comnet
Communication Networks

WHITE PAPER:

Understanding NERC-CIP-014, and the Associated Communications Equipment Infrastructure for Electrical Substation Physical Security

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

For most of the history of the electric power transmission and distribution industry, electrical substations were thought of as assets with relatively minimal physical security concerns. The chain-link fences surrounding them, and the well-known and ominous sounding "Danger-High Voltage, Keep Away" signs were usually sufficient to prevent unauthorized entry to or vandalism of these facilities, and more recently, the prevention of theft of valuable copper and other costly materiel.

Largely unreported within the media, the Pacific Gas & Electric (PG & E) Metcalf substation in San Jose, California, supplying power to the Silicon Valley area was vandalized in April, 2013, with a sniper damaging insulator bushings on 17 power transformers, resulting in $17 million in damage. The incident, which happened shortly after midnight, began when fiber-optic communication lines were severed in two underground vaults near the substation. The probable objective of the vandal was to create a widespread power outage, but fortunately the utility was able to reroute power at the facility, and the public experienced no outages. Another incident occurred in August of 2014; materials were stolen from a construction trailer located at the Metcalf site. Both incidents dramatically underscored the issue surrounding physical security as it relates to the national electric power supply grid.

In the world we now live in, substation security and surveillance have become major concerns on a global scale for electric power utilities and providers. The economic and life safety consequences of deliberate and maliciously incurred power outages are obvious. The threat potential for these unattended and frequently remotely located and easily targeted facilities (which also includes remotely located wind farm and photovoltaic array/solar power generation sites) is considered to be high, and of critical national importance. Physical security protection of this enormous critical asset is clearly required, in terms of CCTV video surveillance, event recording, perimeter detection and monitoring, and controlled access to the site for maintenance and other authorized personnel, particularly at the points of power generation and at electrical transmission and distribution substations.

As the threat potential to the national power supply grid is considered to be so significant, to ensure the maintenance of physical security at electrical substations, in March of 2014, the Federal Energy Regulatory Commission (FERC) mandated the North American Energy Reliability Corporation (NERC) to create a series of Critical Infrastructure Standards (CIP) that would define "physical security risks and vulnerabilities related to the reliable operation" of the bulk power supply system. NERC is a not-for-profit regulatory authority whose mission is to ensure the reliability of the electrical power system in North America, and it is subject to oversight by the FERC and governmental authorities in the U.S. and Canada. NERC's jurisdiction includes owners, operators, and users of the bulk power system which serves more than 334 million people.

FERC had approved the NERCs critical infrastructure protection standard for physical security protection on November 20th, 2014; this standard is defined as NERC-CIP-014. With the advent of NERC-CIP-014, electrical utilities and bulk power providers have entered into an era that was basically unthinkable prior to the events at the PG & E Metcalf substation.

NERC-CIP-014 requires that all power utilities in the U.S. and Canada comply with the security requirements defined by NERC by a given deadline, or they will be liable for sizeable fines. As such, the power utilities in these countries are under intense pressure to meet the difficult security regulations imposed by NERC-CIP-014.

UNDERSTANDING NERC-CIP-014

NERC-CIP-014 is intended as a model, or best practices blueprint for the guidance of not only bulk electric power providers/utilities, but also for physical security professionals to provide the most effective protection of vital outdoor-located electrical transmission and distribution assets. NERC-CIP-014 was largely created as a guideline for the protection of North American electric power substations from physical attack.

NERC-CIP-14 describes a "systems approach" for providing physical security protection of mission-critical substation facilities and other key assets within a utility, and six specific actions have been identified by NERC:

-Deter **-Detect** **-Delay**

-Assess **-Communicate** **-Respond**

NERC also recommends a "defense in depth" concept to "prevent the advance of an attacker". This concept entails the creation of several zones of protection over a wide area, so that the utility may respond to an event over a wider time interval, instead of utilizing a "single, strong defensive line". These zones or layers of protection would typically initiate with the fencing surrounding the substation or other mission-critical facility, as well as controlled access points for authorized personnel, and ultimately terminate at some very critical location, such as the shelter containing the control and metering equipment at the substation.

As part of the NERC-CIP-014 implementation process, each utility must identify their most mission-critical facilities; these are facilities defined as installations that in the event they were damaged or taken off-line, would "result in widespread instability, uncontrolled separation or cascading within an interconnection". As a means of preventing such an event, the utility must "develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery" of these critical assets.

To demonstrate compliance, a utility is required to perform a complete security audit and review, so as to identify any potential threats to the substations and other assets they have determined to be mission critical, confirm the risk assessment with an independent third party, and finally implement the physical security protection necessary to maintain protection of those assets. The utility is then required to submit to another independent third party analysis, to review and evaluate their intended means of providing compliance against the identified threats. These requirements are time-phased, allowing the utility the opportunity to install and integrate the required physical security detection and protection hardware within their facilities.

As the threat potential by terrorist activity to disrupt the delivery of electric power will most likely remain for the foreseeable future, other issues such the theft of valuable equipment assets and vandalism are perhaps more well-known, and must also be considered from a security standpoint. With the price of copper at record levels, and as the use of copper is so prevalent within electrical substations, it has become a very attractive target for theft, often with lethal consequences for the thieves. Maintenance personnel have been injured, and in some cases killed when servicing facilities where electrical components where removed by theft, thereby compromising the safety of the installation when the theft was not detected previously by the utility.

The mitigation approaches and processes that may be employed for NERC-CIP-014 compliance are beyond the scope of this paper, much of which utilizes proven and well-known hardware and mitigation techniques widely available within the industrial security marketplace.

NERC-CIP-5

NERC has also released another highly important security standard; NERC-CIP-5. Although NERC-CIP-014 is largely concerned with the threat of physical security attacks compromising the integrity of the national power supply grid, NERC-CIP-5 addresses the equally serious threat of cyber-security attacks to the entire North American electrical power supply infrastructure.

COMMUNICATIONS EQUIPMENT FOR SUBSTATION PHYSICAL SECURITY & SCADA NETWORK APPLICATIONS

The communication networks within the typical substation can be broken down into two key groups; the SCADA (Supervisory Control and Data Acquisition) subsystem, utilized for interconnecting all of the substation IEDs (Intelligent Electrical Devices) and RTUs (Remote Terminal Units), such as metering, control, and protective relaying equipment onto a common communications network; and the physical security subsystem, consisting of CCTV video for surveillance, perimeter detection and monitoring, and access control, for supporting the security requirements at the site.

Substations are unique in that the environment where the electronic equipment is installed is extremely harsh, with severe voltage transients from circuit breakers and other switchgear, and high levels of EMI (electromagnetic interference) emanating from large power transformers and other high-voltage equipment. As the communications equipment for the SCADA and security sub-systems is usually located in an unconditioned shelter, or outdoors within weatherproof enclosures, it is exposed to a very wide range of operating temperature and humidity with condensation conditions. In this severe environment, ruggedized fiber optic transmission equipment is widely used, largely due to its inherent immunity to intense levels of electrical interference.

Substation-rated managed layer 2 Ethernet switches and layer 3 routers with SCADA firewalls employing integral cellular radio modems have been recently introduced for providing highly secure and reliable communications circuits internal and external to the substation. These devices are particularly useful where the cost of installing a dedicated fiber optic network may be prohibitive, or where right-of-way issues may exist.

License-free industrial-grade/out-of-plant-rated 5 Ghz wireless radio equipment is also widely deployed within substations, primarily for hauling IP video from the camera to the network backbone. These radios are ideal for this application, as they are simple to install, and do not require the costly installation of a dedicated fiber optic cable (and the attendant media converters) to provide this link.

Although copper media-based CAT-5E/UTP and coaxial cable Ethernet extenders are available and widely used for many physical security related applications, they are not usually employed for substation security systems, due to their relative lack of EMI rejection in these electrically noisy environments, as well as their susceptibility to ground loops due to potential voltage difference issues.

SUBSTATION-RATED COMMUNICATIONS EQUIPMENT: THE IEC 61850-3 STANDARD

To maintain high levels of reliability, the communications equipment within the substation must be capable of surviving long-term in this kind of adverse operating environment, and with no degradation to performance or reliability. Two key and universally employed industry standards define the environmental requirements for all communications equipment fielded within an electrical substation: IEC 61850-3 for Ethernet-compatible communications equipment, and IEEE 1613 for legacy non-Ethernet equipment. Equipment meeting these requirements is referred to as being substation-rated.

Recognizing the growing demand for fiber optic transmission equipment capable of meeting these requirements, ComNet recently introduced their Reliance product line of substation-rated managed Ethernet layer 2 switches, layer 3 routers, media converters, and fiber optic serial data modems. These IEC 61850-3 and IEEE 1613 tested and certified products are widely used for substation SCADA networks, and for optically isolating electrically-delicate CCTV video cameras and other equipment related to the physical security protection subsystem from the harmful effects of EMI and high-voltage transients present within the substation. Managed layer 2 Ethernet switches are used for creating VLANs within the SCADA network, the security and surveillance subsystem, and any other communications requirements, such as VOIP telephony, etc. Layer 3 routers are employed for supporting the SCADA security firewalls required for NERC-CIP-5 compliance against cyber-security attacks, and for interconnecting numerous substations and other utility facilities via a high-speed, wide-area optical backbone.

Unlike nearly all traditional industrial security applications, the operating power within the substation is of poor quality, with substantial electrical noise and voltage transients, and it is usually not the commonly available 120/240 VAC, but rather -48 VDC, or high-voltage AC/DC at 88-300 VDC or 85-264 VAC. The 88 to 300 VDC power is derived from large storage battery banks that provide back-up operating power for all of the SCADA system control, metering, and protection equipment within the substation in the event of a localized power outage. ComNet Reliance-series equipment is designed to operate over any of these input power ranges.

Specialized substation-rated/IEC 61850-3 compliant thermal imaging IP CCTV cameras are now available not only for video surveillance and perimeter detection and monitoring purposes, but for remotely monitoring the operating temperature (and possible over-temperature/electrical overload condition) of large pad-mounted power transformers within the facility. Cameras for this application are typically integrated to the substation SCADA network.

With the advent of modern IP video cameras and Ethernet-based access control equipment, it now becomes practical to easily integrate the physical security subsystem to the existing substation Ethernet SCADA network, with all of the equipment sharing a common, open standards-based Ethernet communications platform.

IEC 61850-3 COMPLIANCE FOR PHYSICAL SECURITY SUBSYSTEM COMMUNICATIONS EQUIPMENT: YES OR NO?

Any communications equipment utilized as part of the Ethernet-based substation SCADA system is invariably required to provide IEC 61850-3 compliance, due to the mission criticality of this application. As such, equipment located "within the fence" is usually specified by the utility to this standard. Equipment compliant with IEC 61850-3 is electrically, mechanically, and thermally very robust, and is designed to provide extremely high levels of reliability within the difficult substation environment. However, this comes at a cost; substation-rated communications equipment is available from a relatively limited number of suppliers, and the cost of the equipment is significantly higher when compared to non-substation rated industrial-grade hardware.

But will the fiber optic or wireless microwave radio communications equipment supporting the physical security subsystem benefit from IEC 61850-3 compliance? This is really a judgement call; many utilities and physical security system design engineers and systems integrators associated with the implementation of NERC-CIP-014 are of the opinion that it will not. Although the reliability enhancement derived from IEC 61850-3 compliant hardware can only serve to increase the reliability of the overall network, on a cost-benefit basis it may not be considered worth the additional cost of the equipment. Standard industrial-grade communications equipment rated for deployment in unconditioned out-of-plant environments, and with an operating temperature range of -40 to +75 degrees C, is generally considered as being sufficient for the physical security communications infrastructure within the typical substation.

It is important to note that IEC 61850-3/substation-rated Ethernet communications equipment may be seamlessly electrically and optically integrated with non-substation rated Ethernet communications equipment. As the SCADA network within the substation is almost always interconnected to a remotely located control and monitoring facility, the subsystem supporting the physical security requirements at the substation generally shares and makes effective use of the SCADA network platform.

CASE STUDY: A TYPICAL SUBSTATION PHYSICAL SECURITY COMMUNICATIONS EQUIPMENT SUBSYSTEM

A major utility in the southeastern part of the U.S. is in the process of implementing a series of standardized physical security monitoring and detection subsystems for NERC-CIP-014 compliance at numerous substations within their wide-area transmission and distribution system. Several of these substations support a transmission voltage of 345 KV.

The basic criteria and salient requirements for the physical security subsystem were as follows:

- Seamless integration of the physical security subsystem with the existing/legacy Ethernet-based substation SCADA network/platform
- Utilize newly installed IP video thermal imaging and conventional IP CCTV cameras
- Utilize legacy high-resolution analog CCTV cameras with a separate serial data pan-tilt-zoom control channel
- Install an IP-based access control system for the admittance of authorized maintenance staff to the site
- Provide IP-based electronic surveillance and detection around the entire substation facility perimeter
- Utilize fiber optic transmission equipment wherever possible for the physical security subsystem, to eliminate the possibility of electrical interference/EMI and ground loops due to radiated and conducted emissions emanating from high-voltage power transformers, circuit breakers, switchgear, and other high-tension equipment within the substation
- Employ license-free 5 Ghz microwave radio links for those CCTV IP video camera links where the cost or difficulty of installing new fiber optic cable may be prohibitive.
- Create separate VLANs for the CCTV video, the access control system, and the perimeter surveillance equipment, and any other equipment that is ancillary to the substation SCADA network
- Provide an NVR (Network Video Recorder) for storing/archiving the video from the facility

The Ethernet-based SCADA network system at many of these substations employ a combination of legacy 10/100 and 100/1000 Mbps substation-rated/IEC 61850-3 compliant managed layer 2 switches. Many of these switches provide a copper-only interface for the Ethernet data, with only the uplink ports supporting a fiber optic interface with fixed single-mode optics. Several of the newer-generation switches within some of the sites provide a combination of both copper and optical interfaces for the Ethernet data, with the optical ports SFP-based (Small Form Factor Pluggable), for greater flexibility in terms of user-selection of optical fiber compatibility, and optical transmission distance/path loss.

The thermal imaging and conventional IP video cameras are PoE powered, and derive their +48 VDC operating power from industrial-grade (not substation-rated) shelf-mounted media converters. For those managed switches where an optical Ethernet interface is not available, the outputs of multi-channel media converters are connected directly to the copper ports of these switches. These media converters are co-located with the switches utilized for the SCADA network within the equipment shelter of the substation, and are rack-mounted for optimum use of the available 19-inch equipment rack real estate. The multi-channel media converters provide maximum channel count and density within each rack-mounted card-cage chassis.

Where the managed switches provide an optical Ethernet interface, the media converters located at the field-end or edge of the network are optically connected directly to the Ethernet optical input ports of the switch, eliminating the need for media converters at the switch-end of the link, thereby simplifying the design and enhancing the overall reliability of the system.

The legacy analog CCTV cameras utilize industrial-grade/out-of-plant-rated video encoder units. These shelf-mount encoders are located at the camera-end of each of these links, and convert the baseband video analog output of the camera and the pan-tilt-zoom RS-232 serial control data to an Ethernet data stream utilizing high-quality H.264/MPEG-4 video compression. The frame refresh rate is user-selectable, and may be remotely scaled at any rate from 1 FPS (Frames Per Second), to full-motion 30 FPS. The Ethernet output of the encoder is connected to a shelf-mount industrial-grade media converter, and the media converter at the other end of the link is connected to a copper port on one of the SCADA system managed switches. The video encoder and mating media converter are installed within a small unconditioned weatherproof NEMA enclosure. Software decoding is utilized for remote viewing of the video at the monitoring location of the network, thereby eliminating the need (and related cost) for hardware video decoders.

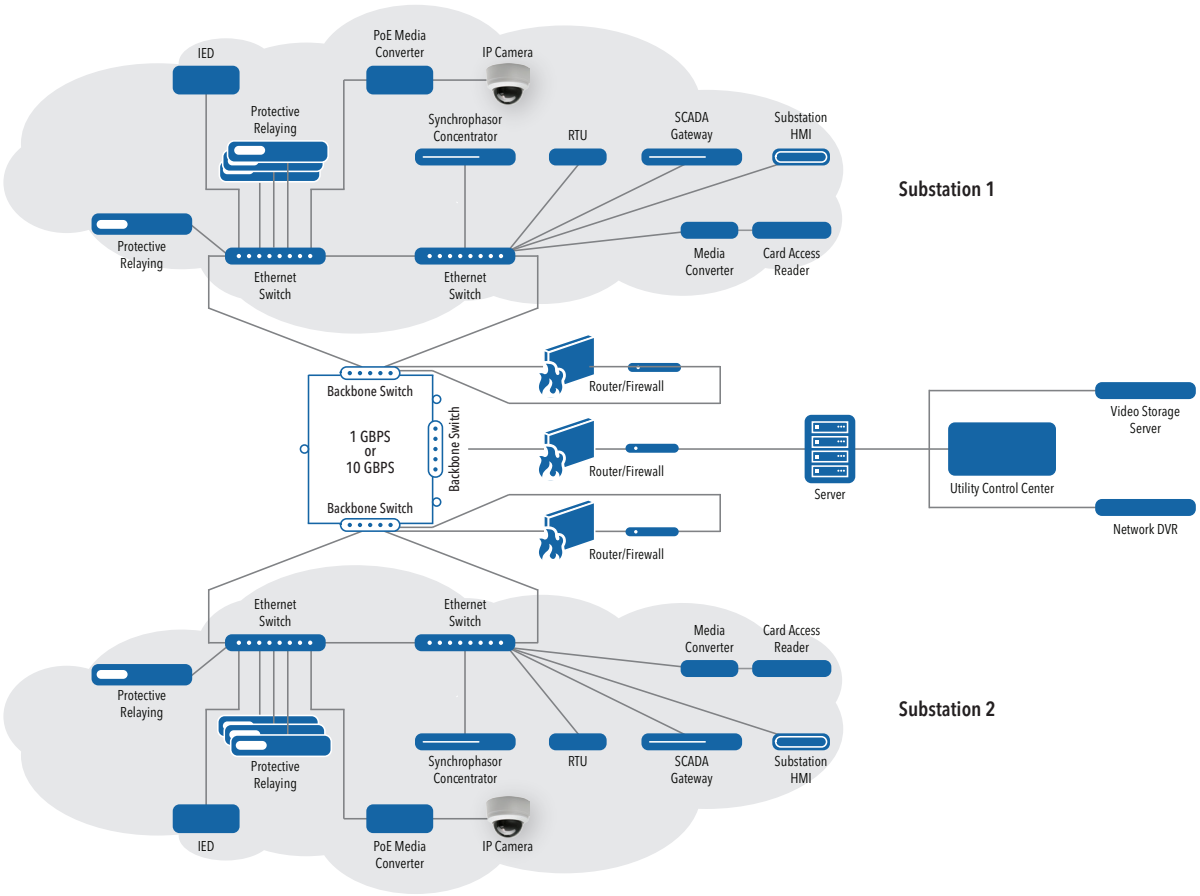
For those newly installed IP video CCTV cameras where it was not considered practical to run new fiber optic cable to these camera locations, industrial-grade/out-of-plant-rated license-free 5 Ghz microwave radio links were installed in a point-to-point architecture for hauling the video from the camera to the substation equipment shelter. These radio links provide the +48 VDC PoE operating power to each camera unit, and the IP video received by the radio at the shelter-located end of the link is also fed into a copper Ethernet port of a substation SCADA system managed switch.

The access control, and perimeter detection and surveillance systems also provide an Ethernet interface, and this equipment is optically connected to the substation SCADA network using the same approach as the CCTV IP video system described above.

The final result was a highly reliable, easy to install and commission, and cost-effective physical security communications subsystem that made use of both legacy and newly installed equipment. The use of industrial-grade (not the more costly substation-rated/IEC 61850-3 compliant) fiber optic and license-free microwave radio links provided complete immunity from any radiated or conducted EMI, and eliminated the possibility of any troublesome ground loops, even when the equipment was installed within the near-field of 345 KV high-voltage equipment.

TYPICAL SYSTEM ARCHITECTURE

Two Electrical Substations with Integrated SCADA Network & Physical Security Subsystem Including IP Video CCTV Surveillance & Controlled Access Card Readers



SUMMARY

The use of substation-rated fiber optic Ethernet transmission equipment, such as media converters, managed Ethernet layer 2 switches for interconnecting the various SCADA system elements within the substation; and 1 gigabit or 10 gigabit layer 2 switches and layer 3 routers with a SCADA firewall for use as a high-speed optical backbone for connecting multiple substations to a common network, provides the user with the potential for significant scalability for their substation SCADA system for future expansion, and a reliable, secure network terminating at the utility's control and monitoring center. Managed layer 2 switches, and layer 3 routers with a SCADA firewall and integral cellular radio modem, can provide a highly cost-effective solution at the edge of the network, where the cost of installing fiber optic communications circuits may be difficult or cost-prohibitive, or where right-of-way issues may exist. All of this equipment will be found to be of considerable value when designing a substation SCADA system for NERC-CIP-5 compliance, or a physical security subsystem for NERC-CIP-014 compliance.

Standard industrial-grade versions of this transmission equipment can provide a highly cost-effective solution with all of the benefits described above for the substation physical security subsystem for NERC-CIP-014 compliance, where the user is of the opinion that they may not require the technical benefits or wish to incur the cost penalties associated with IEC 61850-3 substation-rated hardware.

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