21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2017 Grid of the Future Symposium

A Hybrid Communications Network Approach for Advanced Applications on the Modern Grid

J.-P. KNAUSS
National Grid
USA

SUMMARY

As the industry continues the journey to modernize the North American electrical infrastructure, the need for robust communications and secure network connectivity is becoming of vital importance. Effective communication solutions will be the cornerstone of an infrastructure designed to support the vast array of both existing and future advanced applications that will be needed for a modern grid. Over the years, National Grid has utilized various cellular communication technologies, largely in a hosted (SaaS) environment, for remote visibility and control of thousands of devices across their distribution, sub-transmission, and transmission systems. Continuous technological developments, coupled with relatively short product lifecycles in the cellular communications industry, have posed significant challenges to the industry responsible for maintaining reliable and secure grid connectivity for situational awareness and system operations. With aggressive plans for grid modernization afoot, National Grid has strategically taken the opportunity to create a secure, hybrid communications network capable of supporting both current and foreseeable future needs. The following paper describes the required infrastructure development and functionality of a secure and flexible, hybrid communications network that will allow National Grid to deploy advanced sensing and control equipment as well as associated applications.

KEYWORDS

Telecommunications, Communications, Secure Communications, Hybrid Communications, Cellular, 4G, LTE, Network, Integration, Situational Awareness.

John-Paul.Knauss@nationalgrid.com

INTRODUCTION

Historically, National Grid has remotely monitored and controlled thousands of intelligent devices on their distribution, sub-transmission, and transmission systems through a combination of both private networks as well as cellular communications platforms that were provided in a hosted, Software as a Service (SaaS), environment. While private networks (e.g. RF, fiber, etc.) are generally the preferred telemetry solution, it can be difficult to justify the required infrastructure build-out in remote areas. For such remote facilities, leveraging existing third-party cellular infrastructure has proved to be a viable solution. Over the years, the nature of the rapidly evolving wireless telecommunications industry has presented significant challenges to entities that are in charge of maintaining reliable and secure grid connectivity for situational awareness and system operations.

Although the general perception is that the largest impact to the overall cellular evolution may reside with the millions of cellular phone customers, many utility and public safety organizations, including alarm companies that use these systems to alert police or fire departments to emergencies at homes or businesses, are also significantly impacted. For National Grid USA, the evolutional impacts of cellular based communication systems have been significant due to the widespread deployment of cellular based radios for enhanced situational grid awareness, dating back as far as the turn of the century. From 2002 to 2007, for example, thousands of grid facing protection and control devices were integrated to SCADA operations via earlier cellular technologies (e.g., analog and early digital modems). The arrival of the "analog sunset" presented several challenges to maintaining remote connectivity as thousands of diverse locations required hardware upgrades to the "newer" 2G digital platform in order to maintain connectivity for remote system operators. Over the following years a blend of both 2G and 3G cellular radios were deployed to bridge the evolutional gap. In 2016, National Grid was again faced with a similar dilemma due to the sunset of 2G cellular technology throughout the Telecommunication Industry.

At the forefront of modernizing the power delivery infrastructure in North America, flexible and sustainable communications solutions are a basic requirement, as large amounts of advanced sensing and control devices are being deployed in support of next-generation situational awareness and advanced control systems. Using the lessons learned throughout this journey of technological evolution, National Grid USA has taken the opportunity that a modernization plan implementation has presented, to embark on the design and implementation of a secure, hybrid, communications network that can support its present and future applications.

COMMUNICATIONS NETWORK DESIGN

The experience gained through "smart grid", Volt / VAr Optimization (VVO), and new technology demonstration pilots, showed National Grid that the future of communications technologies deployed across the system would require a flexible model. From a functionality perspective, there is a need to support various types of communications technologies as application requirements can vary greatly, and dictate acceptable solutions. This type of approach will also provide a solution for the challenges due to the constant technological changes, such as the sunset of legacy 2G, and soon to be 3G cellular technologies. In general, the challenge was to be able to effectively provide a communication infrastructure that would have the following characteristics, at a minimum:

1) Able to maintain remote visibility and control of ~1800 distribution and sub-transmission line reclosers and automated switches that were currently integrated to SCADA systems; and
2) Being conducive to integrating newer control technologies such as advanced switched capacitor controls, voltage regulator and loadtap changer controls, advanced sensing technologies, and PQ monitors.

In terms of solution architecture, National Grid had to take a well thought out, and careful approach, to align with the expectations from customers and regulators while specifying a level of quality that was reasonable. Modern network architectures for system critical operations require a high degree of availability, reliability, serviceability, security, and redundancy with varied degrees of cost and complexity. A careful design pursued to fulfil the fundamental requirements and to ensure that associated systems utilizing this network would remain operational should primary components and/or equipment experience a disturbance or failure. Working with their Communication business partner, Private IP (PIP) services were utilized to create a new network with secure connectivity and end-to-end integration to back-office systems [1]. This layer 3 MPLS virtual private network solution facilitates secure connectivity to multiple hub locations, enabling system redundancy, and failover capability (refer to Figure 1).

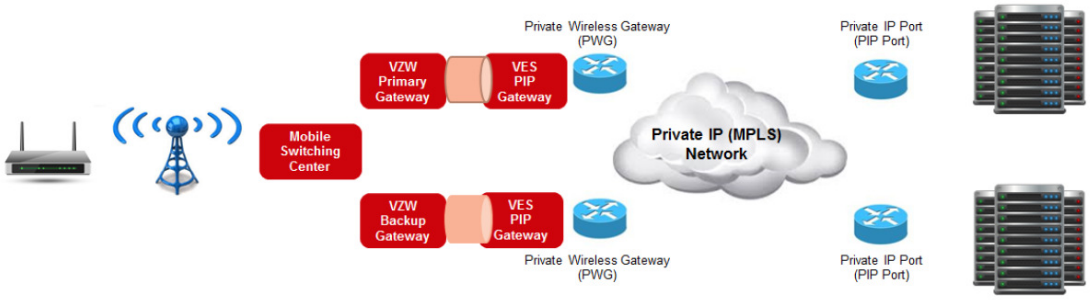

Figure 1 – Verizon PIP Private Network Implemented

With a varying service territory inclusive of existing pockets of private RF infrastructure, as well as remote locations where further network buildout can be difficult to justify, the concept of a hybrid connectivity model was critical for sustainability. Furthermore, network resiliency and scalability were also key considerations as National Grid looks towards future grid modernization plans [2-3]. Through careful planning and design, a network architecture was developed that would allow data from field devices to integrate to both primary back-office systems (e.g., data concentrators, SCADA, management portal, etc.) as well as secondary (backup) facilities should they be warranted. New virtual routing and forwarding (VRF) solutions were identified to establish desired connectivity to all required facilities, including both primary and backup System Control Centers, and Data Centers (refer to Figures 2-3).

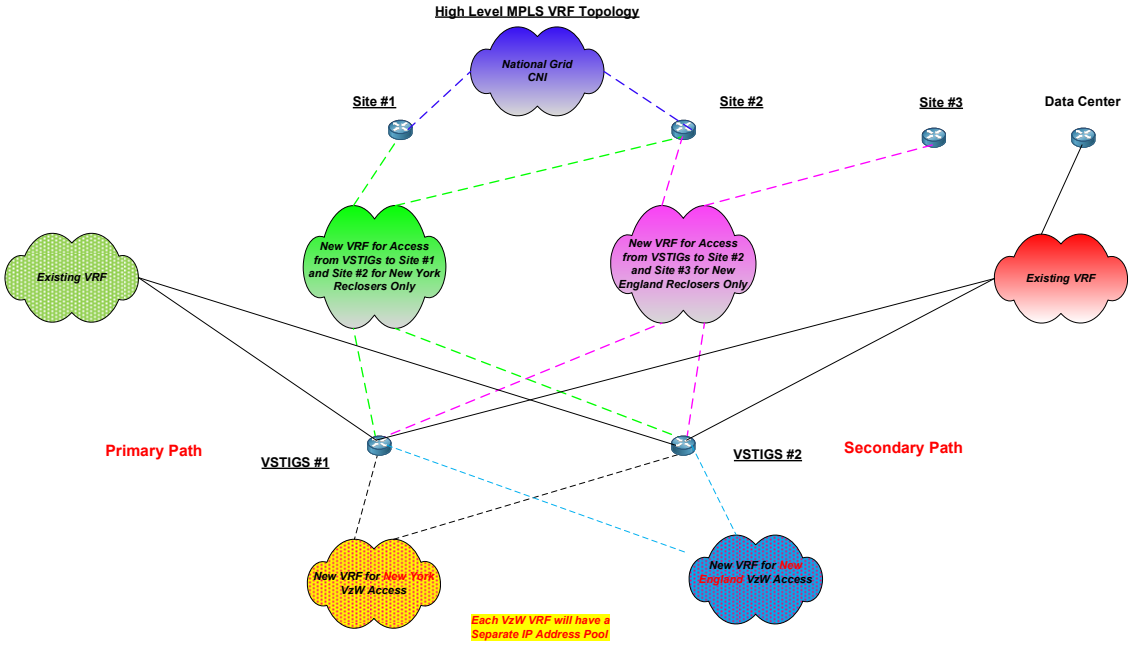

Figure 2 – High Level Network Architecture Overview

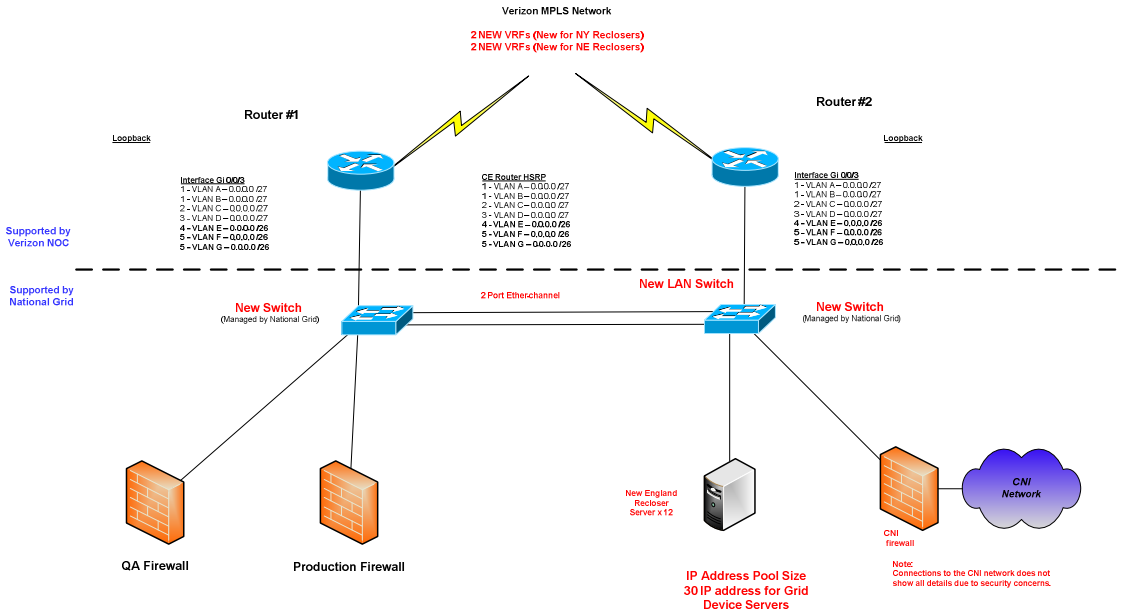

Figure 3 – Single Facility Physical Technology Model Example

The field area network architecture focused on integrating both 4G LTE / LTE-A cellular connectivity as well as several private communications mediums (i.e. numerous RF technologies, microwave backhaul, MPLS, Fiber, etc). Modern hardware solutions, software-defined functions, and field upgradable Network Interface Controllers (NICs), help to address the fast-paced nature of evolving network technologies. A Multiservice-Connect Router platform was selected for remote applications requiring cellular based connectivity [4]. Engineers at National Grid developed an innovative configuration file for these cellular routers that supported routing to both primary and secondary systems. Given the varying nature of both legacy and modern control equipment deployed across their service territory, both serial and Ethernet connectivity was required. To help address this, the router's port forwarding functionality, on-board terminal server, and firewall, was leveraged to simultaneously accommodate both serial and Ethernet communications in a single, secure, package. This approach results in a truly "plug and play", IP addressable, solution for any device on the network.

With the rapidly increasing population of sophisticated sensing and control devices, it was only natural to raise concern about the ability to reasonably manage this volume of new equipment, device addressing (e.g., TCP/IP, DNP, etc.), and associated interfaces. As a means to help aid in device and address management for integration into SCADA and data historian systems, new data concentrators were leveraged as an interface buffer to provide both network isolation and ease for future system considerations (e.g., ADMS, DERMS, etc., refer to Figure 4).

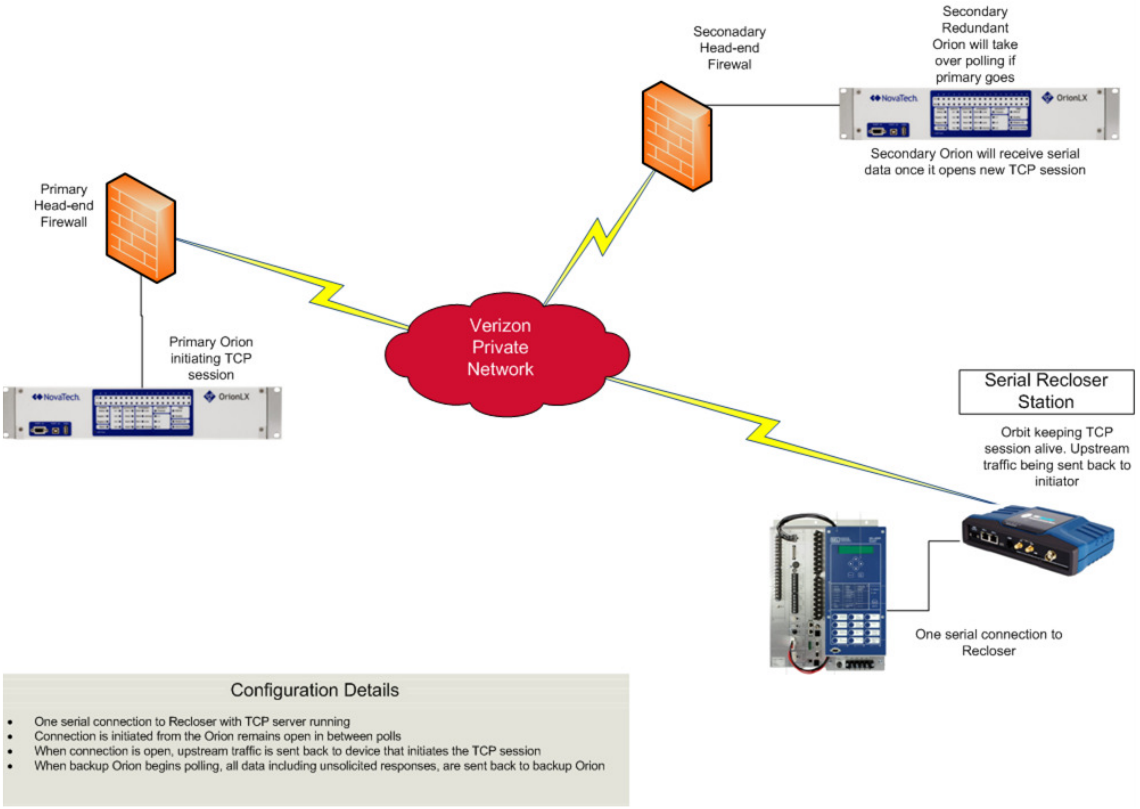

Figure 4 – Device Connectivity Example

These data concentrators are managed and maintained by National Grid's Distribution Control & Integration Engineering team and processes were established for new device integration requests.

Cyber-security was embedded in the entire architecture design from the very beginning. National Grid's Digital Risk & Security team was engaged in all network design phases, where items like firewall rules, protocols, applications, and tools all went through rigorous screening, testing, and approval processes. The design included integration of the entire network to National Grid's Cyber-Security Operations Centre for continuous monitoring and support.

NATIONAL GRID IMPLEMENTATION

With a secure network design in place, the first step was to begin implementation of the required backbone network changes and upgrades. This effort required carefully coordination with a broad group of stakeholders as components of existing networks, with production applications running on them, required changes and/or upgrades. Due to the complexity of the new network design (e.g., ~ 90 required network changes and upgrades) and strict risk management policies in place, this implementation took approximately twelve (12) months to complete. Testing was performed both prior to a given network change and after the change was implemented to ensure that no adverse impacts were realized as a result of the corresponding work. Network updates were performed individually with a forty-eight (48) hour testing and evaluation window following initial implementation. Once all network aspects were complete, thorough testing of the end-to-end architecture commenced to verify distribution field asset data was safely and securely integrated into Control Centers and management systems. Network changes and corresponding testing was generally completed outside of normal business hours as an added safeguard.

Additional hardware components (e.g., data concentrators, modems, installation kits, etc.) were specified, tested in a controlled laboratory environment, and then procured. Detailed technical installation manuals and training materials were then developed and delivered to Operations and Engineering stakeholders across the Company. Coordinating the installation, provisioning, and commissioning of the communications hardware was a significant challenge as each Operations platform had nuances in negotiated labor agreements; this required careful consideration during process development and implementation phases.

Working with the procurement team, a supplier was selected and agreements were put in place to have all hardware pre-programmed with National Grid's Engineering configuration file and ready for direct installation. Innovative thinking on this effort resulted in significant savings on cost and installation time. In addition, processes for assignment of addressing for field devices were developed and rolled out for National Grid's Critical Infrastructure systems (refer to Figure 5). An automated data repository system was established to track, provision, and manage new field device activation requests.

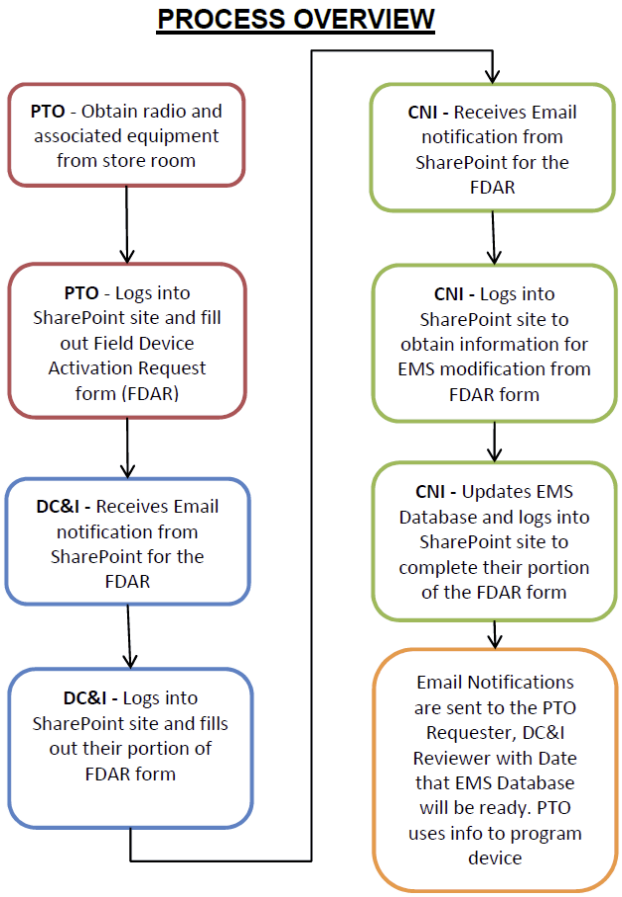

Figure 5 – Field Device Activation Request Process Flow Chart

In areas where the case for private RF solutions was justified (e.g., densely populated areas with high device counts and reasonable terrain, stringent availability requirements, etc.), this network back-bone was used to integrate the equipment in the same fashion. To-date, National Grid has integrated a 700MHz. narrowband RF system on the island of Nantucket, several 900MHz. licensed spread-spectrum systems across their Massachusetts and Rhode Island operating areas, and a 3.65GHz WiMAX network in their "Worcester Smart Energy Solutions" demonstration project.

This design supports flexible and sustainable field communications solutions for the large amounts of advanced sensing and control devices that are being deployed in support of next-generation situational awareness and control.

RESULTS

Through careful design and execution of a sophisticated network backbone, National Grid created a hybrid infrastructure that is capable of integrating different remote communications technologies in a scalable environment. Network redundancy offers new levels of service for mission critical system operations at the distribution and sub-transmission levels. In day-to-day application, the faster network speeds and increased throughput realized through hybrid 4G/LTE/LTE-A cellular platforms and private telecommunication solutions facilitates enhanced functionality for significant gains in operational efficiency. As an example, remote management of field devices (e.g., base configuration, device security, etc.) can now be done through a secure corporate portal. This remote portal can now be utilized for device configuration, troubleshooting and event record retrieval without the need to dispatch a physical crew to a given remote destination. Furthermore, network and security management is now embedded in the design of the network architecture allowing for real-time monitoring and proactive action should anomalies be detected or when general maintenance is required. Device logs are integrated into National Grid's Cyber-Security Operations Center (CSOC) with continued plans for added functionality. This results in a significant reduction in both time and effort for compliance reporting purposes. The system data from National Grid's field devices is routed through secured interfaces to SCADA systems via new banks of data concentrators. Centralized applications can interface to the secure network through various channels and protocols allowing for flexibility in system integration. The new data concentrator architecture is capable of running advanced applications such as Fault Location, Isolation, and System Restoration (FLISR) with user-defined parameters for ultimate flexibility in automation and control.

While the legacy telemetry solution employed for National Grid's distribution and sub-transmission devices met the need for basic SCADA functionality, modern systems and advanced applications require lower latency, as well as higher bandwidth and availability, to achieve the desired functionality. This new network approach offers significant functional enhancements to support current and future application needs for reliably serving customers on the modern grid (refer to Table 1). All of this was achieved while realizing significant cost savings when compared to the previous hosted telemetry solution.

	FUNCTIONALITY						
	SCADA	**Near Real-Time Data**	**Remote Record Retrieval**	**Remote Configuration**	**Remote Device Troubleshooting**	**Advanced Applications Support**	**Data Historian**
Legacy Telemetry Solution	YES	NO	NO	NO	NO	NO	LIMITED
New Network Architecture	YES	YES	YES	YES	YES	YES	YES

Table 1 – Network Functionality Comparison

SUMMARY

The deployment of a secure, hybrid, communications network that is capable of supporting advanced applications on the modern grid has been presented.

The conceptual design and implementation of this new network architecture makes use of best practices and lessons learned through experience with “smart grid”, Volt / VAr Optimization (VVO), and new technology demonstration pilots. This network approach has proven successful in integrating several communication technologies of diverse nature to a common core infrastructure. By doing so, a wide number of new remote communications technologies were able to be implemented quickly and at a significantly reduced cost.

Since deployment in December 2016, National Grid has over 1400 devices integrated via both cellular and private RF technologies. System Operators have near real-time status, control and data to be archived for future needs. Control & Integration Engineers and technical support personnel now have the ability to securely establish remote communications to equipment for event record retrieval, device troubleshooting, and even configuration and settings updates. Security logs are continuously monitored for anomalies and potential vulnerabilities. National Grid has realized significant operational efficiency gains through reductions in required time to complete several tasks that previously required sending a crew on-site.

This network is serving as the foundation for National Grid’s modernization efforts in support of applications such as Distribution Automation (FLISR), VVO and future ADMS and DERMS applications. There are currently two VVO systems that have leveraged this network via cellular based connectivity; one in the state of Rhode Island, and the other in upstate New York. In addition, National Grid is currently planning to deploy a centralized FLISR scheme, where the automation algorithms reside at the data concentrator, with construction scheduled to commence in spring of 2018.

As we continue along a journey to modernize the North American electrical infrastructure, robust, flexible communications and secure network connectivity are fundamental requirements to effectively operate and manage grid assets and to satisfy the increasing expectations of its customers. Innovative and novel implementations such as the one presented here, help to ensure flexibility, resiliency, and scalability as we look towards the future of an ever evolving communication space.

BIBLIOGRAPHY

[1] Verizon Partner Solutions, https://www22.verizon.com/wholesale/solutions/solution/Private+IP+(PIP).html, [Accessed July 2017].

[2] Massachusetts Executive Office of Energy and Environmental Affairs, http://www.mass.gov/eea/energy-utilities-clean-tech/electric-power/grid-mod/grid-modernization.html, [Accessed July 2017].

[3] New York State Reforming the Energy Vision, https://rev.ny.gov/, [Accessed July 2017].

[4] GE Grid Solutions, http://www.gegridsolutions.com/communications/catalog/MDSOrbit.htm, [Accessed July 2017].