comnet
Communication Networks

WHITE PAPER:

Cellular Routers for Use in Substation SCADA and Distribution Automation Communications Networks, & for NERC-CIP-5 Compliance of Critical Electrical Utility Infrastructure

By Bruce M. Berman
ComNet Vice President of New Business Development

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA | WWW.COMNET.NET
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

INTRODUCTION

With the continuing growth of the Smart Grid Initiative, many electrical utilities are now looking for new approaches to connect remotely-located substations, renewable energy sources, and their distribution automation equipment onto a secure and common network. Although a fiber-optic communications network is the first choice for connecting these facilities to a central control and monitoring location, due to its inherently secure connectivity and immunity from the severe levels of EMI typically encountered within the electrically-noisy environment of a substation, or the near proximity of overhead high-voltage three-phase power lines used for distribution, the expense, right-of-way issues, and difficulty of constructing the fiber infrastructure to distant and widely separated facilities is frequently prohibitive and not practical.

Managing and accessing remote equipment in many physically diverse locations can be costly and difficult, along with the obvious necessity of maximizing the power transmission and distribution system uptime and the reliability of power delivery, while reducing operating and maintenance costs. These requirements are a major consideration for many utilities.

Faced with ever-increasing customer service expectations and rising system performance oversight, as well as growing interference issues affecting their existing radio and wireless services, many substation SCADA, distribution automation, and remote metering engineers are now viewing cellular routers as a viable alternative to the popular radio links deployed for use in the 900 Mhz (licensed and license-free service), 3.6 Ghz, and 5 Ghz frequency bands, as well as T-1/DS-1 and E-1 wired-telephony or microwave radio links.

With the advent of industrial-grade and substation-rated, IEC 61850-3 compliant cellular routers, it now becomes practical and cost-effective to provide a simple-to-implement, reliable, and highly secure communications network linking the substation SCADA network, renewable energy generation facilities, the distribution automation network, and remote metering to the utility's central control and monitoring location.

THE CELLULAR ROUTER DEFINED

A cellular router is a communications networking device for uplinking Ethernet data or a combination of Ethernet and RS-232 and RS-485 serial data, through an encrypted broadband cellular radio WAN (Wide Area Network) to the PSTN (Public Switched Telephone Network), via the user's selected 2G/3G or 4G LTE cellular service provider. In addition to the internal cellular radio, these devices may include a combination of a layer 2 managed Ethernet switch, as well as a layer 3 router with a secure firewall for protection against the possibility of a cyber-security breach or intrusion to the network. Serial data capability is desirable for those applications where legacy RTUs, IEDs, metering, protective relaying, data logging, or other terminal equipment is to be seamlessly connected to the network, without the need for an outboard terminal server unit. A fiber-optic interface utilizing field-installable SFPs (Small Form-Factor Pluggable) optical transceivers may be included, for a highly versatile and future-proof connection to any multimode or single-mode cable plant, for use as either the primary or secondary fail-over communications circuit in the event of a loss of the cellular radio link.

In many locations globally, the cellular communications infrastructure is already present, with essentially instant access to a worldwide network. A highly reliable, secure, and continuously available connection is thereby provided.

Typical Substation-Rated Cellular Routers

ENVIRONMENTALLY-HARDENED/RUGGEDIZED EQUIPMENT: INDUSTRIAL-GRADE & SUBSTATION-RATED

Cellular routers fielded "inside of the fence" for substation automation and SCADA applications must of necessity be truly substation-rated, so as to be reliable over the long-term in this extremely difficult and severe operating environment. The majority of the cellular routers currently available to the utility industry are industrial-grade, and are rated for out-of-plant service only; they are not intended for deployment within the extreme EMI substation environment. ComNet is one of the few suppliers that offers a family of cellular routers tested and certified to the requirements of IEC 61850-3 (for Ethernet communications equipment deployed within an electrical substation), as well as IEEE 1613, Class 2.

For most distribution automation applications, particularly where the equipment is to be pole-mounted and in the near-field of high-voltage overhead power lines, the environmental hardening requirements of IEC 61850-3 do not apply, but these requirements should be considered as a guideline. Conventional industrial-grade routers with sufficient EMI/RFI protection, and voltage transient protection on the signal interface and input power rails, will generally be found adequate for these applications. Users with concerns about deploying cellular routers in those distribution automation or remote metering installations where EMI and voltage transient issues may be a significant factor, and desiring the highest possible level of system reliability, are advised to consider a substation-rated/IEC 61850-3 compliant device.

THE NECESSITY FOR HIGHLY RELIABLE COMMUNICATIONS, AND NETWORK FAIL-OVER

Many system operators, particularly those with remotely located substations, have the ability to provide fiber-optic connectivity to the cellular router through an existing optical network. The fiber optic link is generally used as the primary communications path between the substation and the utility's head-end control and monitoring facility. In the event of a failure within the optical cable plant, automatic fail-over to the cellular radio link occurs, providing an extremely high level of fault tolerance, and significantly reducing the possibility of a single point-of-failure within the network from creating a complete loss of communications between the substation SCADA equipment and any other location.

For even higher levels of network availability and reliability, some cellular routers may be equipped with the provision for two SIM (Subscriber Identity Module) cards, for operation with two separate cellular service providers. In this example, one SIM card is allocated to Verizon, and the other to AT & T. The primary cellular communications link may be via the Verizon system, and if that link should experience a failure, such as the cellular service provider's site dropping off of the network, the router will automatically fail-over to the secondary service provider, which in this case would be AT & T. Minimal to zero connection loss to the cellular WAN is then maintained.

OPERATING POWER CONSIDERATIONS

Within the electrical substation, operating power for the SCADA system and other ancillary equipment is derived from unconditioned nominal 24 VDC, 48 VDC, or high-voltage (88 to 300 VDC) station storage battery buss supplies. For distribution automation applications, where the equipment is pad or pole-mounted, typical operating voltages available for the communications equipment/cellular router are typically nominal 12 VDC, 24 VDC, or 48 VDC.

Ideally, the cellular router should be capable of operating directly from these sources of prime operating power, and without the need for any external power supply, thereby simplifying and improving the system design, and reducing the level of system integration. Elimination of an external power supply may be a major consideration for distribution automation applications, where the cellular router and other equipment are pole-mounted within a weather-proof enclosure with limited space.

Redundant power supply inputs may be available for these devices. Utilizing two separate operating power sources provides an extremely high level of reliability; if one of the two power inputs should fail, the other power source is available to provide uninterrupted operating power to the router, with minimal to zero loss of connection to the cellular WAN.

EQUIPMENT HOUSING AND ANTENNA REQUIREMENTS

As this equipment is usually either industrial-grade or substation-rated for deployment in out-of-plant operating environments, the compact and small form-factor cellular router may be installed within any unconditioned weather-proof enclosure with a minimum ingress rating of IP67. The mechanical configuration for these routers may be either DIN-rail mountable, or flange-mount for panel installation. Thermal loading is minimal, with typical heat dissipation on the order of 12 watts or less, depending upon the configuration and complexity of the equipment. Routers where the cellular radio antenna is affixed to the router itself, must be installed in a non-metallic enclosure to prevent serious attenuation/signal loss to the cellular RF (radio frequency) transmitted and received signal.

Unlike conventional cellular telephones, which employ omnidirectional antennas, cellular routers for use in substation SCADA networks, renewable energy generation facilities, remote metering, or in distribution automation applications, are not mobile devices; they are utilized exclusively in a ground-fixed, point-to-point communications network topology. For these installations, directional Yagi-type antennas with a narrow radiation pattern, and power gain to increase the effective radiated power of the transmitted signal, as well as to provide gain of the received signal, are highly desirable, particularly where the path loss between the router and the cellular service provider site may be high. This is a common situation with remote locations, and with the high levels of electrical interference commonly encountered within the substation environment, the need to provide the maximum possible received signal strength may become a consideration from a signal-to-interference plus noise ratio (SINR) standpoint. The mast-mounted Yagi antenna is initially bore-sighted to the cellular service provider's nearest cell site, and then aligned to obtain the maximum received signal indication. This process is quick, making the overall installation and set-up simple, and high levels of technical expertise are not required.

IEEE 1588v2 PRECISION TIMING PROTOCOL (PTP) SUPPORT

For modern substation SCADA applications, where precise timing synchronization between devices may be an important consideration, it is desirable for the cellular router to include IEEE 1588v2 PTP. Inclusion of this standard ensures millisecond accuracy for the sequence of critical event timing, and increases timing accuracy by utilizing state-of-the-art techniques to compensate for layer 2 switch/layer 3 router processing latency, and link propagation delays. It may also be used to eliminate the additional network cabling requirements associated with legacy systems employing IRIG-B, by using common Ethernet data cabling. IEEE 1588v2 PTP support also provides timing accuracy close to GPS, but without the requirements and complexity associated with ancillary GPS receivers and antennas.

REMOTE FIRMWARE AND SOFTWARE UPGRADES

Periodic or as-required firmware and software upgrades may be remotely and securely uploaded to the cellular router from any point within the user's network.

POWER OVER ETHERNET (PoE) CAPABILITY

For reasons related to reliability, the terminal equipment comprising the substation SCADA or distribution automation network is invariably not powered from PoE power sourcing equipment (PSE), but rather derives its operating power from either internal or dedicated external power supply units. For those utilities where the FERC-mandated requirements of NERC-CIP-014 for physical security of selected critical assets are required, PoE supplied from the router is highly desirable for providing operating power to Ethernet-compatible IP-video cameras for surveillance monitoring, access control equipment, and perimeter monitoring hardware. Substation-rated cellular routers including PoE capability are now available, and their use can significantly simplify the design of security networks required to achieve NERC-CIP-014 compliance.

Although beyond the scope of this paper, readers desiring additional information on NERC-CIP-014 are encouraged to read the author's white paper entitled, "Understanding NERC-CIP-014, and the Associated Communications Equipment Infrastructure for Electrical Substation Physical Security":

http://www.comnet.net/Collateral/nerc-cip-014/offline/download.pdf

LOW RECURRING & LIFE-CYCLE/OPERATING COSTS

Many different business-class cellular plans are offered by the popular service providers, such as Verizon, AT&T, and others. These plans can offer substantial cost discounts, depending upon the data usage and throughput requirements of the user. The subscriber typically pays only for the data time used, but the network and cellular connection are always on and available. Additionally, and unlike typical utility-owned 900 Mhz and microwave radio links, the cellular service provider maintains their communications infrastructure, instead of the user, reducing the life-cycle costs to the utility.

Although the recurring cost is largely a function of the cost associated with connecting to the utility's cellular provider, the user has the advantage of the communications reliability afforded by the cellular network, and the high degree of security this network and the cellular router provides. As the data usage and throughput for most substation SCADA and distribution automation applications are normally very low, there is a commensurate reduction in the subscription cost the cellular service provider charges, when compared to a conventional high-bandwidth/high data usage connection. The recurring cost is substantially less when compared to a T-1/DS-1 or E-1 wired telephony circuit, as provided by the utility's telephone service provider.

Distribution automation networks and renewable energy providers have used INMARSAT and VSAT satellite radio links for the connection between their remotely-located SCADA and other field equipment, and the central control and monitoring facility. The recurring costs of operating and maintaining such a communications circuit are significant, and many of these utilities are now replacing their satellite links with cellular radio routers, as an effective means of reducing their communications network expenses.

Return on investment (ROI) is quick, due to the low monthly cellular service provider subscription fee, and the first cost of the cellular router equipment is similar to other radio platforms, such as the 900 Mhz licensed and unlicensed equipment commonly utilized within the utility industry.

NERC-CIP-5 COMPLIANCE: SECURE CONNECTIVITY & NETWORK CYBER-SECURITY PROTECTION FOR SUBSTATION SCADA & DISTRIBUTION AUTOMATION NETWORKS

Nearly all system operators are concerned with the ever-increasing threat of a cyber-attack breaching and corrupting their network. FERC (Federal Energy Regulatory Commission) has mandated the implementation of NERC-CIP-5 as a guideline for hardening selected power generation and substation facilities against the possibility of such an attack, to minimize the obvious damage this could create to the reliable supply of electric power, as well as the potential economic and life safety consequences associated with the loss of power to their customer base. The level of firewall security in a cellular router can range from basic, to extremely robust, with best-of-breed devices providing Deep Packet Inspection (DPI), Authentication Proxy Access (APA), and event logging/Syslog for achieving NERC-CIP-5 compliance at a given site.

CYBER-SECURITY PROTECTION FOR DISTRIBUTION AUTOMATION SYSTEMS

For many distribution automation (DA) applications, the primary firewall resides at some location other than the pole or pad-mounted cellular router; the firewall is typically situated at the head-end of the network, where full control and monitoring of the system takes place. However, many utilities are concerned about the possibility of a security breach within their DA system, with the possible scenario of a cyber-attack, hacker, or unauthorized contract maintenance personnel accessing the network, and forcing a recloser or motor-operated switch to remain latched open; a voltage regulator to significantly increase or reduce line voltage; and other possible

highly undesirable conditions that could impact the reliability, performance, or stability of the system. It is also possible that a breach of the DA network could extend to other segments of the utility, including their enterprise and substation SCADA networks.

CYBER-SECURITY PROTECTION FOR SUBSTATION SCADA NETWORKS

The cyber-security requirements for substation SCADA networks can be quite different when compared to the typical distribution automation system, particularly in a transmission-class facility, where NERC-CIP-5 compliance may be a FERC-mandated requirement. For NERC-CIP-5 compliance, an extremely robust and effective firewall becomes a necessity, and the advantages of DPI, APA, and Syslog for event logging and recording, and the ability of the user to audit the network, become readily apparent.

Where network security is a significant concern for the system operator, a cellular router with a highly robust and effective firewall is a necessity.

If desired, a substation-rated cellular router with an effective firewall meeting these requirements may be obtained with the cellular radio deleted, so the device functions as a combination layer 2 managed switch as well as a layer 3 router, and with or without direct connection to the user's fiber optic network. This is desirable for those substation SCADA applications where the utility has existing fiber-optic or microwave radio networking infrastructure in place, and the need exists to harden their legacy substations or other facilities to comply with the requirements imposed by NERC-CIP-5.

The router should also offer remote management for, and access to, all unused physical Ethernet and serial data communications ports. Any unused port constitutes a potential and possibly unauthorized point of entry, and access to the network may only be permitted at a specific router and an associated port or ports. This can only be granted by the network administrator to accredited and trusted users. These may include contract maintenance and field engineering staff, as well the utility's own employees.

Remote access should extend to all end-point/edge-of-network devices, with extreme granularity for the allowed users, including the time interval during which a user is permitted access to the network, as well as all accessible physical Ethernet or serial data ports, TCP ports, and SCADA protocols. It should also provide PCAP (Packet Capture) for the entire allowed field maintenance or access session.

Dynamic routing and VPN (Virtual Private Network) capability should also be included within the firewall suite residing within the router.

ATTAINING NERC-CIP-5 COMPLIANCE: THE KEY COMPONENTS OF A HIGHLY EFFECTIVE CYBER-SECURITY FIREWALL

Identity Management and Authentication Proxy Access (APA)

NERC-CIP-5 defines the important criteria and salient requirements for network security protection of selected power generation, transmission, and distribution facilities. The capability for identifying the user, and creating specific network privileges for an identified and authenticated user prior to granting access to the network now becomes critical.

Authentication Proxy Access (APA) is a highly sophisticated security feature, which allows the network operator or administrator to manage the substation SCADA or distribution automation system maintenance process. This feature gives full control of the maintenance process to the operator, by granting the capability to create dynamic policies for specific tasks within an explicitly defined time window. Following this time window, the network administrator receives a full report of activities performed during the task. This audit trail comes in the form of an overview log, and a full packet capture of the session.

Before a user is allowed access to the network, he or she must first log in to an internal authentication process with their unique user name and password. Upon validation of the user's profile, specific access is granted only

to predefined routers, devices, and functions, and each operation is logged. Multi-factor authentication may be available when combined with a cyber-physical Integration feature.

Event Logging

The event logging feature allows the network administrator to receive events and logs from any number of remote devices. It supports multiple formats including Syslog, SNMP, & HTTP, and is also capable of polling event tables from any IP, access control, and serial data devices. The events are then received and sent outbound in Syslog format, with additional fields appended, completing a unified Event Log Aggregator (e.g., location, source sub-system, and severity). Following this aggregation, the event logger stores normalized events locally, and forwards the formatted events upstream to a central SIEM (Security Information and Event Management) tool, providing encrypted, reliable, and guaranteed logging in accordance with NERC-CIP-5 standards.

X.509 Certificate Exchange for VPN Connections

VPN tunnels for secure inter-site connectivity with IPsec VPN, GRE (Generic Routing Encapsulation) tunnels, and DMVPN (Dynamic Multipoint Virtual Private Network) technologies should be fully supported. In addition to IPsec (Internet Protocol Security) encryption, X.509 key management certificates should also be provided. This certificate support allows for a secure signed key exchange between a certificate authority, and two secure nodes. Having a third-party authority as a signing participant offers end-to-end security that may be managed and reissued from a trusted central source within the utility's network.

Cyber-Physical Integration

A physical identity server system allows the use of external authentication hardware, such as magnetic card readers, biometric identification sensors, facial recognition cameras, etc., to create a two-factor authentication process to the APA feature. This provides an additional level of validation of the user and his or her credentials, prior to granting the user access to the network. Once the authentication is validated and approved, a set of defined policies allow the authenticated maintenance or service technician to perform their task.

Cyber-physical integration also allows the event logger feature to poll and deliver events from physical access control devices utilized as a key component to the utility's physical security and surveillance system, as it relates to NERC-CIP-014. These assets include but are not limited to access control panels, and controlled access head-end systems and databases.

An Enhanced SCADA-Aware Firewall

A whitelist-based firewall should be provided for every Ethernet and serial data port, so full firewall protection is available at all remote sites within the network. Every SCADA protocol packet (IEC 61850, DNP3 RTU/TCP, ModBus RTU/TCP, and IEC 101/104) is then scanned and validated by the firewall engine for its source and destination, as well as its protocol and packet content.

The structure of the distributed firewall should allow for the creation of a unique firewall at each access point to the network. This is critical for securing against insider cyber-attacks, compromised field devices, man-in-the-middle attacks, and a myriad of alternate attack vectors, by providing a secure baseline.

Two firewall states should be included within the firewall suite: Monitoring, and enforcing. The monitoring state provides an alarm at the utility's control center for any network violation, without blocking the network traffic. The enforcing state is extremely effective for blocking suspicious traffic, while also triggering a violation alarm at the control center.

DPI (Deep Packet Inspection) SCADA Protocols Firewall

A distributed DPI firewall ensures that the operator will have full control over the network, even when faced with a sophisticated attack attempt. While monitoring SCADA commands, this highly robust whitelist-based firewall analyses SCADA network traffic at every Ethernet and serial data port, so full firewall protection is available at all remote sites within the network, as well as at all IEDs, RTUs, or any other terminal device connected to the network. Every SCADA protocol packet (IEC 61850, DNP3 RTU/TCP, ModBus RTU/TCP, and IEC 101/104) is then scanned and validated by the firewall engine for its source and destination, as well as its protocol and its specific packet.

Any detected abnormal traffic behavioral patterns are blocked, any affected subnets are isolated, and alerts to the network administrator are automatically generated.

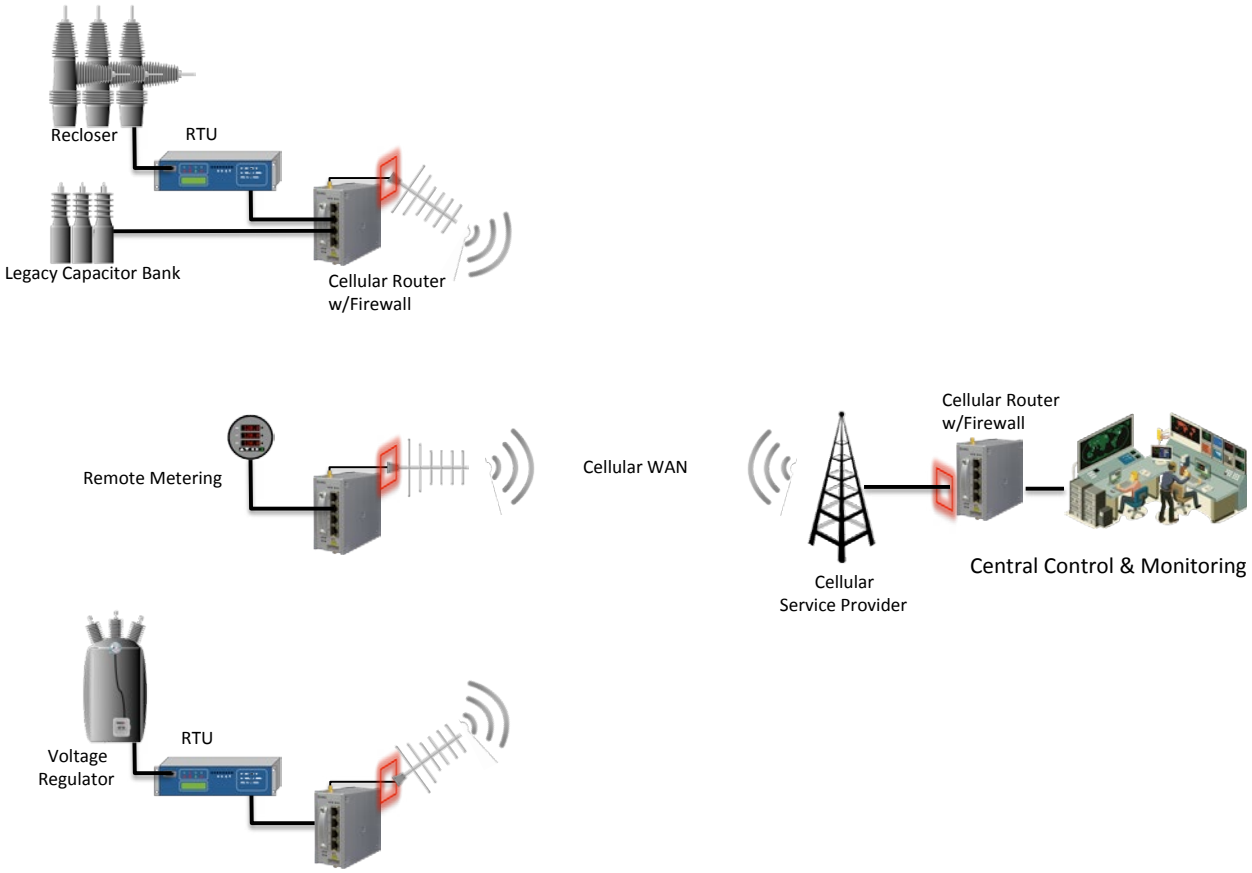
TYPICAL APPLICATIONS

Distribution Automation & Remote Metering

Distribution automation systems require the monitoring and control of remotely-located pole-mounted, pad-mounted ground-level, or underground electrical equipment, such as reclosers, motor-operated switches, capacitor banks, and voltage regulators. Some of the major benefits realized from distribution automation include a decrease in outage time due to system faults, and a resulting increase in customer satisfaction levels. Remote monitoring and control enables the utility to perform diagnostics for rapid detection and isolation of system faults, providing enhanced DA system performance and reliability.

Distribution Automation

Secure Cellular Connection of Pole-Mounted Electrical Equipment



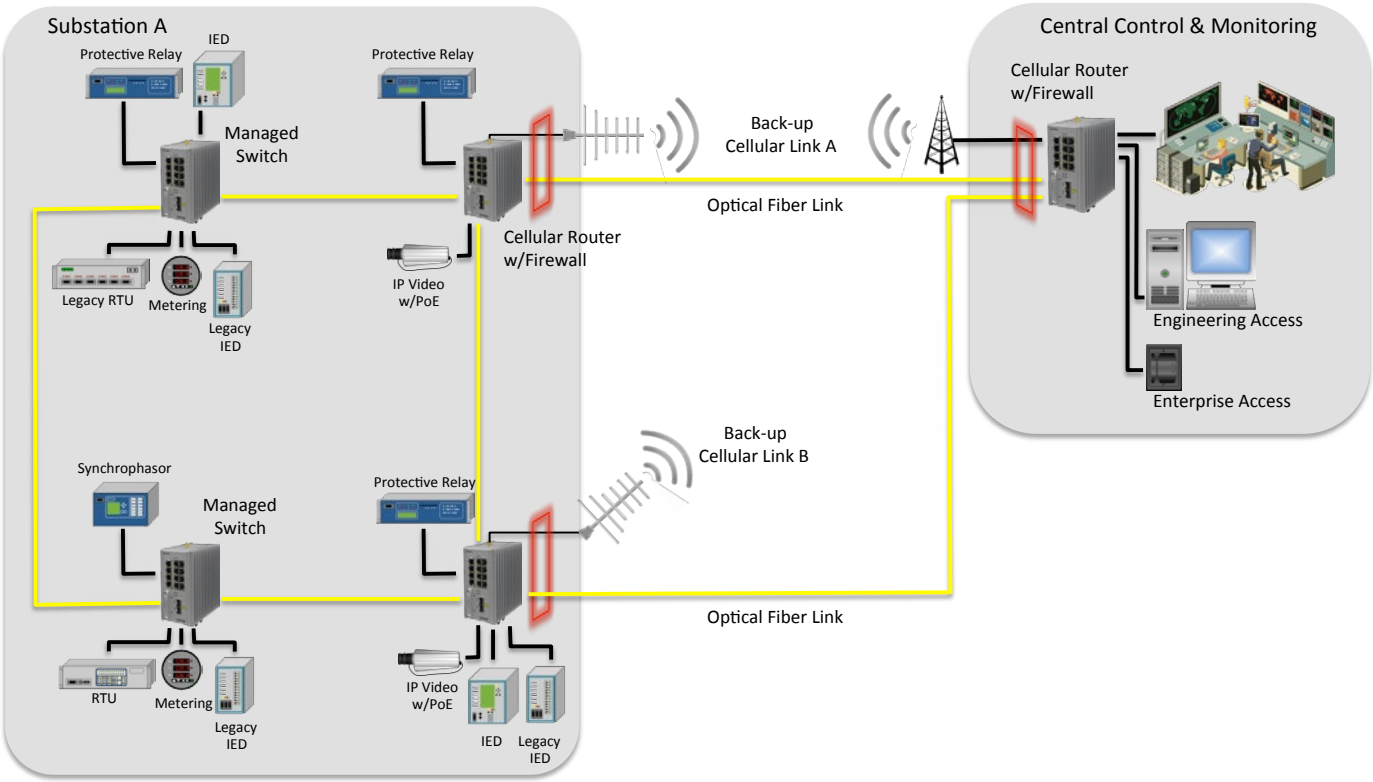
This diagram describes a typical DA system employing Ethernet-compatible and legacy serial data reclosers, capacitor banks, and voltage regulators at multiple sites, all connected via secure cellular routers to the utility central control and monitoring facility. Remote metering is also included. The serial data-compatible equipment is connected directly to the router, eliminating the need for an outboard terminal server. Note that the number of remotely-located sites in this application is virtually unlimited, allowing the creation of a cellular WAN to include all of the DA equipment utilized by the utility.

Substation SCADA Networks

Modern SCADA networks entail the connection of multiple devices such as RTUs, protective relaying equipment, IEDs, metering, synchrophasors, data loggers, and other substation-specific equipment onto a common network. This platform is typically built around a network of substation-rated layer 2 managed Ethernet switches, and a layer 3 router running a secure firewall for cyber-security protection at the site. The router also provides the connection to the utility's WAN.

Substation SCADA System with Optical Fiber Primary Links & Back-up Cellular Links

(NERC-CIP-05 & NERC-CIP-014 Compliant)



This diagram illustrates a substation where layer 2 managed switches are utilized for connecting the RTUs, protective relays, IEDs, synchrophasors, and metering equipment to a fiber-optic and cellular WAN employing cellular routers. PoE-powered IP-video cameras for substation surveillance and monitoring (for NERC-CIP-014 compliance) derive their operating power directly from the router.

A highly secure cellular radio connection is provided by the router via the encrypted WAN to the utility's central control and monitoring facility. A router with a highly effective and robust firewall, and with an internal cellular radio has been added for connection to the existing fiber-optic network, as this legacy substation SCADA system and network must now comply with the requirements of NERC-CIP-5.

Legacy serial data RTUs and IED's are connected directly to the router, and no outboard terminal server is required.

Network fail-over protection is included via the cellular routers. The fiber-optic network is utilized as the primary communications path from the substation to the central control and monitoring location. In the event of a fault within this optical network, the system will automatically switch over to the cellular radio communications circuit, providing uninterrupted service. Two SIM cards installed within the router allow for connection to two separate cellular service providers, further enhancing the availability of the network in the event of a loss of connection to one of the two providers.

SUMMARY

Cellular routers are highly effective for the implementation of reliable and extremely secure Ethernet communications networks for most remote substation SCADA, distribution automation, and metering applications. Legacy serial data terminal equipment may be seamlessly integrated onto the user's network as well, without the need for an outboard terminal server. These routers are also useful for connecting remotely-located renewable power generation facilities to the utility's network.

In many locations, the cellular communications infrastructure is already present, with essentially instant access to a worldwide network. A highly reliable, secure, and continuously available connection is thereby provided, at low recurring operating cost, and with minimal maintenance expense.

Fail-over capability provides fault-tolerant, uninterrupted cellular communications in the event that one of two separate cellular service providers should experience a failure at the cellular radio site providing connectivity to the router, as well as those installations where a fiber-optic network is the primary communication circuit. A fault within the fiber-optic network will automatically fail-over to the cellular radio link.

Substation-rated cellular routers complying with the requirements of IEC 61850-3 and IEEE 1613, class 2 are now available, and provide very high levels of long-term reliability when installed within the demanding operating environment imposed by the typical substation. The standard operating voltages found within the substation plant, or for pole or pad-mounted distribution automation equipment, may be used to provide operating power to the router, without the need for any separate or outboard power supply units, thereby reducing the overall cost and complexity of the system.

Highly effective and extremely robust security firewalls are also available within these devices, for achieving NERC-CIP-5 compliance at existing legacy facilities, or for new substations and distribution automation networks currently in the system design and engineering phase.

PoE is available from these devices, for providing operating power to the physical security and surveillance equipment associated with NERC-CIP-014 compliance at a given facility.

ComNet offers an extensive line of environmentally hardened fiber optic, copper-based, and wireless transmission and networking equipment that is designed to meet the unique requirements of the industrial security, intelligent transportation, industrial control, and the electric power, transmission, and distribution markets.

Bruce Berman is responsible for directing and promoting the application of ComNet products to markets that can benefit from their use. In many cases he educates System Designers and customers on all levels about the benefits that ComNet products and technology bring to their projects.

comnet Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA | WWW.COMNET.NET
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET