Manage Utility IEDs Remotely while Complying with NERC CIP

SUBNET™ SOLUTIONS INC.

Disclaimer and Copyright

The information regarding the products and solutions in this document are subject to change without notice. All statements, information, and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products or solutions.

The software license and limited warranty for SUBNET Solutions Inc. products are set forth in the information packet that ships with SUBNET products and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your SUBNET Solutions Inc. representative for a copy.

In no event shall SUBNET Solutions Inc. or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss of damage to data arising out of the use or inability to use this document, even if SUBNET Solutions Inc. or its suppliers have been advised of the possibility of such damages.

The following are either trademarks or registered trademarks of their respective organizations: SUBNET, SUBNET Solutions Inc., PowerSYSTEM Center, My Passwords and My IEDS are trademarks or registered trademarks of SUBNET Solutions Inc.

Table of Contents

Executive Summary

The abundance of proprietary and vendor-specific protocols and data formats requiring use of vendor-specific integration solutions has resulted in a lack of interoperability in utility business systems and processes. Beyond these traditional issues, other vendor-specific technologies are creating similar barriers to interoperability. For example, vendor-specific password, security, faceplate, and output display capabilities of Intelligent Electronic Devices (IEDs) makes it difficult for utilities to easily manage the access to, and passwords of, all their different IEDs. This limitation also complicates compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards during this process. This, in turn, impairs utilities' ability to efficiently operate, maintain, and manage assets; maintain high reliability of power systems; and efficiently comply with regulatory standards. This paper describes a solution from SUBNET Solutions Inc., called the SUBNET IED Management Solution – PowerSYSTEM Center, which addresses these challenges by providing an integrated system of IED access management and password management.

The Interoperability Challenge

While electric utility systems and processes have consistently provided some of the highest levels of reliability and security in the world, their evolution over time limits the interoperability of solutions. This complicates utilities' ability to conduct increasingly important functions, such as remote access and management of substation information, and compliance with NERC CIP standards.

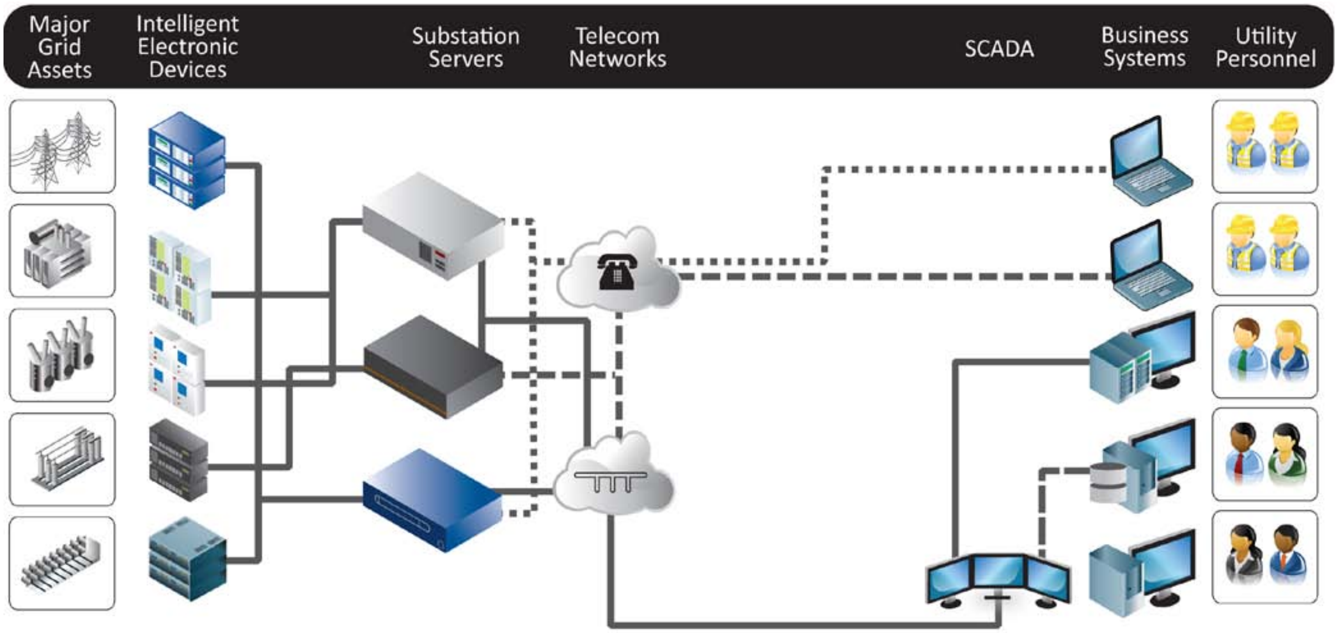

Figure 1: Integration efforts typically involve a combination of different legacy devices from a variety of vendors.

To illustrate this, Figure 1 shows the classes of elements that encompass the key business features of an electric utility:

- "**Major grid assets**" in the diagram include transmission and distribution assets (power lines, breakers, transformers, circuit switchers, capacitor banks, and other equipment investments).
- "**Intelligent Electronic Devices**" (IEDs) include devices and systems in which utilities have invested billions of dollars over the past several decades to more efficiently and reliably operate and maintain the power grid. They provide real-time measurement, monitoring, control, and protection of the high voltage power grid assets. These include meters, relays, Remote Terminal Units (RTUs), Digital Fault Recorders (DFRs), breakers, and transformer monitors from many different vendors.
- "**Substation servers**" include computer servers in the substation that gather and store data from the IEDs.
- "**Telecommunication networks**" allow for voice communications between utility personnel, as well as data communications between intelligent systems at key points throughout the utility's service territory. Utilities deploy various communication technologies, including frame relay, Synchronous Optical Networking (SONET),

wireless, fiber, satellite and Worldwide Interoperability for Microwave Access (WiMAX).

- The "**SCADA**" system acquires and controls the power system from an energy control center.
- "**Business systems**" include a wide variety of utility business computer-based management systems installed in the corporate enterprise. These include energy and asset management systems, outage management systems, data historians, and other analytical tools from many different vendors.
- "**Utility personnel**" include human resources who are responsible for designing, constructing, operating, and maintaining the safe and reliable power grid.

The point of investing in all of these technologies is to create a more intelligent power grid, and individually, each technology performs its primary function very well. The major challenge utilities encounter with these systems is the difficulty of implementing solutions that allow interoperability. The typical result of a utility's integration efforts is a combination of many different legacy integration devices from a variety of vendors, each performing a single, specific integration function, such as the following:

- SCADA vendor specific Remote Terminal Units (RTUs)
- Relay vendor specific communication processors
- Telecom equipment vendor specific dial-up security devices
- Industrial human-machine interface (HMI) vendor products with 3rd-party OPC servers
- Digital Fault Recorders (DFRs) vendor gateway solutions
- Business system specific data-collection drivers or interfaces

A key reason for this lack of interoperability is the abundance of proprietary and supplier-specific protocols and data formats requiring use of vendor-specific integration solutions. Another reason is that utilities' traditional departmentalized approach tends to promote these vendor-specific integration solutions, rather than a more holistic smart grid integration approach. Clearly, a multi-vendor, multi-function approach to interoperability is needed.

The IED Access and Management Challenge

In an important part of the process described above, utility personnel that access data from utility assets face two primary challenges. First, they need to remotely access and manage data from IEDs to optimize operation, maintenance, and asset management, as well as to meet other corporate goals. Their second challenge is to achieve this while enhancing security and fully complying with NERC CIP standards. This section describes each of these two challenges in more detail.

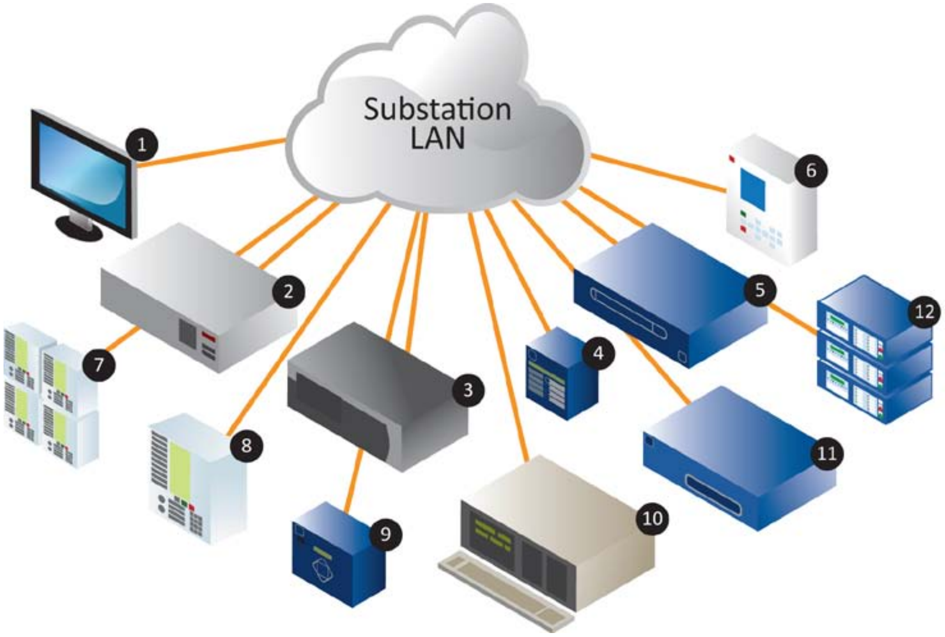

Figure 2: Technological advances enable utilities to remotely interface with and access data from a variety of substation devices. 1. HMI 2. Programmable Logic Controller (PLC) 3. Substation Server 4. Sequence of Events (SOE) Recorder 5. Transformer Monitor 6. Digital Fault Recorder (DFR) 7. Intelligent Electronic Device (IED) 8. Remote Terminal Unit (RTU) 9. Breaker Monitor 10. Differntial Relay 11. Recloser 12. Meters

Remote Access to Utility's IEDs

Technological advances enable utilities to remotely interface with and access data from a variety of utility's devices (see Figure 2). They may do this to confirm or modify device settings or to collect specific information that is not currently collected from the devices. Organizations can use this data for a variety of important applications, including the following:

- Adapt IED settings as needed
- Help analyze and correct line faults and otherwise resolve disturbances

- Identify optimal timing to repair/replace equipment and systems
- Make best use of assets by safely operating closer to tolerances
- Better forecast load to reduce need for spare equipment capacity
- Streamline operations

These functions have very large impacts on reliable power system operation, control of maintenance costs, and optimal use of expensive, aging power delivery assets. To perform these functions, utilities need to manage access to all IEDs, automatically connect to the devices, and centrally manage this access. However, this access is further complicated by the introduction of NERC CIP standards (described below). In order to comply with NERC CIP, some utilities have severely limited, or even eliminated, remote access to substation data. This approach poses several disadvantages, including the following:

- Reduced productivity: IED monitoring and maintenance becomes time-consuming and more costly (e.g., travel time from service centers to substations).
- Reduced value added by personnel: Inefficient processes force personnel to focus on obtaining access, rather than on making use of the information obtained.
- Lack of centralization: Staffing shortages and aging workforces are further strained.
- Increased risks: On-site (at substation) monitoring and maintenance increases risks of errors, outages, and failures; and may compromise worker safety.
- Reduced employee satisfaction: Inefficient processes are frustrating for employees.

Hence, utilities need a way to ensure unfettered remote access to substation data.

NERC CIP Compliance

Potentially limiting or eliminating this remote data access are NERC CIP standards, which were introduced in 2007 and went into effect in June 2009. The standards mandate, among other provisions, that utilities institute authorization and authentication methods for access to information at remote IEDs. This includes the need for password management for IEDs, auditable records of access and password changes, and various reporting requirements. For example, CIP-007.4R5 states:

> *"Account Management – The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access."*

In another example, CIP-007 R5.1.1-4 state that "Each password shall be a minimum of six characters; each password shall consist of a combination of alpha, numeric, and "special" characters; and each password shall be changed at least annually, or more frequently based on risk."

NERC CIP effectively requires utilities to maintain adequate equipment and system password complexity, address password frequency of change, and change default/factory passwords prior to placing equipment in service. The requirements also affect shared account access, user account access privileges review, and securing accounts after personnel changes. In total, utilities must effectively manage access to protected critical cyber asset information. NERC monitors compliance via periodic compliance audits, and failure to meet the standards can result in fines of up to U.S. $1 million per day.

With regard to password management, for example, consider that at one typical substation, each of approximately 30 different devices requires four levels of passwords. This means that 120 passwords must be managed at this single substation (see Figure 3). If a utility owns 100 substations, 12,000 passwords must be managed. For 1,000 substations, the number of passwords grows to 120,000. Considering that password management includes a variety of tasks for each password, including maintaining adequate password complexity, managing frequency of password change, and others, password management alone presents a daunting challenge for utilities (see Figure 4).

First consider one substation…

	1	Substation
x	30	Devices
x	4	Levels of passwords for each device
	120	**Passwords to manage**

But you may manage 1,000 substations…

	1,000	Substations
x	30	Devices
x	4	Levels of passwords for each device
	120,000	**Passwords to manage!**

Figure 3: The password management challenge grows rapidly when considering system-wide assets.

Program Element	Process	End Risk		
Identifying devices	Separate database	Low	Med	**High**
Considering password complexity limitations for various types of IEDs	Matrix within procedure	Low	**Med**	High
Generating compliant passwords	Stand-alone application	Low	**Med**	High
Creating / maintaining list(s) of passwords	Spreadsheets, PDFs, file folder, etc	Low	Med	**High**
Defining frequency of password changes	Work Management System (SAP, etc)	Low	Med	**High**
Maintaining historical audit trail	Passwords: Manual upkeep – Actions: SAP, Corrective maintenance repair, etc.	Low	Med	**High**
Protecting passwords (IEDs) from unauthorized access	Secured file folder	Low	**Med**	**High**
Password update process (both annual and change driven)	Written procedures	Low	Med	**High**
Notifying appropriate personnel of current passwords/changes	Manual alert process (e-mail broadcasts, telephone notifications, etc.)	Low	Med	**High**

Figure 4: The risk of various password management processes without some form of automation is quite high.

Below are details of the key elements of a comprehensive password management program and the manual efforts needed to comply with NERC CIP access and password change requirements:

- **Indentifying Devices** – Utilities need to specifically identify and document Critical Cyber Assets (CCAs) in the system. CCAs are typically logged and maintained in a database.
- **Password Complexity Considerations** – Utilities need to understand the password complexity capabilities for each of the different types of IED included in the list above. Password length and support for special character subsets differ from vendor to vendor and even model to model from the same vendor.

- **Generation of Compliant Passwords** – Utilities need to design and implement a process to ensure compliant passwords are generated for these specific IEDs. Per NERC CIP standards, passwords must be at least six characters and use special characters.
- **Maintaining Passwords Inventory** – Utilities need to create and maintain a list of all current IED passwords and a history of all password changes.
- **Maintaining Password Update Frequency** – Utilities need a method to track the frequency of password changes per IEDs to ensure that all device passwords are changed at least once a year or more often as required.
- **Maintaining Historical Audit Trail** – Utilities need a method to track the history of password changes and track who has had access to these passwords. This is typically managed through manually updated lists.
- **Protecting IEDs from Unauthorized Access** – Utilities need a method to secure the list of passwords and control who has access to these lists. Typically, these password lists are stored in a secure network folder, with access to this folder maintained manually.
- **Maintaining Password Update Process** – Utilities need a method to maintain manual procedures, including detailed password change steps. Maintenance of these procedures can be cumbersome and prone to human error.
- **Notification of Password Changes** – Utilities need a method to inform operators of password changes because password updates on IEDs typically trigger SCADA alarms. Personnel performing the password updates are usually responsible for manually notifying others of pending changes through phone calls or emails sent to operators in advance of the password updates.

Hence, a solution is needed that enables NERC CIP compliance, while enabling efficient remote access and management of IEDs.

SUBNET IED Management Solution

SUBNET Solutions Inc. offers a solution that addresses this challenge. The SUBNET IED Management Solution – PowerSYSTEM Center provides features and benefits in two primary areas: 1) access management, and 2) password management.

Access Management

The SUBNET IED Management Solution – PowerSYSTEM™ Center manages access to IEDs, whether local or remote, providing utilities the access they need to perform a broad range of operational, maintenance, and asset management tasks. It automatically connects to IEDs, so that personnel need not know the process, procedure, or parameters to access the devices; utility personnel can focus on their jobs, not the process of accessing IEDs.

The solution provides single-sign-on capability. It manages role-based access control based on the user's personal IT username and password. Instead of having to know specific connection and password information for every different IED in the system, users need only know their existing IT username and password; the IED management system manages user access rights based on these credentials.

This system operates in a manner similar to the way that network IT systems centrally manage user access to file shares and applications. SUBNET creates solutions that leverage advanced technologies available in today's networking and computer systems. It extends these foundational technologies using electric utility expertise to create advanced solutions that make the grid smarter and more secure.

This solution also centralizes management of the remote access by user, IED, application, task, and command. This provides more efficient management of this process, at a time when staffing shortages due to retiring personnel are increasing. The solution's out-of-the-box reporting provides easy visibility into who accessed which IEDs and when, what changes were made, etc. Users can filter IEDs by regions, name, location, or title to view only desired devices.

No SUBNET client software is required on the end user computer, and no additional local substation hardware is needed. These features reduce costs and help prevent malware on an authenticated users PC from entering substations. The solution supports all common connection types, including Ethernet and dial-up.

SUBNET IED Management Solution – PowerSYSTEM Center provides remote access to utility assets, while helping to comply with NERC CIP requirements (see next section). It minimizes time to establish access to remote IEDs, saving personnel time. The solution increases the reliability of the utility's infrastructure by facilitating remote diagnosis and repair of substation equipment problems. The solution leverages, rather than reinvents, existing IT infrastructure and policies.

Password Management

The SUBNET IED Management Solution – PowerSYSTEM Center automates the password management process for all IEDs, aiding compliance with NERC CIP. It becomes the secure password vault and repository for all IED passwords. More than that, however, administrators can make password changes at pre-scheduled times, while preserving the ability to make password changes on demand or manually, as required. They can grant and control local IED access without additional hardware at the substation.

Administrators can define password policies on a per IED basis to create highly granular control over password policies, rather than a one-size-fits-all solution. Its deep, multi-tiered substation architecture communication support enables scripting to automatically authenticate through the various layers of software and hardware security to reach the target device. This configurable scripting engine is vendor neutral.

The solution provides a wide variety of out-of-the-box reporting. Administrators can obtain an auditable record of all changes to passwords (i.e., a change history) and an auditable record of all IED access, including authorized access and unauthorized attempts. Other reports include user and administrator permission audit reporting, manual access device job scheduling, and integration with standard IT event logging (e.g., Microsoft® Windows® Event Log). These capabilities facilitate NERC CIP audit reporting. Administrators can also receive automatic notifications about password changes, access to systems, and reminders to change or update passwords.

By providing role-based access control and comprehensive password management functionality, the SUBNET IED Management Solution – PowerSYSTEM Center facilitates NERC CIP compliance and is a key part of a comprehensive solution needed for full compliance. It simplifies and facilitates NERC CIP audits by delivering easily maintained and accessible audit records. And, of course, it lowers security risk.

The solution allows employees to better focus on their job function. It minimizes labor required to perform password changes by simplifying the password maintenance process. As a result, it lowers risk and increases reliability.

Because the solution is multi-vendor, it frees the utility to use the best or most appropriate hardware and software throughout their utility wide system, rather than locking in the utility to specific vendor solutions. At the same time, the solution leverages the existing practices and processes of existing IT infrastructure, reducing costs and increasing efficiency. For example, the utility can make use of existing Microsoft Active Directory authentication, leverage existing data warehousing systems, and avoid staff training on new technologies.

Unified Grid Intelligence

Figure 5 shows how the SUBNET IED Management Solution – PowerSYSTEM Center solution fits into what SUBNET calls a Unified Grid Intelligence.

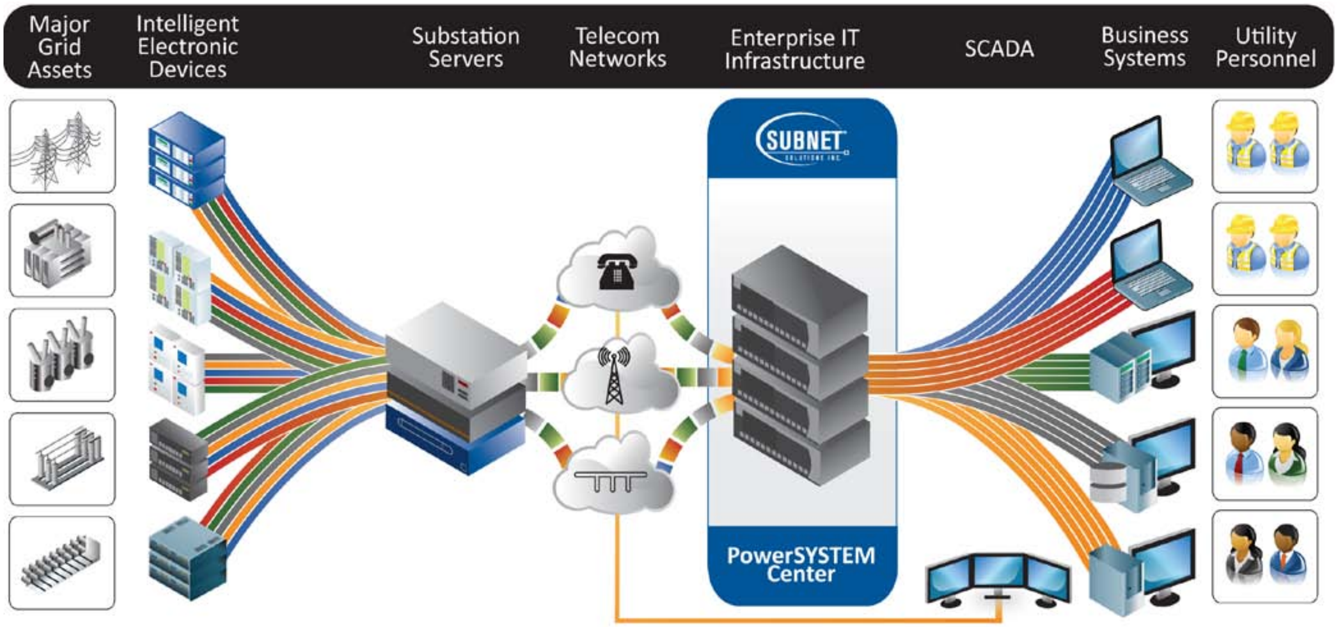

Figure 5: The SUBNET IED Management Solution - PowerSYSTEM Center solution securely manages the exchange of data between corporate networks and substations.

SUBNET's Unified Grid Intelligence philosophy is a holistic approach providing interoperable solutions between many different field IEDs, to many different business systems, over many different types of communication networks. The goal of these solutions is to provide true multi-vendor, multi-function interoperability between any intelligent electronic device, to any utility business system, securely over any communication network. SUBNET's solutions integrate with utilities' existing IEDs, IT networks, and engineering productivity tools to deliver data efficiently and securely to analysts, maintenance personnel, and SCADA operators.

As part of this Unified Grid Intelligence, Figure 5 shows that the SUBNET IED Management Solution – PowerSYSTEM Center is designed to be deployed at a centralized location on the utility enterprise. The solution helps convert a power system full of smart substations into a smart power grid. System intelligence unifies the source of real-time information to any utility business system that requires it, enabling timely, informed and secure operation of the entire power system. The solution is also easily upgraded and will evolve with technological change as needed.

Conclusions

For utility industry professionals who need to remotely access and/or manage IEDs while complying with NERC CIP regulations, SUBNET offers an IED Management Solution that provides simple, effortless, and secure access to remote IEDs that can be systematically controlled, recorded, and easily managed. SUBNET's IED Management Solution centrally controls and manages both remote and local IED access on a per-user, per-IED and/or per-application basis without requiring additional hardware in every substation. The solution enables personnel to centrally manage passwords and password change policies and processes whether automatic or manual ("on demand"), and supports both Ethernet and secure dial-up connections.

Benefits of implementing this solution include the following:

- Improved efficiency of expert personnel
- Improved access of substation data by authorized personnel
- Enhanced security
- Reduces risk of injury
- Minimizes substation disruption
- Facilitated compliance with NERC CIP legislation, avoiding fines
- Minimizes disturbances, improving reliability
- Minimized travel, reducing maintenance costs

For More Information

SUBNET Solutions Inc.
Tel: 1.403.270.8885
Email: info@SUBNET.com
Website: www.SUBNET.com
Facebook: www.facebook.com/subnetsolutions
Twitter: www.twitter.com/subnetsolutions
LinkedIn: www.subnet.com/linkedin

About SUBNET

SUBNET Solutions Inc. is a global software solutions provider for electrical utilities. SUBNET focuses on Making Substations More Intelligent®. Founded in 1992, SUBNET is an industry leader providing intelligent solutions that securely connect real time electrical utility field information with utility business systems to enable Smart Grid solutions. Over 200 utilities worldwide rely on SUBNET software to safely manage and monitor thousands of substations.