture uses a virtual firewall running in the VMware cluster. This firewall is not integrated with NSX in order to meet NERC-CIP requirements. While true that installations in distribution substations (as of this writing) are not subject to meet NERC-CIP requirements, we chose this configuration to have a consistent architecture for both transmission and distribution substations. For operational consistency, it is recommended to use the same manufacturer's virtual firewall as is running in your data center. This will enable the same management tool set and policies to be used in both the data center and substation.

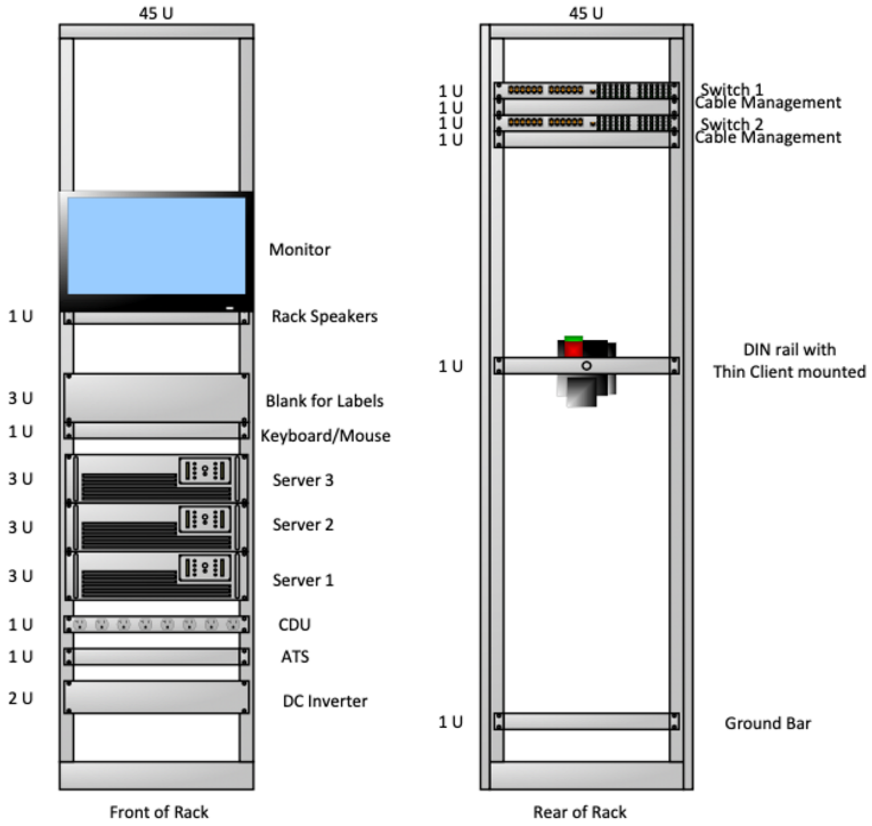
The virtual firewall is configured in a High Availability (HA) pair to protect against failure and to enable software upgrades without the need for a planned outage. The firewall's virtual router is used for network segmentation due to the low number of VLAN's required and the relative low bandwidth requirements. Ensure that the virtual firewall chosen supports the capacity required for your specific needs, sessions, rules, security zones and IPSEC tunnels.

Rack and Power

The Substation Management Platform will be located in the control building in the electric substation. These control buildings were typically designed to support equipment mounted in 19" two-post racks. Consideration must be given during the selection of the hardware components to ensure that it will fit in the available space. Equipment used in the SMP that is more than about 18 inches deep will likely require a four-post mounting system. It is recommended that the chosen rack meet or exceed the IEEE 693-2018 standard for Seismic testing and is braced properly. See Figure 5 - Sample Rack Elevation.

Most substation equipment rooms are powered by DC battery systems. Typical voltage for these systems is 48, 125, or 250 VDC. 125 VDC is the most common. 120/240 VAC may also be available but is subject to outage. If using AC-powered devices, the use of an inverter attached to the station battery system is recommended. The use of an automatic transfer switch may also be considered to provide redundant power feeds to the equipment. The redundant feeds would be station AC power and station DC power via the inverter. The existing battery plant in the substation control room is sized to provide battery power for a minimum duration, usually 12 hours. Consideration must be given when adding additional equipment to ensure that the battery system has enough capacity to support the additional load while maintaining the required duration. All powered equipment must be connected to the station ground bus separately from the power cord ground.

FIGURE 5. Sample Rack Elevation



CONCLUSION AND NEXT STEPS

Transforming and modernizing the energy industry is at the forefront of utility operational objectives. Traditional architectures in electric utilities are typically costly to maintain and inflexible. Utilities seeking to modernize the Grid and enhance situational awareness, require a new approach, one that leverages a common, virtual architecture from the data center to the edge providing more agility and higher levels of interoperability, security, and reliability.

This Common Design Architecture paper shows how the Dell Technologies, VMware and Intel standard Substation Management Platform is leveraging emerging technologies to strengthen and modernize the grid, to improve reliability, security and safety, and operational practices. The use of machine virtualization in the electric utility grid is having a major impact on electric utilities' operations, and VMware machine virtualization is the foundation of the Substation Management Platform.

The Substation Management Platform solution and technology offers a more flexible, cost-effective, and lasting solution to deliver increased grid reliability and system resilience. Through proven projects delivered to date, we have found there is clear ROI evidence in the electric utility industry for moving away from today's hard-wired, traditional substation architectures to a virtualized architecture on a standardized Substation Management Platform. The benefits are reduced overall costs, including hardware, installation, engineering, and maintenance; fewer wiring and terminations, which minimizes potential electrical hazards to improve safety; server redundancy and reliability; automated self-monitoring and alerting; and enhanced cybersecurity.

Please contact your Dell Technologies, VMware or Intel representative for more information on how we can provide a comprehensive portfolio of products, solutions, services, and partnerships for electric utility companies to become agile and dynamic producers and suppliers of increasingly clean, efficient resources.

[1] Virtual FIrewall used for network segmentation and provides for ESP in NERC-CIP environment.
[2] Servers must meet IEC61850-3:2013 standard for Substation Devices.
[3] DMZ/Application network has access to Data Center and Local networks.

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

DELL Technologies