INL/EXT-09-15321

# National SCADA Test Bed Substation Automation Evaluation Report

October 2009

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-09-15321

# National SCADA Test Bed Substation Automation Evaluation Report

October 2009

Idaho National Laboratory
INL Critical Infrastructure Protection/Resilience Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

INL/EXT-09-15321

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

# National SCADA Test Bed Substation Automation Evaluation

*October 2009*

Reviewed By: _____

Date: 11/3/2009

NSTB

National SCADA Test Bed

*Enhancing control systems security in the energy sector*

**DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any employee, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, or any information, apparatus, product, or process disclosed in this publication, or represents that its use by such third party would not infringe privately owned rights.

# ABSTRACT

Increased awareness of the potential for cyber attack has recently resulted in improved cyber security practices associated with the electrical power grid. However, the level of practical understanding and deployment of cyber security practices has not been evenly applied across all business sectors. Much of the focus has been centered on information technology business centers and control rooms. This report explores the current level of substation automation, communication, and cyber security protection deployed in electrical substations throughout existing utilities in the United States. This report documents the evaluation of substation automation implementation and associated vulnerabilities. This evaluation used research conducted by Newton-Evans Research Company for some of its observations and results. The Newton-Evans Report aided in the determination of what is the state of substation automation in North American electric utilities. Idaho National Laboratory cyber security experts aided in the determination of what cyber vulnerabilities may pose a threat to electrical substations. This report includes cyber vulnerabilities as well as recommended mitigations. It also describes specific cyber issues found in typical substation automation configurations within the electric utility industry.

The evaluation report was performed over a 5-month period starting in October 2008.

# EXECUTIVE SUMMARY

The Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program commissioned a study by the Idaho National Laboratory (INL) NSTB Program in Fiscal Year (FY) 2009 to evaluate security of substation automation in the electricity industry.

In order to determine the level of automation deployed in North American utility substations, INL used the Newton-Evans Research Company survey, *The World Market for Substation Automation and Integration Programs in Electric Utilities: 2008–2010, Volume I North American Market*,[1] for some of its data. Research showed the level of substation automation varies widely. The survey respondents were comprised of investor-owned utilities, public power, and rural electric cooperatives, including Canadian entities.

The data from this report indicates the level of substation automation varied a great deal depending on type of substation, type of utility, the size of the utility, and survey question interpretation. Overall, 81% of transmission substations had some level of automation, while 57% of distribution type substations had some level of automation[1]. The level of automation ranged from Stage 1 to Stage 4. Automation stages are defined in Table MS-1 of this report.

Smaller rural electric cooperatives tended to have more deployed automation than investor-owned utilities and public municipalities as they have a smaller number of substations to upgrade. A significant number of substations in the larger investor-owned utilities had no automation at all. Rural electric cooperatives are generally smaller requiring less expense to provide an increased level of substation automation. In addition, rural electric cooperatives generally cover a larger area per meter base; therefore, a higher level of substation automation is more easily justified economically.

Another observation of this study was that utility personnel had excellent security awareness of measures that are required as well as published "best practice guides." Smaller utilities not part of the "bulk electric system" closely followed the Critical Infrastructure Protection (CIP) 002–009 Standards.

Research showed that there were many different vendors supplying equipment depending on which substation automation device was used. In an application where many of the devices connected are from different vendors, they may or may not share similar vulnerabilities, however some vulnerabilities tend to be common across these devices, which require the application of protective schemes to reduce their vulnerability footprint in system installation.

INL recommends initiating additional research to develop recommended guidance to implement cyber security in substation automation technologies and architectures. This guide would provide additional detail for securing communications related to substation automation and the equipment itself. The request for such research and documented guidance was common among utility personnel interviewed.

# MANAGEMENT SUMMARY

The consequence of an aggressor gaining cyber access to automated systems and networks is their ability to usurp monitoring and control of control system connected equipment. Once a foothold is established at the substation level, further migration into the central control room network could provide the aggressor with access to the entire utility system.

The Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) program commissioned a study by the Idaho National Laboratory (INL) NSTB Program in Fiscal Year (FY) 2009 to evaluate substation automation in the electricity industry. There is significant proactive effort within the industry and utilities to implement security in their respective electrical substations. Utilities are in a continual process of migration from older electromechanical relays to newer, modern microprocessor-based relays. In addition, they are also upgrading other substation automation devices to the latest technology. This process requires continued emphasis on implementation of cyber security as required by regulations, standards, and best practices. It is projected that this modernization process will continue until such time that older relays and other substation automation devices have been replaced according to individual company automation standards.

The results of this study imply that substation automation for electrical substations is standard now for utilities, and implementation will continue. Therefore, the need for applicable standardized cyber security implementation practices is also needed.

Cyber security must be implemented for substation automation equipment using the cradle-to-grave philosophy. From the equipment specification stage to the equipment disposal stage, cyber security is a necessity for this industry sector. To protect electrical substations from cyber threats, mere compliance to applicable standards or other methods will not be sufficient. A proactive best practice model using latest industry technology and vendor implementation must be used.

Key questions regarding substations include: what level of automation is implemented, and assuming some level of automation, what is the risk that these automation systems can be exploited to cause damage or widespread power outages? The Newton-Evans Research Company Substation Automation 2008 (NESA 2008) survey provides good insight into helping answer these questions. The survey defines four stages of automation with respect to intelligent electronic devices, or IEDs. These automation stages are listed in Table MS-1.

Table MS-1. Stages of substation automation.

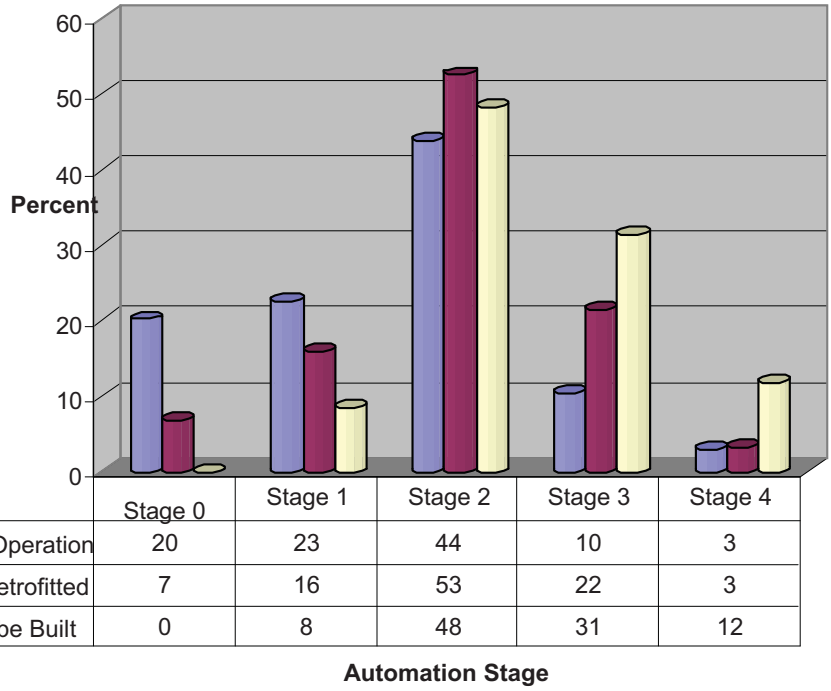
| Stages of Substation Automation | |
|---|---|
| Stage 0 | No automation technologies installed. |
| Stage 1 | Most equipment manually operated through local switching. Some programmable Intelligent Electronic Devices (IED) implemented, but no communications with central control room other than some monitoring. |
| Stage 2 | Some electromechanical devices remain. Installed IEDs are integrated, using two-way serial communications capability and no substation LAN, allowing monitoring and control from the central control room. |
| Stage 3 | Some electromechanical devices remain. Installed IEDs are integrated, using two-way serial and/or LAN communications allowing monitoring and control from the central control room. |
| Stage 4 | Installed IEDs are integrated, using LAN communications. Applications are run at the substation level to automate various substation functions with full control from the central control room. |

Respondents to the survey were asked to categorize their substations into these stages. Because automation philosophies are often different between transmission and distribution substations, the results are broken down separately for each of these categories.

## Substation Overview

## Transmission Substations

Approximately 17,325 transmission substations are in the U.S. and Canada. Of these, 4,594 (27%) are represented in the survey, which includes a cross section of investor-owned utilities, public power, municipals, and cooperatives. Of the 4,594 substations represented, 3,594 were categorized by the survey respondents. Figure MS-1 shows the results.



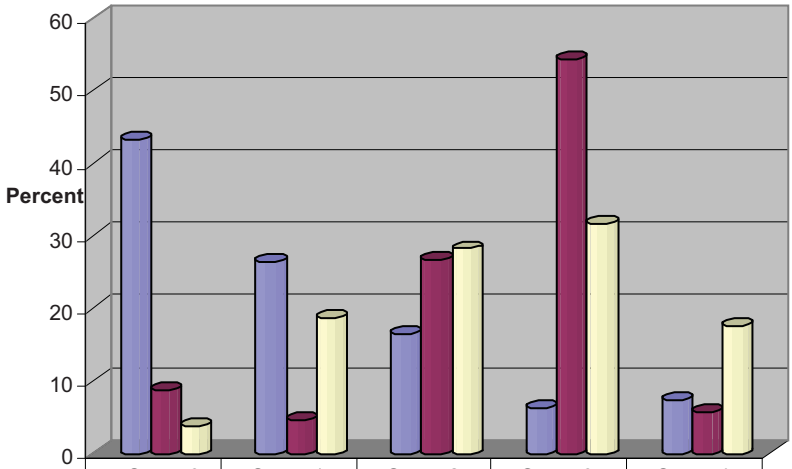

| | Stage 0 | Stage 1 | Stage 2 | Stage 3 | Stage 4 |
|---|---|---|---|---|---|
| Now In Operation | 20 | 23 | 44 | 10 | 3 |
| To Be Retrofitted | 7 | 16 | 53 | 22 | 3 |
| New to be Built | 0 | 8 | 48 | 31 | 12 |

Figure MS-1. Transmission substation automation levels.

As seen in Figure MS-1, most transmission substations fall into the Stage 2 category. This is true for both existing substations and those planned to be retrofitted or built new. Not surprisingly, new substations are more likely to be integrated at Stages 3 or 4 than existing or retrofit substations. Also, nearly 20% of existing substations have no automation at all; another 20% have IEDs that are not integrated. In other words, from these results 4 in 10 of the respondent transmission substations currently have no communications paths to IEDs.

## Distribution Substations

Distribution substations show more disparity between current and planned automation levels. According to Figure MS-2, more distribution substations have no automation than any other category with 69% of respondents indicating no integrated IED communications. The bulk of retrofit substations are planned to be integrated at Stage 3. Nearly all new distribution substations have planned substation automation with a minimum level of Stage 2 and half of all respondents planning Stage 3 and 4 installations.




| | Stage 0 | Stage 1 | Stage 2 | Stage 3 | Stage 4 |
|---|---|---|---|---|---|
| Now In Operation | 43 | 26 | 17 | 6 | 7 |
| To Be Retrofitted | 9 | 5 | 27 | 54 | 6 |
| New to be Built | 4 | 19 | 28 | 32 | 18 |

**Automation Stage**

Figure MS-2. Distribution substation automation levels.

According to the NESA 2008 survey,[1] Figure 3 shows an estimate forecast for respondent expenditures associated with substation automation. It is evident that substation automation implementation is increasing and older electromechanical devices are continually being replaced with microprocessor-based devices with varying levels of communications integration. Figure MS-3 shows that substantial funding is planned by utilities on substation automation and integration programs.

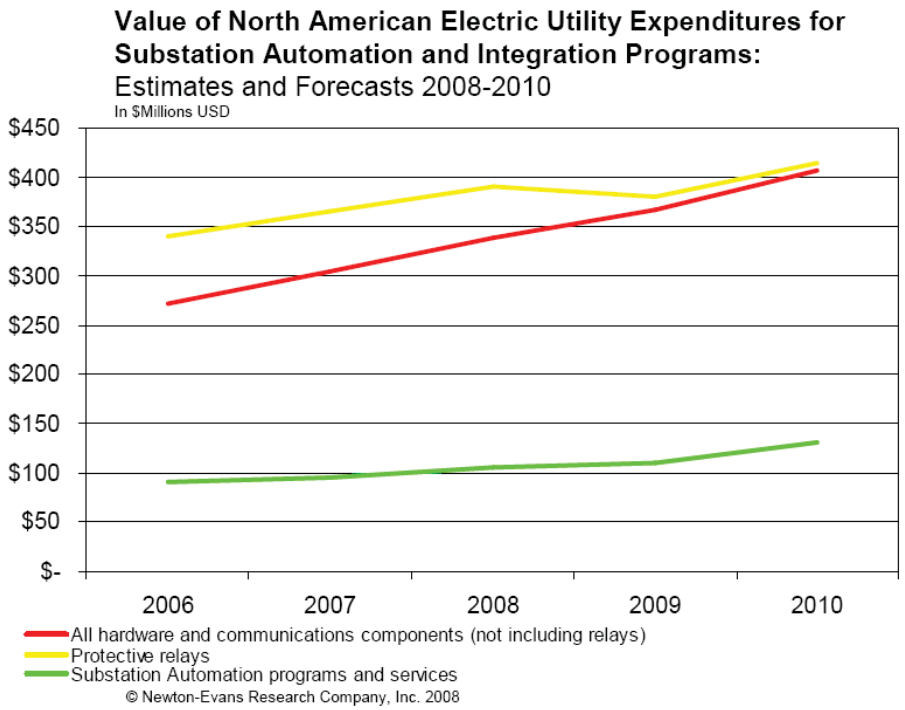



Figure MS-3. Substation automation expenditures for North America.

## GENERAL RECOMMENDATION FOR SUBSTATION SECURITY

Given the potential system consequences and gaps in security identified in this report, it is clear that there is still work to be accomplished to achieve an acceptable level of security with respect to substation automation. The needed security improvements will require not just a commitment from utilities, but a coordinated effort among utilities, manufacturers, service providers, regulators, and others. The sections that follow contain recommendations of actions necessary to aid in this effort.

### Recommended Practices

Some recommended practices have been written by the DOE NSTB program, Department of Homeland Security Control Systems Security Program (CSSP), or other entities that apply to substation automation systems. These include:

- "Recommended Practice for Securing Control System Modems," Department of Homeland Security, January 2008.
- "Wireless Recommended Practice," Electric Power Research Institute et al., 2009.

However, no recommended practice document focuses on substation automation devices, communication types, and specific mitigation strategies for substations. Therefore, the INL recommends that a subsequent document be generated, "Recommended Practices for Securing Substation Automation Devices." A second recommendation for this effort would be the generation of procurement language for substation automation, similar to existing language written for SCADA/Energy Management System (EMS) and process control systems[5].

## Vendor Assessments

Through NSTB and other program efforts, several substation automation devices have been assessed for their level of cyber security. In every case, cyber vulnerabilities have been found. Work is ongoing with vendors to mitigate these vulnerabilities. However, most of the work has been focused on answering specific questions for specific projects, so there has been no comprehensive effort to assess the majority of substation automation devices and the communications devices they rely on.

Assessments of the most commonly used substation automation devices should be performed, including RTUs and protective relays in particular. In addition, the products of the major vendors of communications equipment should also be assessed.

## Onsite Assessments

Based on INL onsite visits and other contacts with utilities, there is a desire and a need to know more about implementation of substation automation security. Onsite assessments provide real-world practical solutions for industry partners. Onsite assessment recommendations:

1. Perform at least one full hands-on onsite assessment with a utility that has already implemented substation automation at Levels 3 and/or 4 to determine the component and systemic vulnerabilities that are present.
2. Support utilities in the process of upgrading their substations specifically in the area of cyber security to help them through some of the security issues and learn what issues arise in these cases. These lessons learned could be rolled into a substation automation recommended practice document for others to use as they implement substation automation systems.
3. Include in one substation automation assessment, the communication provider for leased line systems. The pervasive attitude that serial, non-routable communications are relatively secure is based on the assumption that the provider's system is secure. This assumption should be validated by including an assessment on the security of the provider's network.

## Training

Most of the utility personnel who were visited as part of this effort indicated an interest in training opportunities that include increasing awareness of potential substation vulnerabilities, methods of detecting intrusions or attacks, and ways of recovering from attacks. One of the issues with substation automation is that, as opposed to control center security, engineers often make more of the decisions in terms of security as opposed to Information Technology (IT) personnel, especially in non-networked environments. Engineers often are not as aware of security issues and implementation tradeoffs. Providing training opportunities, whether in live classes or online tutorials or both, would be of great help. In some cases, INL could adapt training programs already in place to meet these needs. Other training programs may need to be developed, but would be worthwhile to help increase the general knowledge and awareness of engineers with respect to security.

## ACKNOWLEDGMENT

This document is developed for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability to assist in understanding the extent to which the North American electrical substations are being automated. Idaho National Laboratory would like to recognize the valued expertise, accommodating consulting support, and survey preparation and information provided by Chuck Newton and his research team, Newton-Evans Research Company, Inc. In addition, Idaho National Laboratory would like to thank the utilities that provided valuable insight and participated in meaningful discussions on the current state of substation automation in electrical substations.

# CONTENTS

ABSTRACT ..... iii

EXECUTIVE SUMMARY ..... v

MANAGEMENT SUMMARY ..... vii
- Recommended Practices ..... x
- Vendor Assessments ..... xi
- Onsite Assessments ..... xi
- Training ..... xi

ACKNOWLEDGMENT ..... xiii

ACRONYMS ..... xxi

1. PROJECT OVERVIEW ..... 1
   - 1.1 Background ..... 1
   - 1.2 Purpose ..... 2
   - 1.3 Audience ..... 2
   - 1.4 Previous Work Completed ..... 2
   - 1.5 Methodology ..... 3

2. SECURITY ..... 5
   - 2.1 Cyber Security ..... 5
   - 2.2 Physical Security ..... 7

3. CYBER VULNERABILITIES OF SUBSTATIONS AND RECOMMENDATIONS ..... 8
   - 3.1 Substation Vulnerabilities ..... 8
     - 3.1.1 Substation Automation Security Vulnerabilities ..... 8
   - 3.2 Cyber Vulnerabilities ..... 10
     - 3.2.1 Vulnerability: Physical Access ..... 10
     - 3.2.2 Vulnerability: Clear Text Protocols (DNP 3.0) ..... 11
     - 3.2.3 Vulnerability: IED Accessibility/Use of Routable Paths to End Devices ..... 12
     - 3.2.4 Vulnerability: Separate Protection and Control ..... 13
     - 3.2.5 Vulnerability: Open Source Information Available ..... 14
     - 3.2.6 Vulnerability: Dual-Ported RTU Vulnerability ..... 15

4. POTENTIAL CONSEQUENCES OF EXPLOITATION OF VULNERABILITIES ..... 16
   - 4.1 Power Outage ..... 16
   - 4.2 Grid Instability ..... 16
   - 4.3 Loss of SCADA Control ..... 17
   - 4.4 Loss of SCADA Related Information ..... 17

5. SUBSTATION AUTOMATION TECHNOLOGIES ..... 18
   - 5.1 Categorizing Phases of Substation Automation ..... 18
     - 5.1.1 Stage 1 Automation ..... 19

5.1.2 Stage 2 Automation ..... 20
5.1.3 Stage 3 Automation ..... 20
5.1.4 Stage 4 Automation ..... 21
5.2 State of Substation Automation Overview ..... 21
5.2.1 Transmission Substations ..... 21
5.2.2 Distribution Substations ..... 22
5.2.3 Substation Automation Forecast ..... 23
5.3 Substation Automation Technologies ..... 24
5.3.1 Remote Terminal Units ..... 26
5.3.2 Programmable Logic Controller ..... 27
5.3.3 Substation controller/gateway ..... 28
5.3.4 Protective Relay ..... 29
5.3.5 Smart Meters ..... 30
5.4 Communications Paths ..... 31
5.4.1 Substation to Control Center ..... 33
5.4.2 Substation to Substation ..... 34
5.4.3 Engineering/Maintenance Access ..... 35
5.4.4 Substation to End Device ..... 37
5.4.5 Vendor Access to Substation ..... 38
5.5 Protocol Usage ..... 39
5.6 Vendors of Communication Equipment ..... 40
5.6.1 Leased Line ..... 40
5.6.2 Fiber Optic ..... 41
5.6.3 Licensed Radio ..... 41
5.6.4 Microwave ..... 42
5.6.5 Spread Spectrum ..... 42
5.6.6 T-1 ..... 43

6. Substation Automation Case Studies ..... 44
6.1 General Observations ..... 44
6.2 Investor-owned Utility 1 ..... 44
6.2.1 Overview ..... 44
6.2.2 Substation Communications ..... 44
6.2.3 Substation Automation ..... 45
6.2.4 Substation Physical Security ..... 45
6.3 Electric Cooperative 1 ..... 45
6.3.1 Overview ..... 45
6.3.2 Substation Communications ..... 45
6.3.3 Substation Automation ..... 46
6.3.4 Substation Physical Security ..... 46
6.4 Municipality ..... 47
6.4.1 Overview ..... 47
6.4.2 Substation Communications ..... 47
6.4.3 Substation Automation ..... 48
6.4.4 Substation Physical Security ..... 48
6.5 Investor-owned Utility 2 ..... 48
6.5.1 Overview ..... 48
6.5.2 Substation Communications ..... 49

6.5.3 Substation Automation ..... 49
6.5.4 Substation Physical Security ..... 50
6.6 Electric Cooperative 2 ..... 50
6.6.1 Overview ..... 50
6.6.2 Substation Communications ..... 50
6.6.3 Substation Automation ..... 51
6.6.4 Substation Physical Security ..... 51
6.7 Observations from Utility/Substation Visits ..... 51

7. STANDARDS AND RECOMMENDATIONS ..... 52
7.1 Bulk Electric System ..... 52
7.2 Other Standards ..... 52

8. GENERAL RECOMMENDATIONS FOR SUBSTATION SECURITY ..... 53
8.1 Recommended Practices ..... 53
8.2 Vendor Assessments ..... 53
8.3 Onsite Assessments ..... 53
8.4 Training ..... 54

9. SUBSTATION TECHNOLOGIES ..... 55
9.1 Substation Overview ..... 55

10. REFERENCES ..... 57

# FIGURES

Figure MS-1. Transmission substation automation levels. ..... viii
Figure MS-2. Distribution substation automation levels. ..... ix
Figure MS-3. Substation automation expenditures for North America. ..... x
Figure 1. Current and planned usage of substation security measures. ..... 5
Figure 2. Encryption of protocols used for communications between substation and external host. ..... 6
Figure 3. Security of remote connections (such as modems, wireless, IP). ..... 6
Figure 4. Extent of use of password management system for remotely accessible IEDs. ..... 7
Figure 5. Ethernet port security implementation for IP communications to substations. ..... 7
Figure 6. Vulnerability of clear-text communications public switch telephone network. ..... 11
Figure 7. Vulnerability of communications via the Internet. ..... 12
Figure 8. Accessibility to substation devices via a modem. ..... 13
Figure 9. Current use of separate protection and control (P&C) devices used for monitoring and control of substation equipment. ..... 14
Figure 10. Stage 1 substation automation. ..... 19
Figure 11. Stage 2 substation automation. ..... 20
Figure 12. Stage 3 substation automation. ..... 20
Figure 13. Stage 4 substation automation. ..... 21
Figure 14. Transmission substation automation levels. ..... 22
Figure 15. Distribution substation automation levels. ..... 23
Figure 16. Substation automation expenditures for North America. ..... 24
Figure 17. Substation automation devices deployed in transmission substations—current and planned. ..... 25
Figure 18. Substation automation devices deployed in distribution substations—current and planned. ..... 26
Figure 19. RTU manufacturers by market share. ..... 27
Figure 20. PLC manufacturers by market share. ..... 28
Figure 21. Manufacturers of substation controller/gateway by market share. ..... 28
Figure 22. Protective relays manufacturers by market share. ..... 30
Figure 23. Smart meter manufacturers by market share. ..... 31
Figure 24. Example diagram highlighting substation communications paths. ..... 32
Figure 25. Substation to control center communications channels—current and projected. ..... 33
Figure 26. Substation to control center communications channels by utility type. ..... 34
Figure 27. Substation-to-substation communications by channel type. ..... 35
Figure 28. Substation-to-substation communications by entity type. ..... 35

Figure 29. Engineering and maintenance communications by type. 36
Figure 30. Engineering and maintenance communications by entity type. 36
Figure 31. Substation-to-end device communications by type. 37
Figure 32. Communications-to-end devices by entity type. 37
Figure 33. Vendor communications by type. 38
Figure 34. Vendor communications by entity type. 38
Figure 35. Current and future protocol usage among utilities. 39
Figure 36. Protocol use by entity type. 40
Figure 37. Vendors of communication equipment. 40
Figure 38. Vendors of fiber optic communications equipment. 41
Figure 39. Vendors of licensed radio equipment. 42
Figure 40. Vendors of microwave equipment. 42
Figure 41. Vendors of spread spectrum equipment. 43
Figure 42. Vendors of T-1 multiplexers. 43
Figure 43. Typical communications to substation. 45
Figure 44. Communications to substation. 46
Figure 45. Typical substation control building. 47
Figure 46. Simplified communications architecture. 49
Figure 47. Simplified communications diagram. 50

## TABLES

Table MS-1. Stages of substation automation. vii
Table 1. Stages of substation automation. 19
Table 2. Substation devices. 55

# ACRONYMS

| | |
|---|---|
| ABB | Asea Brown Boveri |
| BES | Bulk Electric System |
| CDMA | Code Division Multiple Access |
| CIP | Critical Infrastructure Protection |
| CSSP | Control System Security Program |
| DNP | Distributed Network Protocol |
| DOE | Department of Energy |
| DPCD | Digital control protective devices |
| EMS | Energy Management Systems |
| FY | Fiscal Year |
| GE | General Electric |
| GSM | Global System for Mobile Communication |
| HSPD-7 | Homeland Security Presidential Directive 7 |
| IEC 60870-5 | International Electrotechnical Commission telecontrol protocol |
| IED | Intelligent Electronic Device |
| IEEE | Institute of Electrical and Electronic Engineers |
| INL | Idaho National Laboratory |
| IP | Internet Protocol |
| IT | Information Technology |
| LAN | Local area network |
| LTC | Load tap changer |
| MAC | Media Access Control |
| MDS | Microwave Data Systems |
| MitM | Man-in-the-Middle |
| NERC | North American Electric Reliability Corporation |
| NESA | Newton-Evans Company Substation Automation |
| NSTB | National SCADA Test Bed |
| OE | Office of Electricity Delivery & Energy Reliability |
| P&C | Protection and control |
| PLC | Programmable logic controller |
| PSTN | Public switched telephone network |
| R&D | Research and Development |
| RTU | Remote terminal unit |

| | |
|---|---|
| SCADA | Supervisory Control And Data Acquisition |
| SEL | Schweitzer Engineering Laboratory |
| SONET | Synchronous Optical Network |
| TCP | Transmission Control Protocol |
| USB | Universal Serial Bus |
| VAR | Volt Amp Reactive |
| VoIP | Voice over IP |

# National SCADA Test Bed Substation Automation Evaluation Report

## 1. PROJECT OVERVIEW

Homeland Security Presidential Directive 7 (HSPD-7)[2] empowers the U.S. Department of Energy (DOE) as the Sector-Specific Agency to lead the federal government's efforts to help protect critical energy infrastructures from physical and cyber attacks. DOE assigned the Office of Electricity Delivery and Energy Reliability (OE) to fulfill this role as the designated Sector-Specific Agency for critical infrastructure protection.

DOE-OE, National Laboratories, industry, and academia are working to help lead a national effort to modernize the electric grid, enhance security and reliability of the energy infrastructure, and facilitate recovery from disruptions to energy supplies.

The nature of developing credible defenses for critical cyber components is a necessary dynamic activity. The rapid advances in cyber technology in business systems has fostered an equally dynamic explosion in identified exploits and vulnerabilities used, developed, and currently being deployed. Control systems have traditionally been isolated from any open nonproprietary communication networks. Economics, fast response time, and new features possible with new technology are the primary motivation for upgrading legacy systems. The issue with this evolution is that security awareness and the possibilities of cascading or unintended cyber consequences have lagged in the deployed development of control systems. Part of this project is to research security issues to prevent or minimize the effects of exploitation, incapacitation, or degradation of critical infrastructures and key resources, specifically in the substation automation arena. The other part is educational awareness to asset owners and component vendors on ways to improve cyber security.

### 1.1 Background

DOE-OE is responsible to ensure a secure and reliable flow of energy to America's homes, businesses, industries, and critical infrastructures. One of the major OE efforts in this area is to plan, manage, and oversee multi-laboratory research and development (R&D) programs performing research on control systems security conducted in the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB).

The NSTB program was established in 2003 by DOE-OE to help improve the security of cyber assets in the energy sector, especially for SCADA systems, through specific research and development, system assessments, testing, validation, training, and outreach. The NSTB supports both industry and government efforts in improving the security of control systems hardware, software, and operation for energy communications and control infrastructure.

NSTB cyber vulnerabilities assessments to date have focused primarily on control systems located in control centers and on specific devices and technologies used in protecting data essential to the reliable and efficient operation of the electric grid. While compromises to these control systems have immediate impacts on electric grid operations, significant grid impacts can also occur when compromised remote and unmanned substations are used to access and manipulate local or networked systems and equipment.

A large amount of control system equipment is located within unmanned substations. Substations are located both in remote rural and dense urban locations and are much more numerous than control centers as a matter of necessity. Evaluation of this substation control system equipment from a cyber perspective is deemed necessary in order to gather all information supporting this industry sector.

## 1.2 Purpose

The main objective of this effort is to determine the extent to which electrical substations are vulnerable to directed cyber attacks and to provide recommendations for mitigation of identified common vulnerabilities. This is a direct response to the Roadmap priority[4] of identifying best practices for physical and cyber security for remote facilities.

Energy Management Systems (EMS), Digital Control Systems, and SCADA systems intelligently automate the protection and control of interconnected energy systems integral to the nation's energy sector. Protecting and improving these systems against malicious cyber attacks and reducing system vulnerabilities are vital to national security.

Today's utilities are finding that substation automation devices are increasing in functionality and complexity. Newer devices are incorporating communications along with the microprocessor-based functionality enhancing the capability of the device. It is becoming standard for substation relays to provide protection, control, and communications all in one box.

In general DOE-OE has tasked Idaho National Laboratory (INL) to investigate:

- To what stage are the North American substations automated?
- How fast are the utilities willing to upgrade to newer digital technologies?
- Are utilities aware of and incorporating sound cyber-intrusion prevention designs and procedures?
- Are the North American substations susceptible to cyber intrusion?

This document presents information gathered on the implementation of current and emerging substation automation technologies and configurations in the majority of the nation's substations. Malicious cyber attacks on these automated infrastructure systems can jeopardize national security by affecting the ability of the nation's critical infrastructures to provide essential services to the country's asset owners and populous in general.

## 1.3 Audience

This report provides a graded approach to substation automation information. The intended audience may have high-level or detailed working knowledge of substation control systems, system communication protocols, and substation protection. Relevant information would be useful to:

- Electrical utilities
- Intelligent electronic device (IED) component manufactures
- Managers and security consultants
- Substation engineers, systems designers, and architects
- System administrators and other information technology (IT) professionals who administer substation automation systems.

## 1.4 Previous Work Completed

INL has previously performed cyber assessments on substation automation components and larger control systems as part of the NSTB. This testing provides a secure, repeatable, and defensible challenge to specific system configurations or components for either asset owners or vendors seeking to validate component and system configurations.

## 1.5 Methodology

INL has been chartered to correlate laboratory analytical challenges/exploits against the level of automation deployed in the nation's electrical substations.

The project is contracted with the electric utility industry research company Newton-Evans Research Company Inc. to assist in obtaining relevant substation automation data. Analyzing information of a representative subset of North American substations provides a better understanding of the current level and extent of deployed automation technologies used in substations. The INL and Newton-Evans project team developed additional survey topics to enhance industry response and establish a better understanding of the current substation automation landscape. This report will analyze and assess the level of potential vulnerability risks inherent in these applications.

Newton-Evans has over 30 years experience in working with the electric utility sector, gathering utility information and providing the results to government agencies, utilities, standards committees, etc. Newton-Evans has established five stages of deployed automation (Stage 0 being no automation, to Stage 4 being fully integrated and automated from a central control station). The substation automation survey by Newton-Evans, hereafter referred to as NESA 2008, provides information for general trending, but does not present enough technical information to determine granularity of deployed automation.

The NESA 2008 survey draws from a sample base of 100-plus utilities involved in power generation, transmission, and distribution. The type and number of respondents was comprised of the following:

| Location and Type | | No. of Respondents |
|---|---|---|
| U.S. | Investor owned | 30 |
| | Public Power | 33 |
| | Public Power | 29 |
| Canada | | 13 |

Factors, such as type, service, and level of regulation affect extent of deployed substation automation. The needs and requirements of small regional distribution utilities are different than multi-state generation/transmission utilities. This large variation in deployed automation has impacted how asset owners have interpreted questions pertaining to substation automation in the primary NESA 2008 survey using either very broad or very narrow definitions of substation automation.

Analyzing this survey information provides an opportunity to better understand the current automation technologies being implemented now and planned for the future within the nation's substations.

The assumptions using the NESA 2008 data for this report are:

- The 106 responders to the survey provide an acceptable cross-sectional representation of the status of substation automation in North America
- The survey information reflects an accurate operational system configurations snapshot of existing and planned substation automation designs.

INL performed five field evaluations of utility substations to gain insight and obtain a "pulse" of a limited number of utilities in order to evaluate systems and processes being implemented, current trends on equipment upgrade projects and policies, rationalization, reason, motivation, and how commercial energy sector personnel perceive current and future cyber threats.

Field visits provide a better understanding of how the survey questions were answered. During the site visits, a team from INL and Newton-Evans interviewed utilities that represent large investor-owned utilities, municipalities, and smaller rural electric cooperatives. The host utility team ranged from one person to an integrated team consisting of representatives of Cyber Security, Asset Management, Control Engineering, and Planning Management. The INL/Newton-Evans team asked each utility a specific number of subject/talking points questions relating to the current status of their substation automation. Questions include the number of substations under the utility control and what type of equipment is being used and how. Future growth plans were also queried to determine what level of upgrade automation the utility is planning for future deployment. This question and answer session was designed to foster free-flow conversations among all attendees, answering questions where possible about cyber attack, prevention, and where to find further information on exploits and remediation information. The visit also included a physical visit to at least one representative substation where possible. Proprietary or sensitive information identified and protected by the utility is not part of this report.

# 2. SECURITY

There are two primary interrelated areas of security with respect to substation automation and electrical substations. These are cyber security and physical security.

Cyber security focuses on the prevention of unauthorized access to computer-controlled devices and potential control/manipulation of substation automation equipment used in electrical substations. The goal of cyber security should be the prevention of unauthorized intrusion and access to electronic communication and control mechanisms both locally and remotely.

Physical security is the protection of physical assets and includes fences, gates, locks, doors, video surveillance cameras, and electronic intrusion detection of control rooms and remote facilities (substations, generators, transmission lines) as well as policies with regard to protective and timely response. The primary goal of physical security is to keep unauthorized people out of electrical substations.

These two areas interface when physical access or intrusion is required to initiate a cyber intrusion.

Figure 1 shows current and planned use of substation security measures from the respondents of the NESA 08.

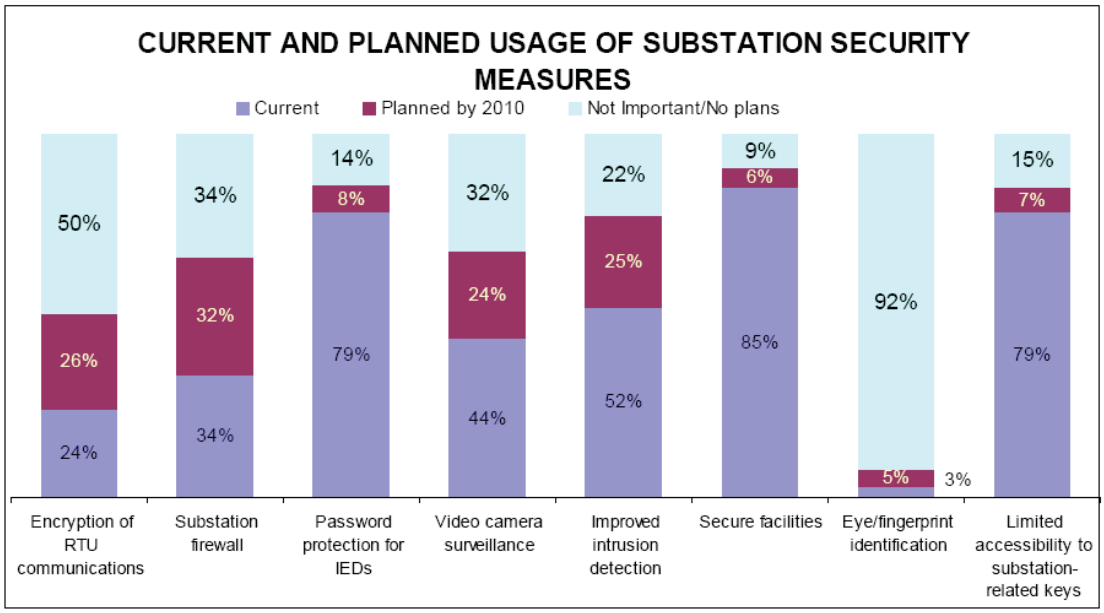



Figure 1. Current and planned usage of substation security measures.

## 2.1 Cyber Security

For control systems deployed in critical infrastructure operations, such as substation automation, unplanned, untested, and unauthorized changes to the production configuration or operation is an unacceptable action. Control systems frequently have stringent uptime requirements, where availability of the system has the highest priority. This emphasis on availability mandates that any changes, patches, or upgrades to the control system must be extensively tested and documented for reliability and functionality before being deployed.

For substation automation, cyber security focuses on preventing unauthorized access/control of the cyber components related to the substations.

Unauthorized cyber intrusion may occur through various means such as:

- Substation communication access points including modems, Voice over Internet Protocol (VoIP), radio, microwave, wireless, Ethernet
- Clear-text communication protocols
- Third-party maintenance access/accounts
- Unauthorized or untested component patches that cause unintended application failure or include undetected malware, which can either allow unauthorized access or consumes all available industrial control system cyber resources causing a denial of service.

The NESA 2008 study asked respondents specific questions about implementation of cyber security of substation automation. Specifically, one question asked was if encryption was used on any protocol used for communication between a substation and external host, as shown in Figure 2. The majority of respondents do not use encryption. Use of encryption may not be necessary depending on the risk exposure, system configuration, and other cyber security methods implemented.

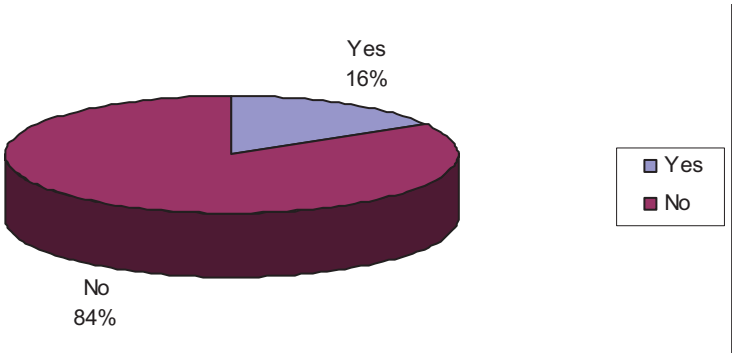



Figure 2. Encryption of protocols used for communications between substation and external host.

Remote connections to substations allow for SCADA monitoring and control, engineering and maintenance, vendor support, and data gathering. Securing these connections is an integral part of cyber security. A question was asked in the NESA 2008 survey if these connections were secured and if some type of authentication was required before remote access was granted. The majority of respondents indicated that these remote connections are secure. Secure connections are defined as authentication required before access is granted. Results are summarized in Figure 3.

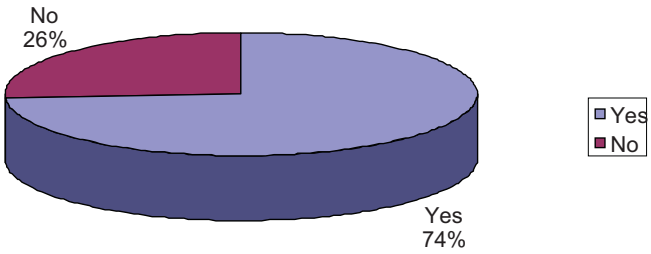



Figure 3. Security of remote connections (such as modems, wireless, IP).

Password management is required per Critical Infrastructure Protection (CIP) standards for applicable entities. A question was asked in the NESA 2008 survey if respondents had a password management system in place for remotely accessible IEDs. The majority of the respondents had password management systems in place as shown in Figure 4.

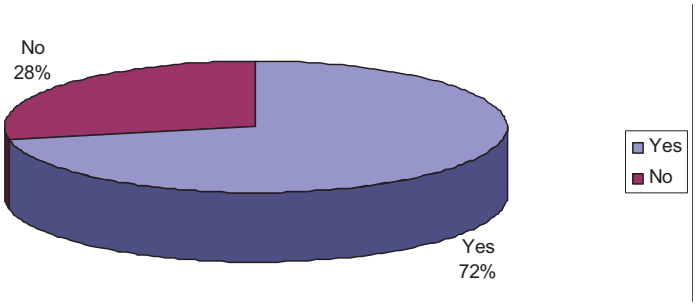



Figure 4. Extent of use of password management system for remotely accessible IEDs.

## 2.2 Physical Security

Physical security is required to maintain safe and reliable operation of substation equipment. Control structures and systems need security measures such as fences, locked gates, locked doors, video, and motion detection to ensure unauthorized entry does not occur and to monitor all entries. Motivation ranges from simple theft of equipment and materials (copper and aluminum assets, tools, and computers) to the intent to impair or destroy the ability to deliver electrical power. A more subtle issue is physical access to the automated control system network at a remote substation and injecting software that allows future unauthenticated remote access. The level of protection of physical assets is generally commensurate with potential damage and recovery of the asset.

A credible scenario where physical security and cyber security tie together is where a physical break into an electrical substation results in an unauthorized Ethernet connection to a port on a substation Ethernet switch. The aforementioned scenario is an application where port security provides mitigations against unauthorized cyber access to a substation network. According to the NESA 2008 survey, the majority of the respondents use port security on their Ethernet ports, as shown in Figure 5.

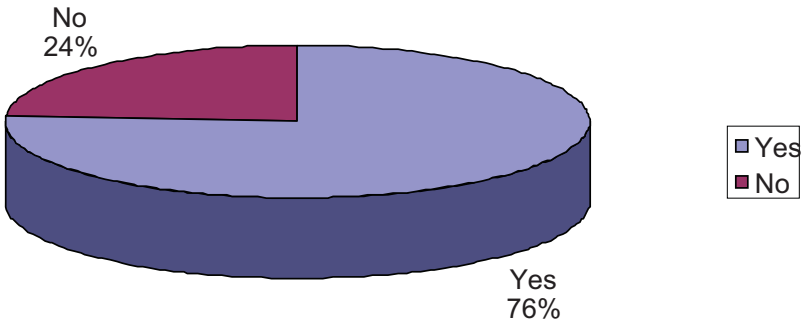



Figure 5. Ethernet port security implementation for IP communications to substations.

# 3. CYBER VULNERABILITIES OF SUBSTATIONS AND RECOMMENDATIONS

## 3.1 Substation Vulnerabilities

It is important to characterize the inherent vulnerability that is a part of substation automation. These characteristics are intended to be used for their own evaluation of cyber security implementation to determine their risk or threat to their system. For example, if the end user determines that the effort to exploit a vulnerability is significantly high, they may feel that the identified vulnerability may not be as high of a priority to address than others that are identified.

The following are four characteristics of a cyber attack against a substation:

- Access to the system or substation
- Intruder level of skill or knowledge
- Intruder level of system knowledge of substation automation
- Effort involved to exploit a specified vulnerability.

Each one of these factors must be evaluated by the organization implementing security to determine if the implemented security specific for their application meets a minimum level of security as well as best practices. This minimum level may be from industry standards, recommended practices, or company-specific policies and procedures.

Substation security is a growing issue within utility companies. In order to compromise substation security, an adversary must have at least some of the following information for a successful cyber attack on a particular substation.

- Access to company communications
- Know the communication parameters (i.e., local area network [LAN], wide area network, public switched telephone network [PSTN])
- Knowledge of proper passwords/secure ID
- Knowledge of vulnerabilities that can be exploited to gain unauthorized privilege
- Knowledge of relay software
- Knowledge of substation remote terminal units (RTUs) and IEDs
- Knowledge of routable and non-routable communications
- Knowledge of applicable protocols
- Knowledge of controlled process configuration.

### 3.1.1 Substation Automation Security Vulnerabilities

The following vulnerabilities were either observed directly or were obtained anecdotally. The description of each vulnerability includes how it may be exploited thus contributing to a compromised system. This list of vulnerabilities is not intended to be a complete set of all known vulnerabilities.

#### 3.1.1.1 Default Passwords Remained in Substation IEDs

Substation IEDs provide a large part of substation automation. If unauthorized access to either a network connected IED, modem connected IED, or physical access is obtained, then the unauthorized user can gain full control of the device. Full control may consist of any or all of the following: reconfiguring the device, planting malicious code within the device, and using the IED to operate a substation device resulting in loss of electrical power or damage to equipment or grid instability. Default passwords are easy for attackers to obtain and should never be used in field operations.

#### 3.1.1.2 Substation Communication Rides on same Backbone as Internet Traffic Separated by a Virtual Local Area Network

If unauthorized access is obtained via the Internet to utilities corporate or business network, then the substation LAN can also be accessed by an attacker. This results in cyber exposure to not only substation automation devices, but also the control system. Once an attacker gains control of substation automation components, then consequences described in Section 7 are a possibility.

#### 3.1.1.3 Substation Relays Accessible via Public Switched Telephone Network

If substation relays are accessible to the public switched telephone network (PSTN), then these relays can potentially be compromised. The consequences of such a compromise are similar to those described in Sections 6.1.1 and 7.

#### 3.1.1.4 SCADA LAN is not Separated from the Corporate LAN.

The corporate LAN has more exposure to the Internet than the SCADA LAN. This exposure provides a potential path for multi-stage cyber attack on the SCADA LAN. Providing an additional separation of the SCADA LAN from the Internet adds to the "defense in depth" security posture.

#### 3.1.1.5 No Firewall between SCADA LAN and Corporate LAN

See Section 6.1.1.4.

#### 3.1.1.6 SCADA Network Information Found on the Internet

If SCADA network information is publically available, then unauthorized access is that much easier to obtain. Once unauthorized access is established to a corporate or SCADA LAN, see Section 6.1.1.2

#### 3.1.1.7 Substation Communications use Clear-text Protocols (i.e., DNP3)

Communications that use clear-text protocols can be monitored using network "sniffers." Sniffers are able to obtain passwords and view the communications strings in order to perform reverse engineering of the substation automation communications. Successful reverse engineering of substation communications can allow an unauthorized user to take control over substation automation devices as described in Section 6.1.1.1.

#### 3.1.1.8 Substation Communications use Local Service Providers' Telecom System

Use of the PSTN does not inherently provide any cyber security or protection of information. Communications that use the PSTN are potentially subjected to network monitoring and may be subjected to unauthorized exploit of the communication channel.

#### *3.1.1.9 Use of Unencrypted Wireless Communications from Control Center to Substation LAN*

See Section 6.1.1.7.

#### *3.1.1.10 No use of Door Alarms on the Control House Portion of the Substation*

Use of door alarms provides an additional layer of physical security to electrical substations. Without this layer of security, local access to substation automation devices becomes easier to accomplish without being detected.

#### *3.1.1.11 Use of Dual-ported RTUs and IEDs*

Dual-ported devices have the potential for one network access point to be a vulnerability to the other network access point. A successful cyber attack on this device has the potential for one network to be available to the other network that is connected to this device.

#### *3.1.1.12 Remote Engineering Access to IEDs via IP Network*

Unauthorized access to the network that has engineering access to IEDs allows exposure of the IEDs to be compromised, see Section 6.1.1.

#### *3.1.1.13 Government-required Application Information about Electrical Systems Found on the Internet*

Some government applications require specific electrical information as part of the application. After review and approval of these applications, the results are posted on the Internet, including some of the electric utility information. Evaluation of the electrical utility information end usage should be considered as a part of the application process.

## 3.2 Cyber Vulnerabilities

A discussion of substation vulnerabilities and potential consequences follows. These vulnerabilities are not new; however, their importance is significant and consequences can be great. Specific application to substations and substation automation equipment provides a distinctive analysis of them.

### 3.2.1 Vulnerability: Physical Access

Physical access vulnerability allows unauthorized physical access to substation critical assets. This includes physical access to SCADA field devices that can be physically controlled or damaged, and data transfer paths of the SCADA system such as unrestricted access to the Universal Serial Bus (USB), switch, and other ports. Examples are devices located outside the protected area and any other path that allows unrestricted physical access to critical assets. Based on INL researchers' field observations and some anecdotal information, nearly all entities had physical locks on both the gates at substations and control houses. Not all entities had door alarms, motion sensors, or remote monitoring cameras. A continuing problem that entities are experiencing with physical locks is that other organizations or subcontractors may have keys to the gate or control house. Some companies are moving toward use of key card access or some way of logging (such as biometrics) who enters or exits the substation yard and control house.

A well-accepted rule of computer security is that once an attacker has acquired physical access to a machine, it is generally trivial for that attacker to fully compromise the system. As technology improves, this is becoming less of an issue, but for now, if an attacker has physical access to a machine, the attacker can generally breach its security

#### 3.2.1.1 Vulnerability: Physical Access to Network Equipment

Unauthorized network access through physical access to network equipment includes the lack of physical access control to the equipment. It also includes the lack of security configurations functions that limit functionality even if physical access is obtained. A common finding is a lack of port security on network equipment. A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall.

**Recommendation.** Port security should be implemented to limit connectivity to hardware interfaces. Given the static nature of SCADA environments, port security can be used to ensure Media Access Control (MAC) addresses do not change and new devices are not introduced to the network. Actions, such as limiting known MAC addresses to specific interfaces and disabling unused interfaces, should be implemented to assist in network security.

#### 3.2.1.2 Mitigations for Physical Access Category

Protect all critical cyber assets by isolating them in secured areas inside the physical security perimeter as described in CIP-006, "Physical Security of Critical Cyber Assets."

Physical access to an asset generally implies compromise. A user can take a number of steps to mitigate the risk of attacks via physical access. The first and most important of these is to not allow physical access to a system by untrustworthy people. Additional security measures should also be taken that restrict access and damage potential once physical access is obtained (i.e., network port security and strong authentication).

### 3.2.2 Vulnerability: Clear Text Protocols (DNP 3.0)

Based on the NESA 2008 study,[1] more than half of surveyed utilities were using Distributed Network Protocol (DNP) 3.0 LAN, while 54% were using DNP 3.0 serial. This demonstrates the importance of implementing secure communications with the use of DNP 3.0.

DNP 3.0 traffic is a clear-text protocol and is sent unencrypted and is, therefore, vulnerable to reverse engineering and Man-in-the-Middle (MitM) attacks. The vulnerability is diagrammed in Figure 6.

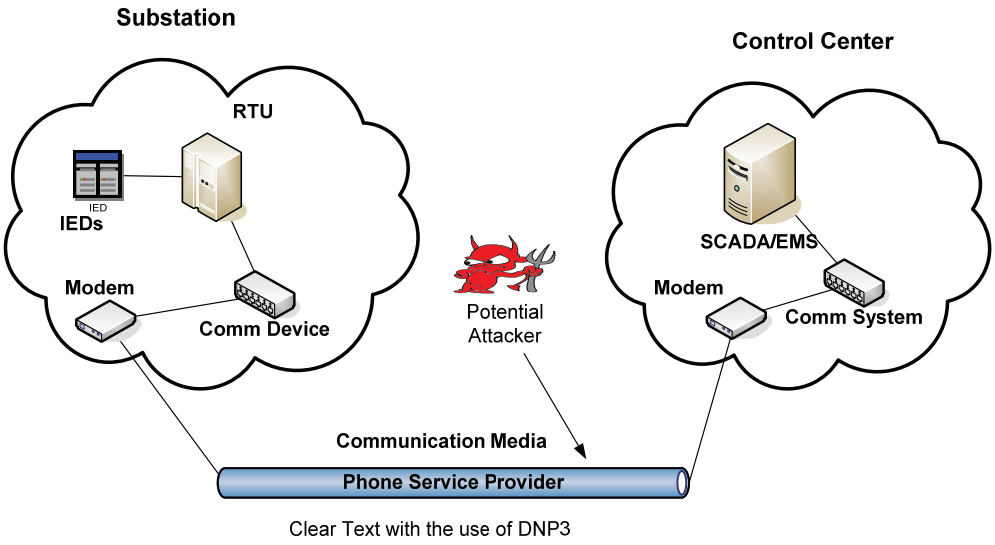



Figure 6. Vulnerability of clear-text communications public switch telephone network.

INL has written a DNP 3.0 decoder module to extract data values associated with point numbers/types for DNP 3.0 traffic on previous systems that INL has analyzed. These values were kept in a local data store available for future use as a replayable source of historically correct data, or altered and reused as an attacker might require. The availability of accurate historical data can make it possible for an attacker to provide misleading data while an attack is conducted, keeping system operators from knowing the true state of the process.

INL cyber researchers have successfully performed MitM attack on a DNP3 protocol. However, INL cyber researchers have demonstrated it would be easier to target the end device, such as a modem or RTU, via cyber methods or social engineering methods for exploitation. See Figure 7 for a diagram illustrating this vulnerability.

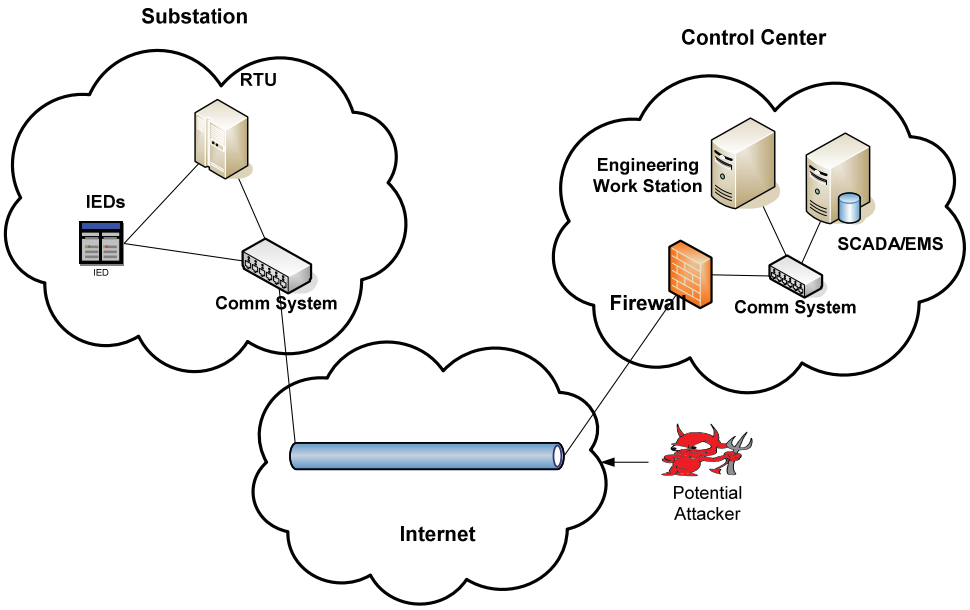



Figure 7. Vulnerability of communications via the Internet.

**Recommendations**. System designers can make it more difficult to attack a system employing DNP3 by requiring implementation of some type of authentication. Another potential method to configure the field equipment is to only allow connections from the IP addresses of the systems that are expected to connect to those devices by adding a firewall at the substation. In addition, use of encryption or secure DNP3 if possible.

### 3.2.3 Vulnerability: IED Accessibility/Use of Routable Paths to End Devices

According to the NESA 2008 study,[1] 59% of the respondents use routable paths to end devices. Some of these end devices are most likely relays. If not an individual relay, some type of communication hub that allows access to multiple relays is used.

One previously identified vulnerability relating to programmable relays or digital control protective devices (DPCDs) is a power outage. In this case, remote control of the DPCD is performed.

Remote control of the end device allows the adversary to perform any number of consequences (see Section 7).

Mitigation can be performed at many levels. These include having only local access to the device for engineering and maintenance or having a secure connection to the device.

The NESA 2008 study [1] also shows dial up access is the number one communication link for remote engineering access. Approximately 40% of the respondents mention this type of communication link for remote engineering access.

Mitigation for this vulnerability includes use of dial back modems, encryption, modems that allow only designated number for access, and passwords as part of the access to the modem. See Figure 8 for accessibility to substation devices via a modem.

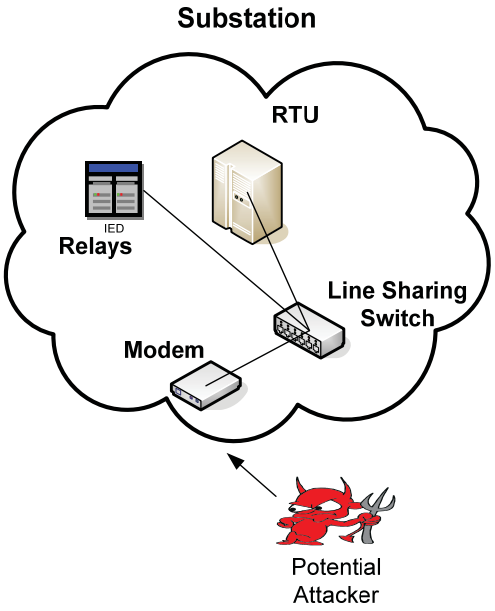



Figure 8. Accessibility to substation devices via a modem.

### 3.2.4 Vulnerability: Separate Protection and Control

According to the NESA 2008 study,[1] 55% of the respondents use separate protection and control devices for transmission application, as shown in Figure 9. Investor-owned utilities reported the highest percentage of separate protection and control. This was partially because investor-owned utilities generally handle more transmission level of protection and control.

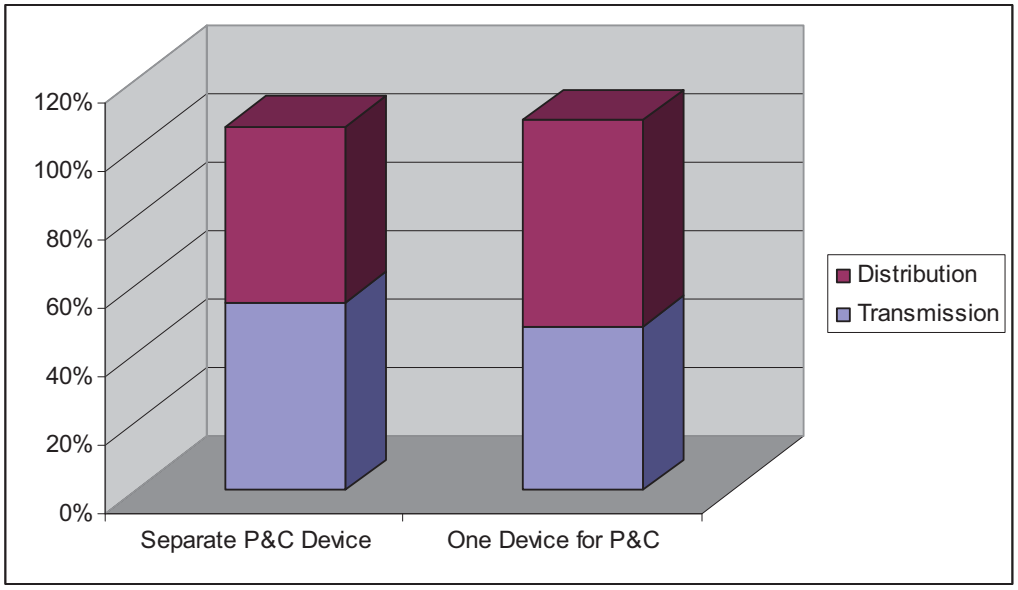



Figure 9. Current use of separate protection and control (P&C) devices used for monitoring and control of substation equipment.

The issue with respect to separate protection and control is a function of reliability versus functionality versus vulnerability. Having one unit for both P&C provides more functionality; however, if the device is compromised, then the DPCD is more vulnerable to specific cyber attacks.

Mitigation can be performed at many levels. These include only having local access to the device for engineering and maintenance, having a secure connection to these devices for remote access, and a secure SCADA connection for monitoring and control.

### 3.2.5 Vulnerability: Open Source Information Available

Availability of open source information concerning the software, devices, topology, configuration, and purpose of a control system may be the first criteria in an attacker's identification and selection of a target. To a degree, the accessibility of the information is not strictly in the control of individual owners or vendors. However, it is possible to establish a process to baseline the information that has been made publicly available on the product and then track and respond to the increase or decrease of the available information over time.

After a tour of an entity's substation, INL researchers performed an Internet search of the utility communication system hardware vendor. A network diagram with IP addresses was found on a web site detailing specific information about the setup. This was forwarded to the utility for removal from this open source.

Utility providers must maintain a delicate balancing act in order to keep company proprietary-specific information about substation automation secure such that adversaries find it difficult or impossible to obtain while available enough for employees to be able to effectively work and maintain the SCADA/EMS and substation automation systems.

Mitigation can be performed by ensuring that the entity's Internet information, as well as related web sites (i.e., vendors or integrators web sites), do not have specific information about the SCADA/EMS control system and related substation automation equipment. In addition, information should only be released to authorized requests.

### 3.2.6 Vulnerability: Dual-Ported RTU Vulnerability

A vulnerability that could have an impact on SCADA systems, and consequently the power grid, involves dual-ported RTUs, which allow two utilities to have communication with the same RTU. Dual-ported RTUs are common in areas where coupling exists between larger and smaller utilities. The RTU sharing is a cost convenience in that it eliminates independent RTUs.

Anecdotally, the communication system of one utility could be used as an attack vector to access the RTU, or the RTU could be accessed directly by plugging into the communications. Once in the RTU, the pathway to the other utility could be used to access the other utilities EMS/SCADA system.

The main method to prevent this is not to use dual-ported RTUs. None of the substations that INL visited used dual-ported RTUs.

One possible method of mitigation is for utilities to adhere to appropriate standards to reduce the chances of this vulnerability occurring.

A second possible method of mitigating this DNP3 vulnerability is to install physical security for the RTU to prevent access to the communications links. This could include guns, guards, and gates, or some form of vault that protects not only the RTU, but the hardwire communications connections.

A third possible method of mitigating this vulnerability is to use encryption or authentication between the RTU and EMS/SCADA that is performed inside the RTU at the RTU end, and an equivalent process at the EMS/SCADA (typically at the control center).

# 4. POTENTIAL CONSEQUENCES OF EXPLOITATION OF VULNERABILITIES

## 4.1 Power Outage

A power outage may be executed via the SCADA or access to the protective relay. A power outage is merely the unwanted opening of an electrical device resulting in a loss of electrical power for a targeted area. For purposes of this report, a power outage is described as being executed via the protective relay.

Protective relays include a multitude of serial ports. These serial ports simultaneously service SCADA demands (metering and control) and provide engineering access (sequence and disturbance data retrieval, setting, status, metering, etc.). Once an attacker has gained access to the setting level of the protective relay, they have full control of the device and can therefore open the electrical device with the relay and force a power outage for a targeted area.

A cyber attack via the engineering access path on a non-routable protocol requires that the attacker compromise three devices at the substation to enter the engineering access port of the targeted protective relay. These devices are the dial-up modem, telephone line-sharing switch, and the protective relay. Once compromised, the attacker has the access necessary to carry out a very effective attack. A cyber attack via a routable protocol (IP/Internet) requires compromising a firewall, a network switch, and the protective relay. In either case, a malicious power outage is a distinct possibility.

A phone line-sharing switch has multiple ports on its rear panel for connecting various devices. The purpose of the phone line-sharing switch is to share one telephone line for voice, fax, and data duties. A portion of these devices are believed to be in service in their default configuration.

Protective relays include serial ports for user programming and other interrogation functions. These relays are frequently found connected to a modem and can be remotely reconfigured using a terminal session over the dial-up connection. These relays typically require two levels of authentication to access the privileged level where the relay can be programmed. The initial authentication level gives the user the ability to retrieve cursory information, but not the ability to reconfigure the relay. The second authentication level gives the user the ability to reprogram the relay. Most of these relays are shipped with default passwords for each level of authentication. These relays are frequently found in the field with the default passwords still enabled.

Mitigation for successive password attempts include simple security measures to prevent brute force password discovery by closing the connection and timing the user out for a period following three successive authentication failures.

## 4.2 Grid Instability

Grid Instability is fluctuations in voltage and frequency, which may result in a power outage. Grid instability may be caused by many factors. These include but are not limited to:

- Generation oscillation
- Heavy load oscillation
- Power factor or Volt Amp Reactive (VAR) correction errors
- Frequency oscillation
- Under-loaded or over-loaded system
- Large faults.

Some of these can be initiated by an adversary via a compromised substation automation device.

Another example of grid instability may be initiated by compromising the reactive/VAR control devices. Without reactive/VAR control on an electrical distribution system, voltage collapse may occur resulting in loss of electrical power.

Mitigation is similar to Section 3.2.3 (i.e., security of the substation automation devices that control the aforementioned factors causing instability).

## 4.3 Loss of SCADA Control

Substation automation is highly dependent on software running on communication devices. These devices all allow communication between the control center and the substation. In typical communication systems, the communication channel is monitored for health status. The loss of the communication channel will alarm on the control centers SCADA/EMS after a set period of time.

Loss of SCADA control may be the result of interrupting the communication channel that links the control center to the substation. Interrupting the communication channel will cause loss of SCADA control for a specific substation.

Interruption of the communication channel may also be the result of a physical break in the communication link or via a cyber intrusion. If a utility loses SCADA control, then the utility will have to dispatch electrical linemen for manual operation of substation circuit breakers when events dictate such operation. This potentially results in longer outage times.

The communications link from the substation to the control center should be monitored and an alarm set if a heartbeat or other communications parameter is set indicating a loss in communications beyond a reasonable period.

## 4.4 Loss of SCADA Related Information

Some types of substation automation devices perform monitoring and storing of substation-related information. If these devices are compromised such that important information is no longer retrievable or lost, then this may impact company operations. Impact may be seen to varying degrees depending on amount of backup systems in place and the relative importance of the information. A few specific examples of information that may be lost when automation devices are compromised are metering information, sequence of events information, and some types of fault recordings.

# 5. SUBSTATION AUTOMATION TECHNOLOGIES

For the purposes of this report, the INL has defined substation automation to provide a clear understanding of the state of the industry. In conducting the research associated with this subject matter, INL found that different entities have different interpretations of substation automation. Substation automation has many facets associated with it. Substation automation not only includes the hardware that provides the vehicle for information exchange of end devices, but also the associated software and communication to these end devices. For example, substation automation software can be configured for automatic response or manual response to electrical events on the power grid. Electrical events include fluctuations in voltage, frequency, and power. In addition, integrating communications to substation automation devices provides more functionality, but is inherently more vulnerable to attack.

Substation automation is the function and process of using the necessary hardware and software to provide information exchange and potential control between end devices (i.e., IEDs) and another smart device (i.e., a server, RTU, or communication processor) by various communication methods and media. The information collection point and control hub may ultimately be at a control center where the SCADA/EMS is located. In some instances, the information collection point and control hub is located at the substation. This is the highest level of substation automation.

## 5.1 Categorizing Phases of Substation Automation

The degree to which substation automation (SA) is implemented can be measured by a graded approach. The amount varies greatly between different types of entities as well as substations owned and operated by the same entity. The degree in which substation automation is implemented can be summarized as:

- The number of installed microprocessor-based IEDs, RTUs, etc.
- The software and hardware configuration of the IEDs, RTUs, etc.
- Software automation programs running at the substation level
- The amount of integration via communications of the IEDs, RTUs, etc.
- The amount of provisions for remote communications to the substation and to these end devices.

One of the key questions regarding substations is just how automated are they, and assuming they are automated, what is the risk that these automation systems can be exploited to cause damage or widespread power outages? The NESA 2008 survey provides good insight into helping to answer this question. The survey defines four stages of automation with respect to IEDs. These automation stages are defined in Table 1. Stages of substation automation.

Table 1. Stages of substation automation.

| Stages of Substation Automation | |
|---|---|
| Stage 0 | No automation technologies installed. |
| Stage 1 | Most equipment manually operated through local switching. Some programmable IED implemented, but no communications with central control room other than some monitoring. |
| Stage 2 | Some electromechanical devices remain. Installed IEDs are integrated, using two-way serial communications capability and no substation LAN, allowing monitoring and control from the central control room. |
| Stage 3 | Some electromechanical devices remain. Installed IEDs are integrated, using two-way serial and/or LAN communications allowing monitoring and control from the central control room. |
| Stage 4 | Installed IEDs are integrated, using LAN communications. Applications are run at the substation level to automate various substation functions with full control from the central control room. |

### 5.1.1 Stage 1 Automation

Substation Automation Stage 1 is illustrated in Figure 10. In Stage 1, IEDs have been deployed, but they are not integrated at the substation. There may be a possible communication link to an RTU for control of substation devices, but no other IED integrated to RTU.

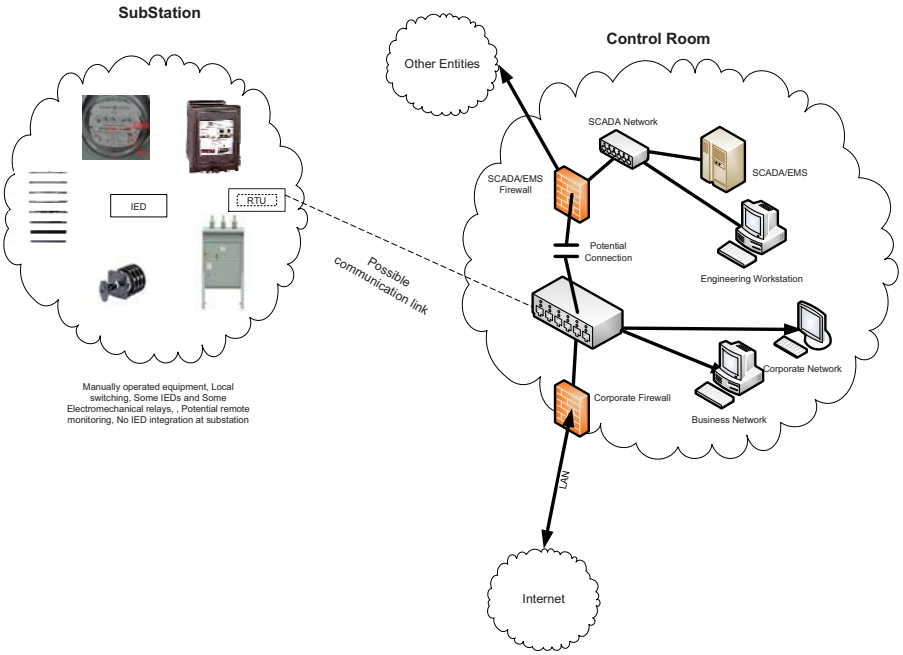



Figure 10. Stage 1 substation automation.

### 5.1.2 Stage 2 Automation

Substation automation Stage 2 is illustrated in Figure 11. In Stage 2, IEDs have been deployed and integrated, allowing monitoring and control of the substation from the central control room. Full two-way communication exists on serial connections, possibly with two-way radio, microwave, or line-of-sight communication. Relay integration is defined by connecting the relays though the use of a communication cable to a centralized processor or gateway.

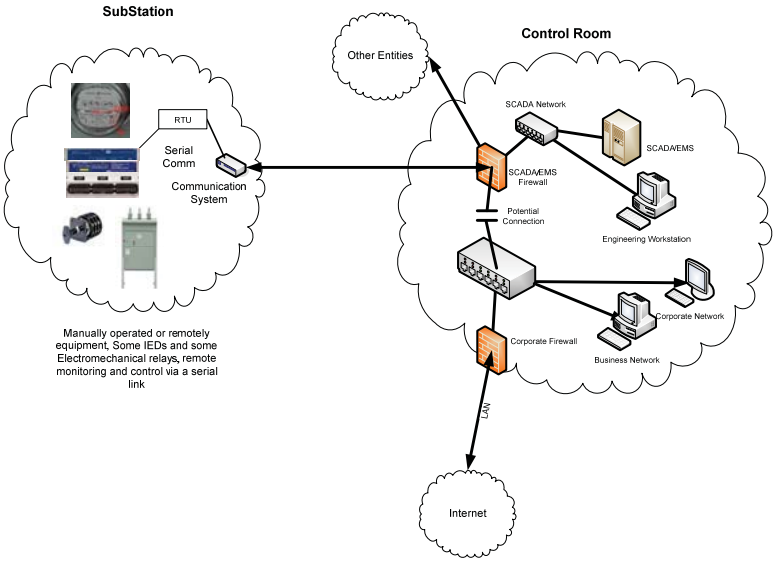



Figure 11. Stage 2 substation automation.

### 5.1.3 Stage 3 Automation

Substation automation Stage 3 is illustrated in Figure 12. In Stage 3, IEDs have been deployed and integrated, allowing monitoring and control at the substation from the central control room. Full two-way communication exists on serial connections and/or LAN using TCP/IP.

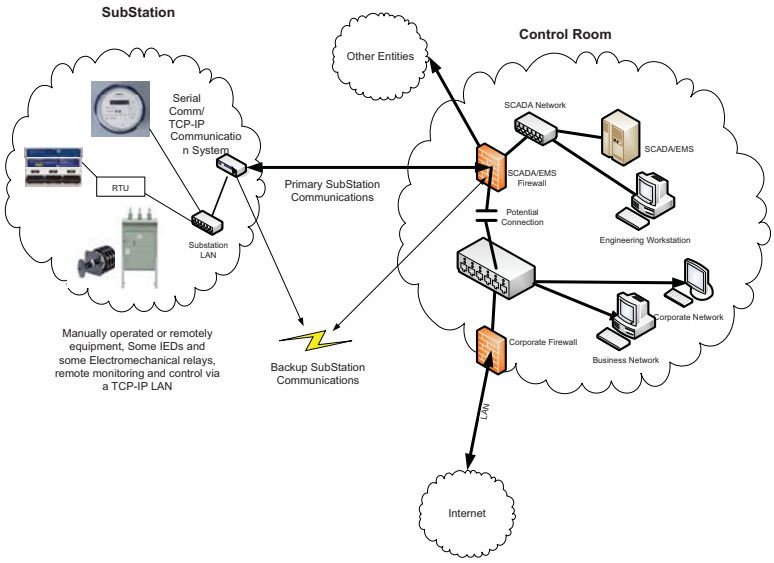



Figure 12. Stage 3 substation automation.

### 5.1.4 Stage 4 Automation

Substation automation Stage 4 is illustrated in Figure 13. In Stage 4, IEDs have been deployed and integrated, allowing full control of the IED at the substation from the central control room. Full two-way communication exists using TCP/IP protocol on LAN. Integrated firewalls are installed, and the SCADA system is separated from normal business IT traffic.

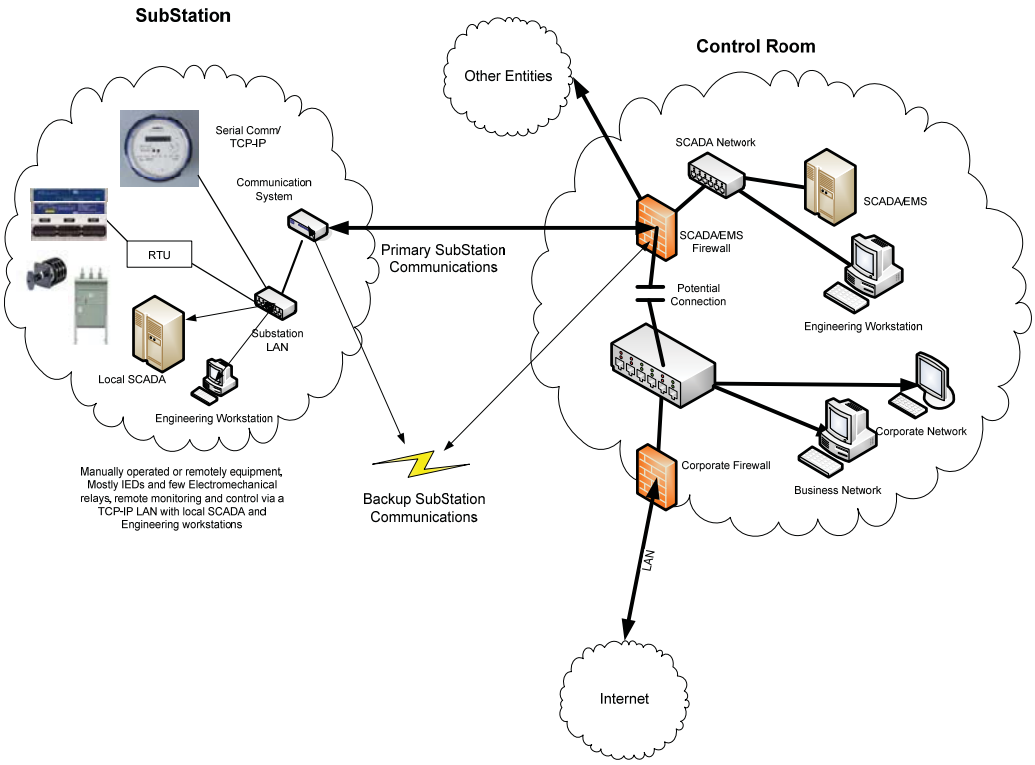


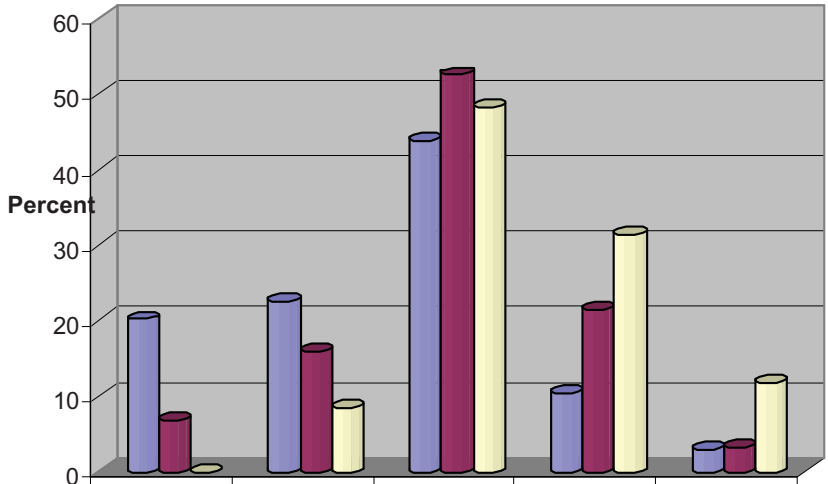

Figure 13. Stage 4 substation automation.

## 5.2 State of Substation Automation Overview

Respondents to the Newton-Evans substation automation survey were asked to categorize their substations into the defined automation stages. The results are shown in the next two sections. Because automation philosophies are often different between transmission and distribution substations, the results are broken down separately for each of these categories.

### 5.2.1 Transmission Substations

Approximately 17,325 transmission substations are in the U.S. and Canada. Of these, 4,594 (27%) are represented in the survey, which includes a cross section of investor-owned utilities, public power, municipals, and cooperatives. Of the 4,594 substations represented, 3,594 were categorized by the survey respondents. Figure 14 shows the results.




| | Stage 0 | Stage 1 | Stage 2 | Stage 3 | Stage 4 |
|---|---|---|---|---|---|
| Now In Operation | 20 | 23 | 44 | 10 | 3 |
| To Be Retrofitted | 7 | 16 | 53 | 22 | 3 |
| New to be Built | 0 | 8 | 48 | 31 | 12 |

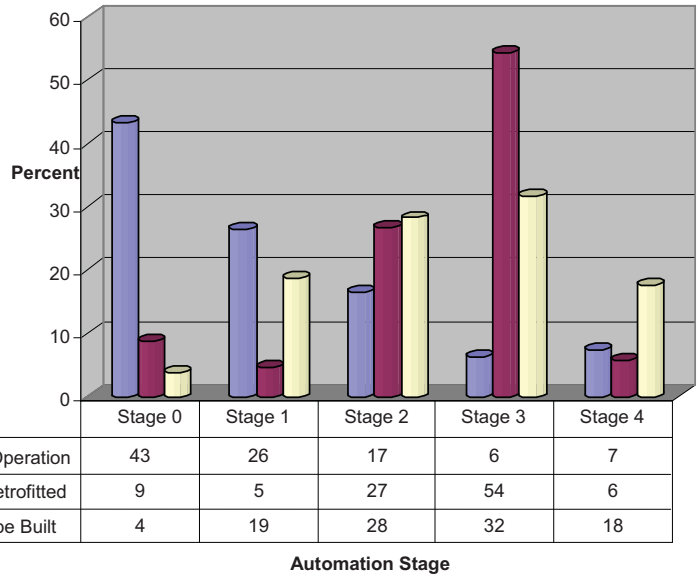
**Automation Stage**

Figure 14. Transmission substation automation levels.

As shown in Figure 14, most transmission substations fall into the Stage 2 category. This is true for both existing substations and those planned to be retrofitted or built new. Not surprisingly, new substations are more likely to be integrated at Stages 3 or 4 than existing or retrofit substations. Also, nearly 20% of existing substations have no automation at all, and another 20% have IEDs that are not integrated. In other words, from these results four in 10 substations currently have no communications paths to IEDs.

### 5.2.2 Distribution Substations

Distribution substations show more disparity between current and planned automation levels. According to Figure 15, more distribution substations have no automation than any other category. Retrofit and new substations are most likely to be integrated at Stage 3.




| | Stage 0 | Stage 1 | Stage 2 | Stage 3 | Stage 4 |
|---|---|---|---|---|---|
| Now In Operation | 43 | 26 | 17 | 6 | 7 |
| To Be Retrofitted | 9 | 5 | 27 | 54 | 6 |
| New to be Built | 4 | 19 | 28 | 32 | 18 |

Figure 15. Distribution substation automation levels.

### 5.2.3 Substation Automation Forecast

According to the NESA 2008 survey,[1] Figure 16is an estimate forecast for expenditures associated with substation automation. It is evident that substation automation implementation is increasing and older electromechanical devices are continually being replaced with microprocessor-based devices with varying levels of integration. Nearly all new distribution substations have planned substation automation with a minimum level of Stage 2 and some with the more popular Stage 3 level. Figure 16 shows that substantial funding is planned by utilities on substation automation and integration programs.

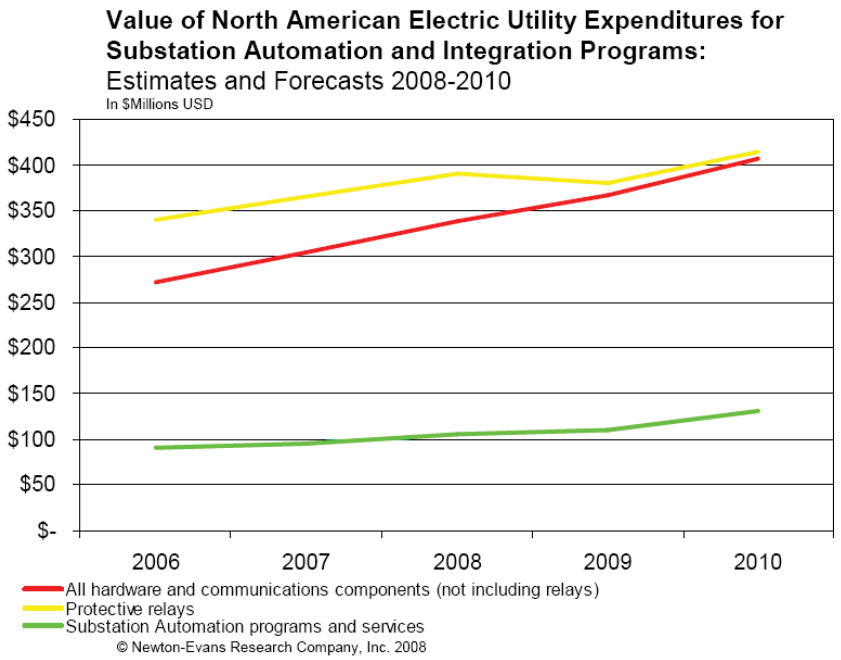



Figure 16. Substation automation expenditures for North America.

## 5.3 Substation Automation Technologies

Substation automation devices are typically electronic devices that measure, monitor, control, and protect the substation devices described in the previous section. This section describes:

- Major substation automation components
- Leading vendors in substation automation
- Communications equipment vendors for substation automation
- Communications media and technologies used in substation automation.

The graphs and charts in this section are important to gain an understanding of the most widely mentioned technologies and vendors used in substation automation.

In Section 5, substation automation levels are defined. These levels extensively use the term IED, which is a generic term referring to "smart" devices in the substation. These smart devices typically have a processor and some onboard storage and memory. They also typically have one or more communications ports designed to be connected to a "master" device, which polls the device for information and may also send control requests depending on the type of device and its application. Microprocessor-based relays, smart meters transformer/voltage regulator controllers, and digital fault recorders are examples of devices referred to as IEDs. RTUs usually are not included in this group, since they are usually the "master" that polls these devices.

Figure 17 shows devices most likely to be included in a substation automation system for transmission substations. Figure 18 shows the devices likely to be included in distribution substations. Between these two figures, there are some noteworthy differences. In transmission substations protection is the most commonly used device, while in distribution stations RTUs are the most common. Transformer monitoring is more common at the transmission substations. This is due in part to the high

cost and long replacement lead time associated with transformers as well as the potential impact of their failure.

Load tap changer (LTC) transformers are more important at the distribution level. At the distribution level, equipment protection is still important, but other issues including power quality and revenue metering become more important closer to the loads.

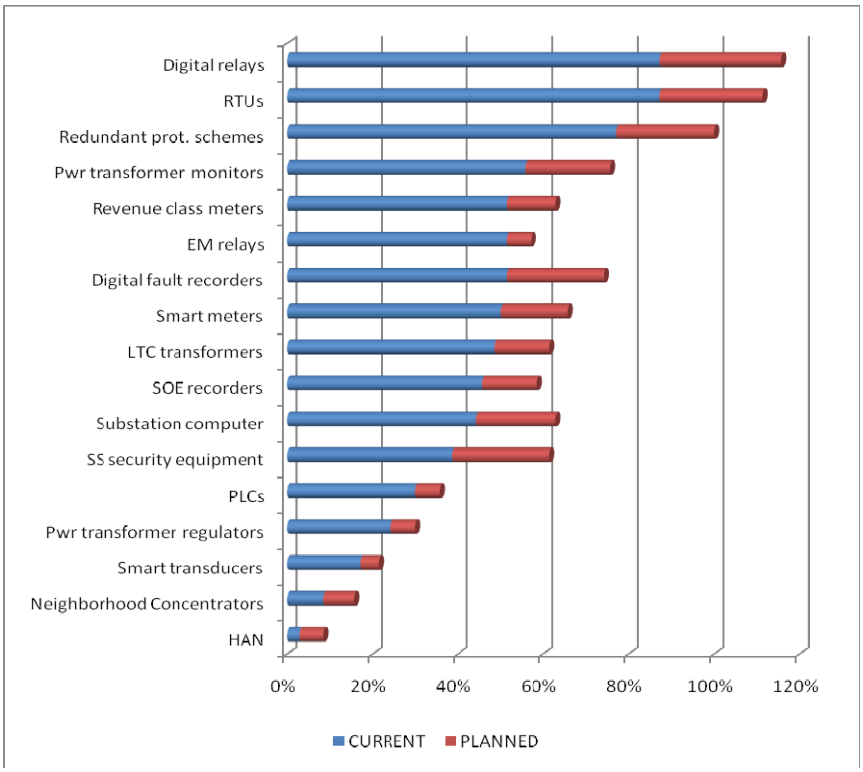



Figure 17. Substation automation devices deployed in transmission substations—current and planned.

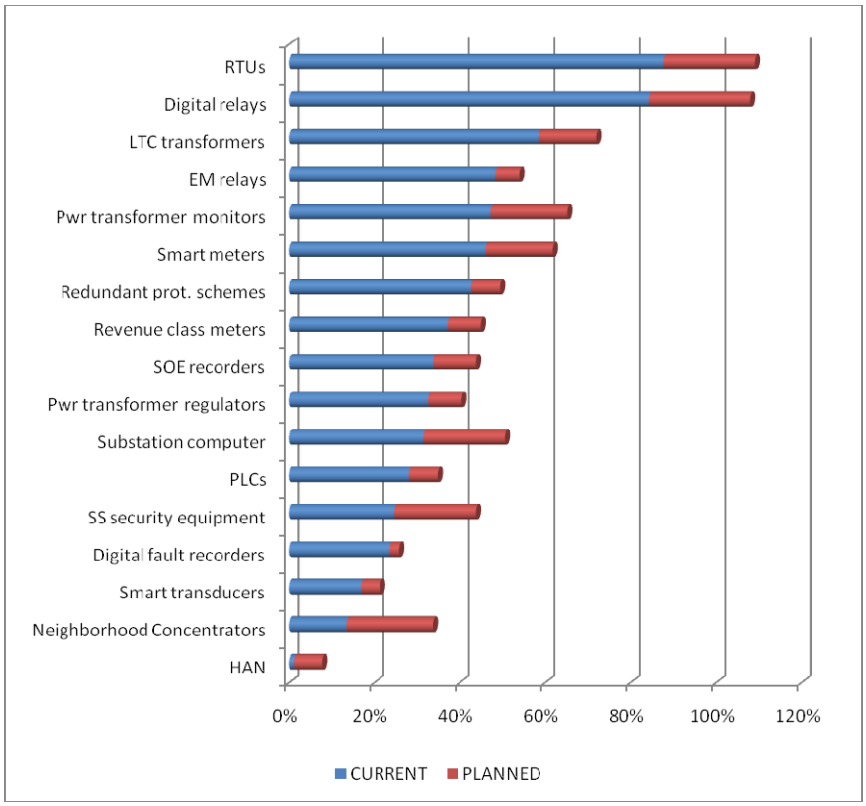



Figure 18. Substation automation devices deployed in distribution substations—current and planned.

From a cyber perspective, some of the devices are more important than others in terms of their potential to cause major consequences to the system. These devices are the ones that have control capability or have critical operational data. These devices include RTUs, programmable logic controllers (PLCs), microprocessor-based protective relays, voltage regulator controls, substation controllers/computers, and possibly smart meters.

Devices that have monitoring functionality only are less important from a cyber perspective. These devices include sequence of events recorders and transformer monitors. These devices do not have control features inherent in them; however, they still can be used to gain a foothold on a network in a multi-stage attack. One can assume that devices with no processor or communications capability (e.g., electro-mechanical relays) present no cyber risk.

### 5.3.1 Remote Terminal Units

Remote terminal units are programmable devices used to monitor the status of substation devices, gather basic metering data, and provide supervisory control capability from a remote SCADA or EMS. RTUs are often classified as either "dumb" or "smart." Dumb RTUs typically have basic digital and analog inputs and outputs and one or more communications ports to connect them to a SCADA front end. Because these earlier RTUs were often supplied by the same manufacturer as the SCADA system, many of them support only the proprietary protocol supplied by the manufacturer. They have very limited onboard processing capability or data storage.

Smart RTUs have additional communications and processing capability as compared to dumb RTUs. From a communications perspective, smart RTUs typically have multiple communications ports, often including Ethernet ports, and add the capability to act as a "master" to poll data from IEDs and forward it

to a SCADA/EMS system. To accomplish this, they support multiple protocols, including non-vendor specific "open" protocols like DNP 3.0 and Modbus that are used by multiple manufacturers. They also have additional processing capability, often including the ability to incorporate PLC-style program logic.

From the NESA 2008 survey, 87% of respondents indicated that RTUs are part of their automation strategy for transmission substations, 88% for distribution stations. Figure 19 shows the breakdown among manufacturers of RTUs by market share. As shown from the figure, General Electric (GE) is the market leader in this arena with Telvent and Advanced Control Systems somewhat distant competitors. The survey does not distinguish between smart and dumb RTUs in this case, but one can assume that the vast majority of new RTUs are smart RTUs. The market for dumb RTUs is restricted mainly to replacement parts or units for legacy systems.

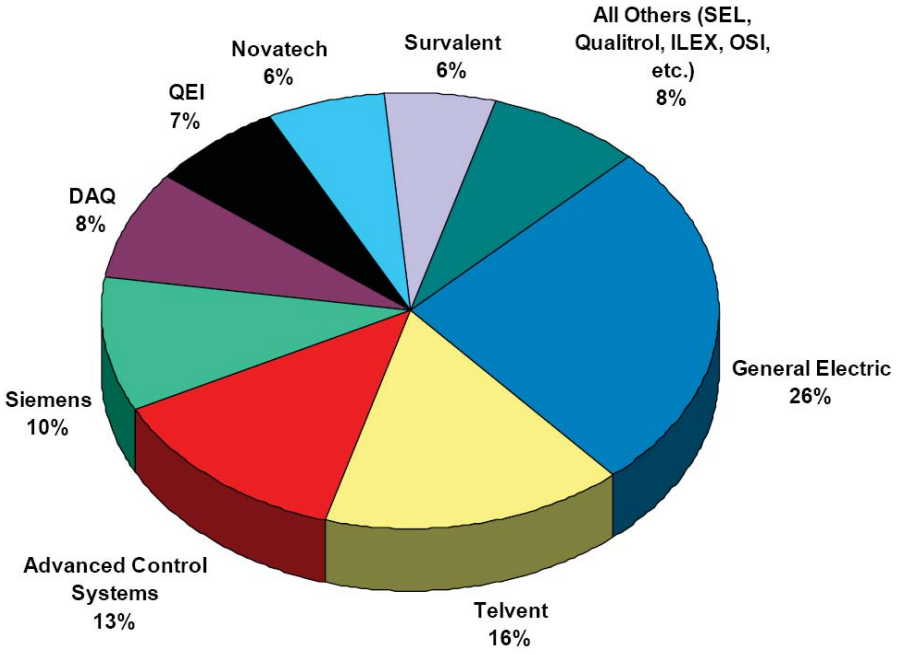



Figure 19. RTU manufacturers by market share.

### 5.3.2 Programmable Logic Controller

PLCs provide many of the same functions as smart RTUs; however, they are not nearly as popular as RTUs for substation automation. This is partly because most utilities have historically used RTUs, and because as a more generic platform, PLCs require more programming than a typical RTU to perform the same functions. Only 30% of respondents indicated they use PLCs in transmission substations, 28% for distribution substations. Modicon is the clear leader in this market, with almost half of the market share, as shown in Figure 20. Allen Bradley and Cutler Hammer make up most of the rest of this market.

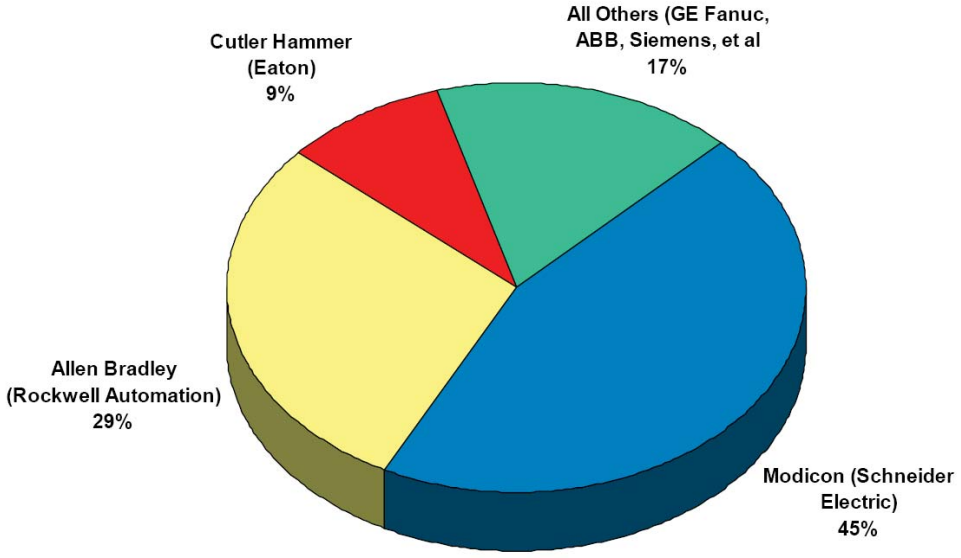



Figure 20. PLC manufacturers by market share.

### 5.3.3 Substation controller/gateway

The substation controller is a more recent development than either the PLC or RTU. Substation controllers typically have more focus on communications capability as opposed to analog input and output field signals. Many have up to 16 serial ports and one or more Ethernet ports to allow these devices to aggregate data from multiple IEDs and forward them to a SCADA/EMS system. Many also have the ability for an engineer to log in and access the IEDs directly as well. According to the NESA 2008 study, Novatech is the leader by market share in this arena, with GE close behind, as shown in Figure 21. Because Schweitzer Engineering Laboratory (SEL) and Subnet Solutions both use Subnet's software, Subnet/SEL could be considered the third-largest supplier in this market.

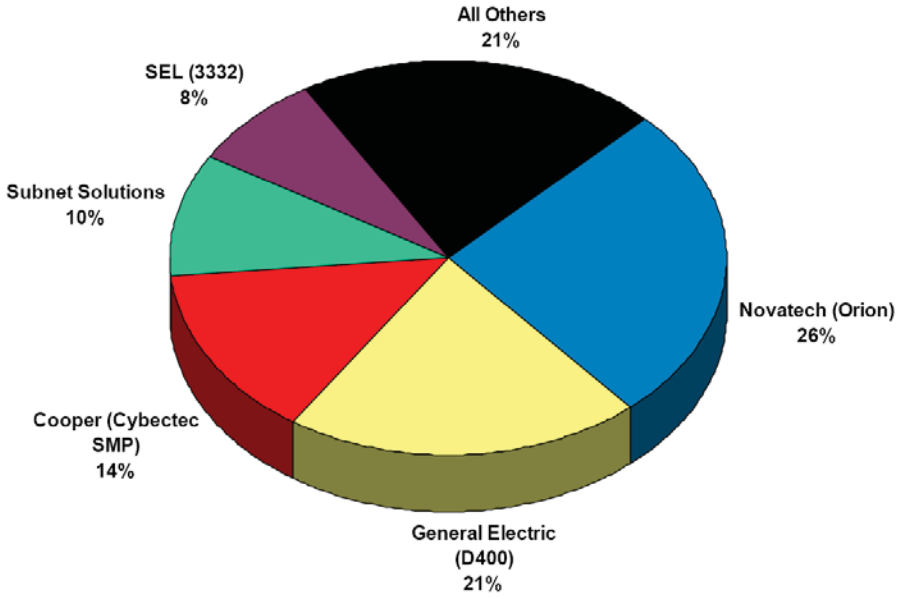



Figure 21. Manufacturers of substation controller/gateway by market share.

### 5.3.4 Protective Relay

Protective relays, as their name implies, are used to protect critical and expensive equipment including transformers, generators, substation buswork, and transmission and distribution lines. Relays use current and/or voltage inputs from the equipment being protected to sense off-normal, or fault conditions. The protective relay is typically used to detect conditions such as over-current, under-voltage, over-voltage, under-frequency, and over-frequency. In addition to the threshold alarm level, there is often a time delay as well, such that the more the measured value exceeds the alarm value, the faster the relay will signal a fault condition and trip its associated breaker.

Differential protection senses the difference between incoming current and outgoing current and assumes that if these are not approximately equal, then there is an internal short circuit fault and trips the protected equipment offline. Differential protection is used to protect high-value assets including transformers, generators, substation buswork, and sometimes transmission lines.

Distance protection is used almost exclusively for transmission lines and uses voltage and current to calculate the line's impedance (similar to resistance). If there is a fault condition on the line, the impedance changes, the relay senses this change, and signals breaker(s) to trip to protect the system.

Older, electromechanical relays typically require one relay per function per phase. Newer, microprocessor-based relays can typically perform multiple functions on all three phases in a three-phase system. In addition to their protective functions, microprocessor-based relays often have other functions that traditionally have been provided by separate devices, including metering, sequence of events recording, digital fault recording, and supervisory control. As a result, some of these older devices are being replaced by advanced protective relays.

In transmission applications, protective relays are often in redundant configurations. Two relays, often from different manufacturers, are connected in parallel with the same inputs. If either senses an off-normal condition, that relay will trip the proper circuit breaker(s). If they both sense the off-normal condition, both will try to trip the breaker(s).

For transmission line protection, communication between the relays on either end is often used to coordinate fault detection and selective tripping. If a relay on one end of the line senses a fault, it sends a signal to the other relay to trip its breaker, such that the line is completely isolated. Often the protection for overhead transmission and distribution lines includes high-speed reclosing, where the breaker closes again almost immediately after tripping. This is done to try to maintain continuity of power, using the assumption that whatever caused the fault has burned or fallen off the line and will not short-circuit the line again once the breaker closes. Relays are usually programmed with several iterations, or "shots," of reclosing, often with increasing time intervals between shots. If after several shots the fault does not clear, the relay de-energizes the line and locks out the control circuit to prevent line energizing until the fault is investigated, and the relay is reset.

Protective relays are the most common devices included in a substation automation system, according to the NESA 2008 study. For new installations, microprocessor-based relays have almost completely replaced electromechanical relays. This conclusion is based on INL's interactions with utilities. There is still a fairly large market for replacements for electromechanical relays; however, since many existing substations still use them. GE and Asea Brown Boveri (ABB) dominate this market. For microprocessor-based relays, SEL currently has the largest share of the market, with GE and ABB having the next largest shares as shown in Figure 22.

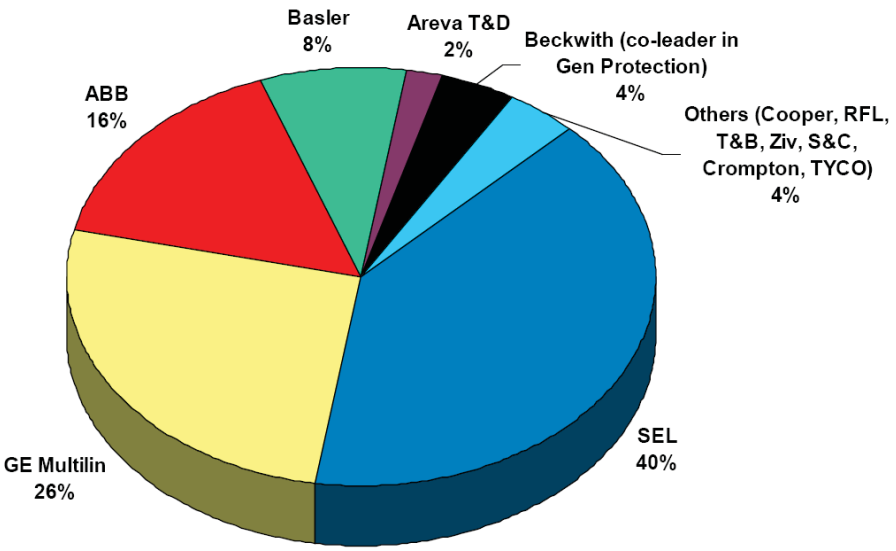



Figure 22. Protective relays manufacturers by market share.

### 5.3.5 Smart Meters

Smart meters are digital devices that collect and sometimes store data with respect to voltage, current, power, frequency as well as demand and energy usage. Revenue class meters are highly accurate versions of these meters that are used for billing purposes. It should be noted that smart meters are not typically categorized with automatic meter reading technologies.

Newer smart meters also may have power quality monitoring capability, allowing them to detect and record voltage sags or swells, momentary outages, undervoltages or overvoltages, line harmonics, transients, and other power system anomalies. It is expected that more control features will be implemented in the future smart meter designs to support load shedding schemes devised by the implementing utility. Figure 23 shows the breakdown of market share for the manufacturers of smart meters. Satec, an Israeli company and a relatively new player in this market, is the current leader.

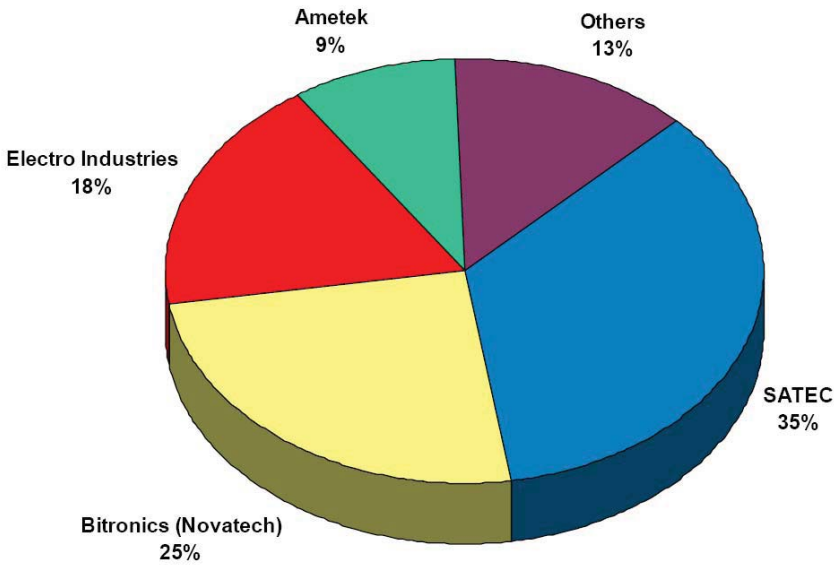



Figure 23. Smart meter manufacturers by market share.

## 5.4 Communications Paths

Communications links provide the potential pathways for an attacker to gain access to the end devices described in the previous sections. Figure 24 shows a sample of the types of paths one might expect to find in a typical substation.

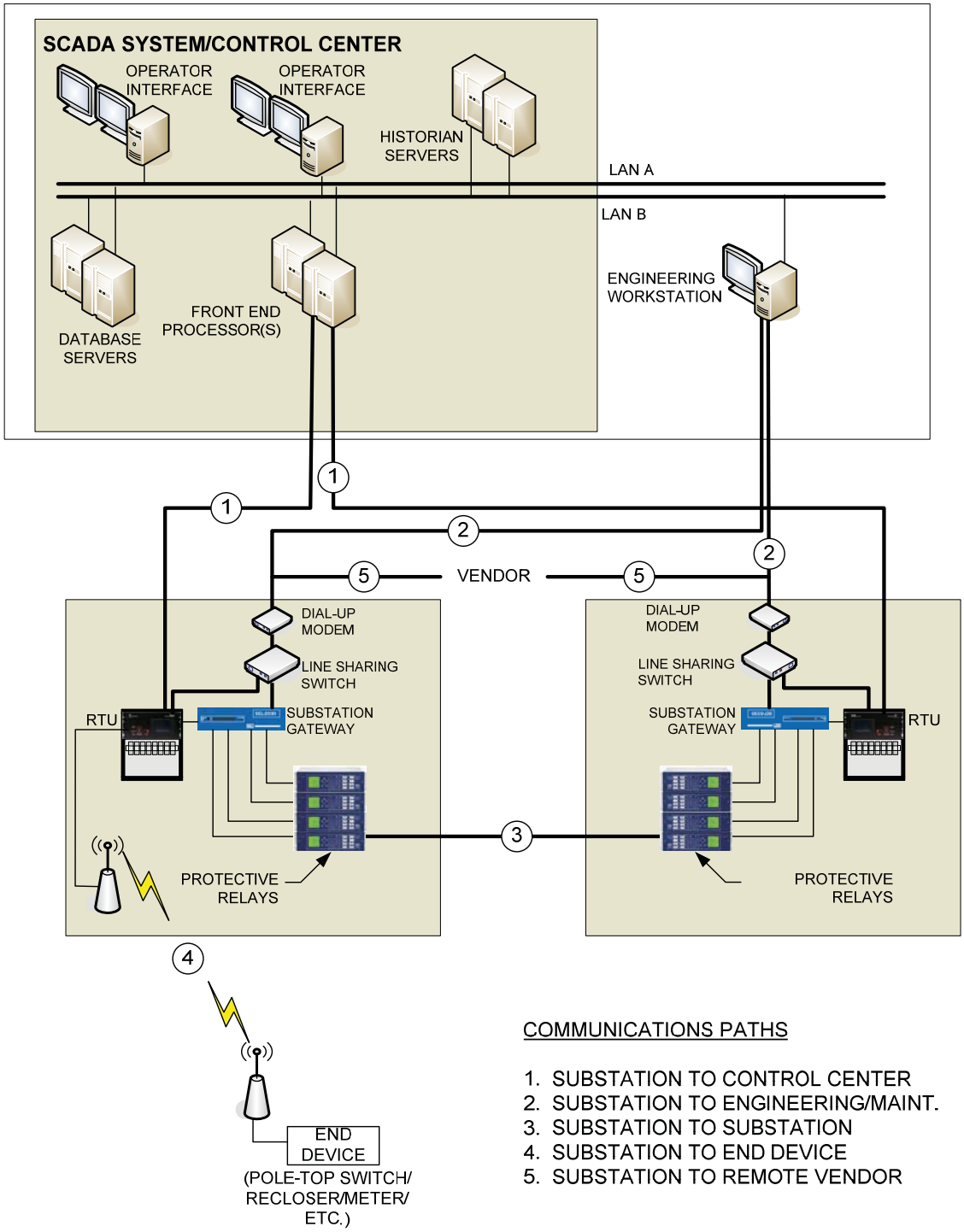



Figure 24. Example diagram highlighting substation communications paths.

### 5.4.1 Substation to Control Center

The communications link between the substation and the control center is most often used for SCADA. Nearly every respondent to the NESA 2008 report indicated some type of communications between the substation and control center, as shown in Figure 25. Of the responses, about half indicated that they use fiber for this link. Another 40% indicated that they use leased lines, and only slightly fewer use licensed radio links. One thing to note about these responses is that a typical utility may have more than one type of communications media in this path.

This result probably overstates the use of fiber in this path. If, for instance, a utility has 300 substations and they indicate they use fiber and leased lines, there could be any proportion of each (i.e., 15 could have fiber or 299 could have fiber). Anecdotal evidence suggests that larger utilities still have a majority of leased lines or radio links for communication paths.

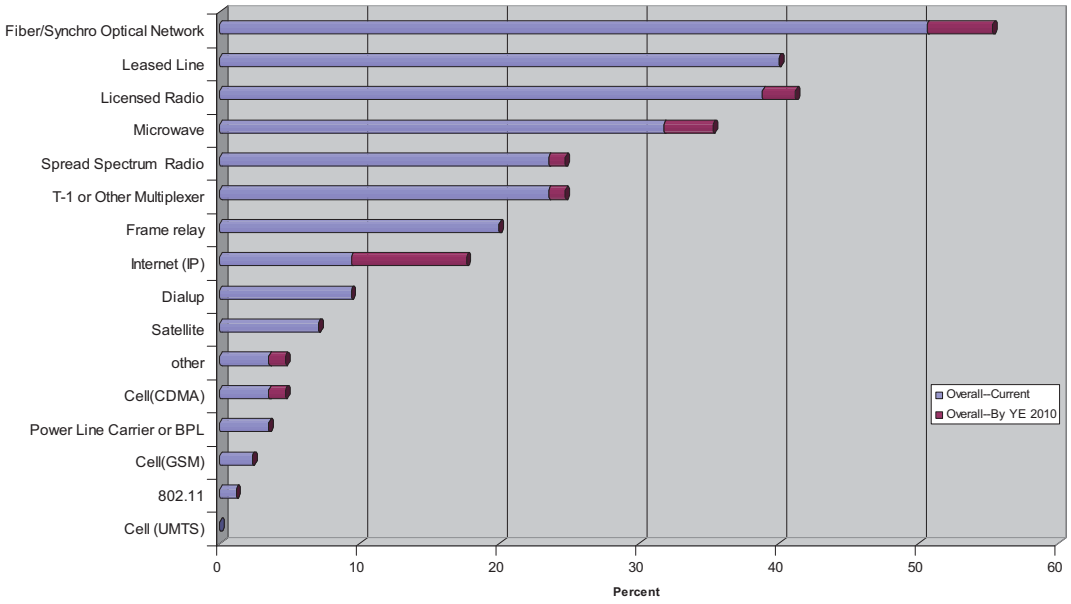



Figure 25. Substation to control center communications channels—current and projected.

The survey also asked about the respondents plans to add links in this path. Internet/IP links were indicated most often, with fiber and microwave being the next most popular.

Figure 26 shows the breakdown of responses by the type of respondent (i.e., investor-owned utility, municipal power company, or electric cooperative). Of these groups, investor-owned utilities are most significant in terms of the number of substations they represent and importance to the overall grid. This group reported a larger percentage of most communications types than the overall average. This is again likely because larger utilities have more of a mix of communications types. The smaller municipalities and cooperatives in general have more homogeneous communications systems. They do outnumber investor-owned utility responses in a couple of categories, though, particularly in spread spectrum and Internet communications.

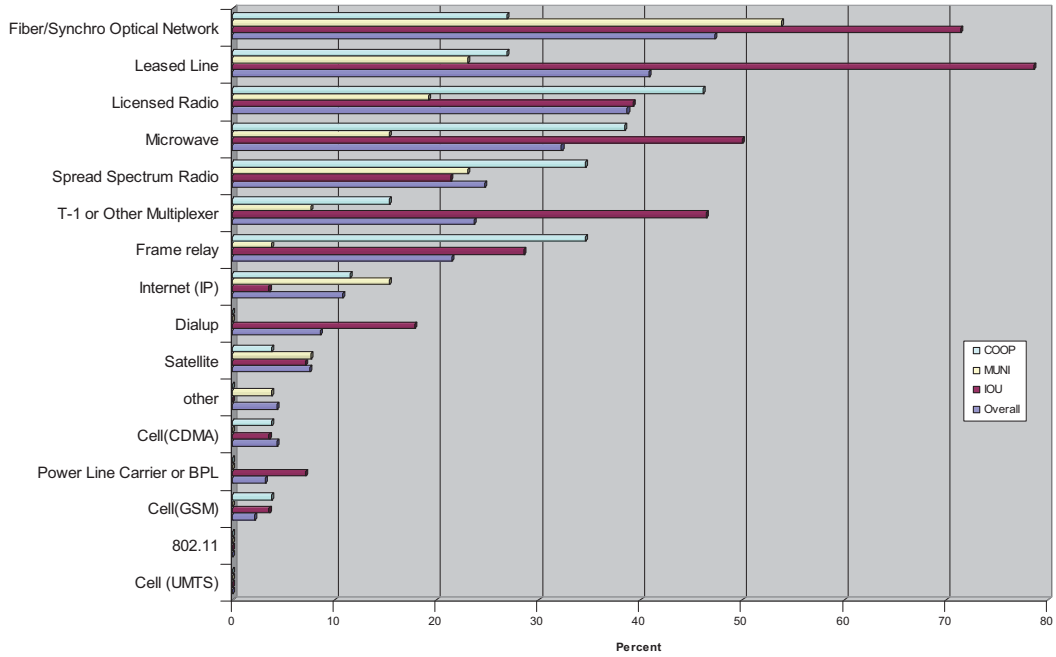



Figure 26. Substation to control center communications channels by utility type.

### 5.4.2 Substation to Substation

Substation to substation communication links are used primarily for transmission line protection. According to the responses to the NESA 2008 study shown in Figure 27, fiber optic communications are also the most used form of communications in this path, with power line carrier a distant second. Power line carrier, as the name suggests, uses the actual power line as the communications medium, and uses modulation of a radio frequency signal superimposed on the 60 Hz wave to transmit and receive information. Microwave radio is the third-most popular communications type. As with substation to control center communications, Internet/IP communications is the largest growth area according to the survey.

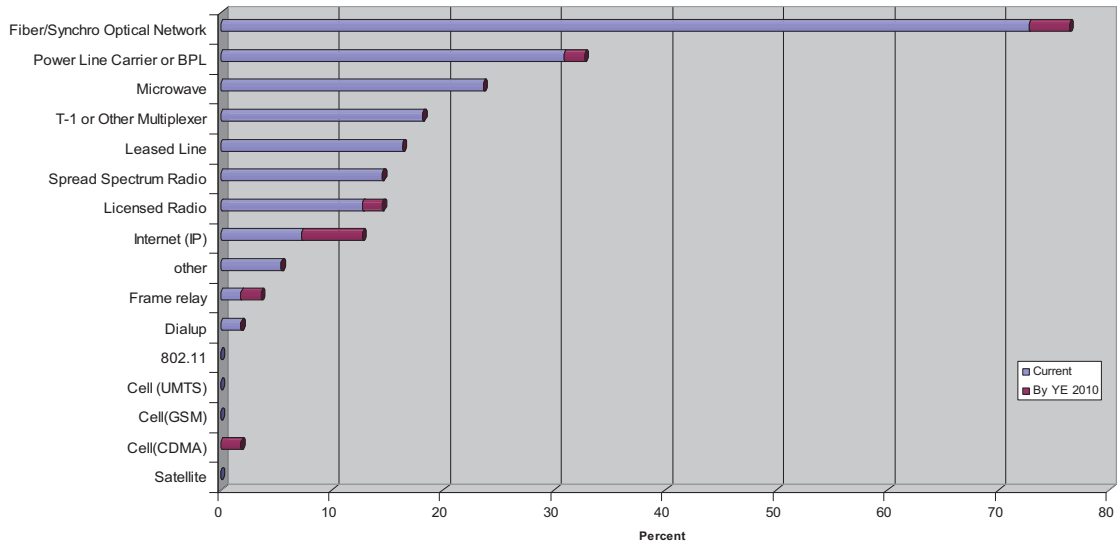



Figure 27. Substation-to-substation communications by channel type.

Figure 28 shows communications channels by entity type. As shown in the figure, investor-owned utilities are slightly more likely to use fiber than average and very much more likely to use leased lines and licensed radio. Public power entities are much more likely to use fiber than any other channel type. Cooperatives have a much higher utilization of spread spectrum radio and frame relay than the others.

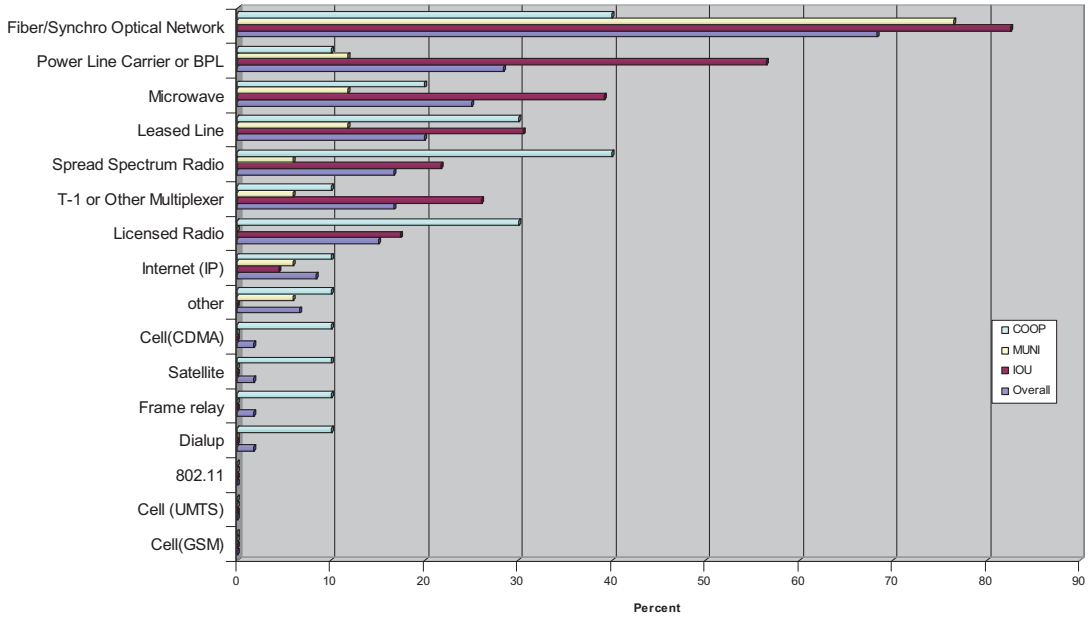



Figure 28. Substation-to-substation communications by entity type.

### 5.4.3 Engineering/Maintenance Access

Engineering and maintenance access provides engineers and technicians the ability to log in remotely to perform tasks such as programming devices, checking their status, download new firmware, and upload event reports or error logs. Figure 29 shows the types of channels used for this purpose. Dialup circuits

are the most common, with fiber optic a close second. Internet was the third-most popular and was also the most common path considered for future implementation. Licensed radio, microwave, and cellular communication are small but growing communications circuits being considered for remote access.

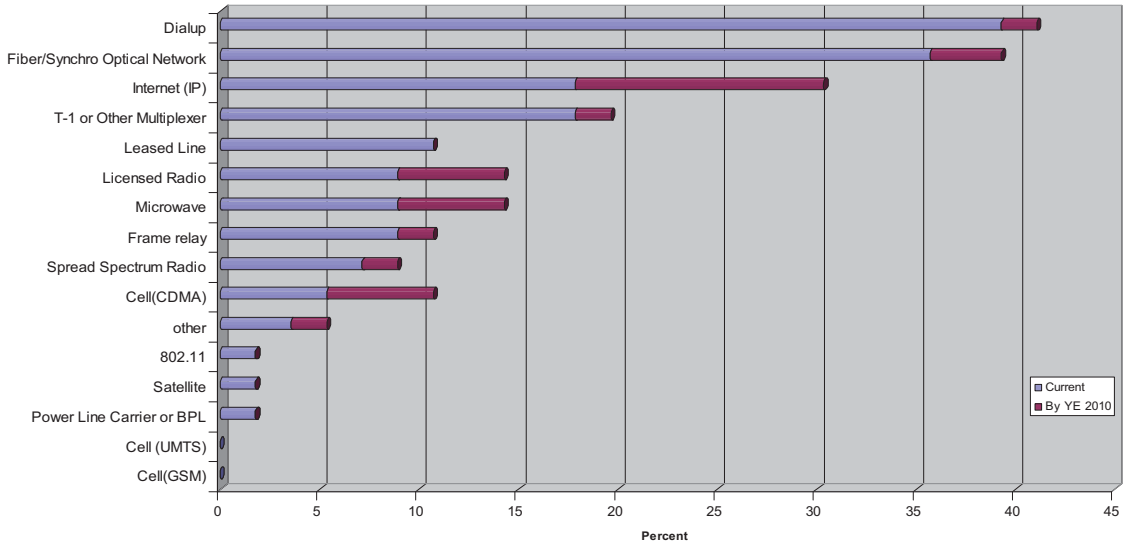



Figure 29. Engineering and maintenance communications by type.

Figure 30 shows the breakdown of engineering access by entity type. As shown from the figure, investor-owned utilities are more likely than average to use dialup or T-1 channels to access devices remotely. Public power entities are again very likely to use fiber for this purpose, and cooperatives use dialup, Internet, and frame relay in almost equal proportions.

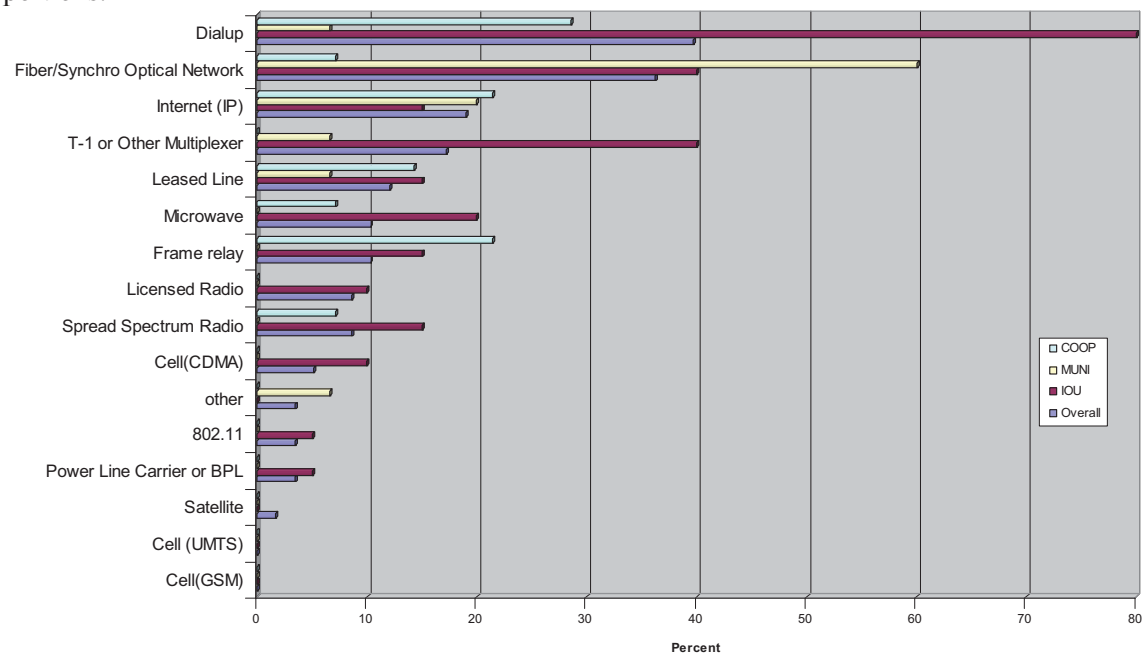



Figure 30. Engineering and maintenance communications by entity type.

### 5.4.4 Substation to End Device

Figure 31 shows a breakdown of substation-to-end device communications by type. Substation-to-end device communications can be for such things as capacitor bank control, control of pole-top switches, or reclosers or perhaps for advanced metering infrastructure. The communications types used most often for this purpose are fiber optic, spread spectrum radio, and Internet. As in previous cases, Internet usage shows the most planned growth, along with Code Division Multiple Access (CDMA) cellular.

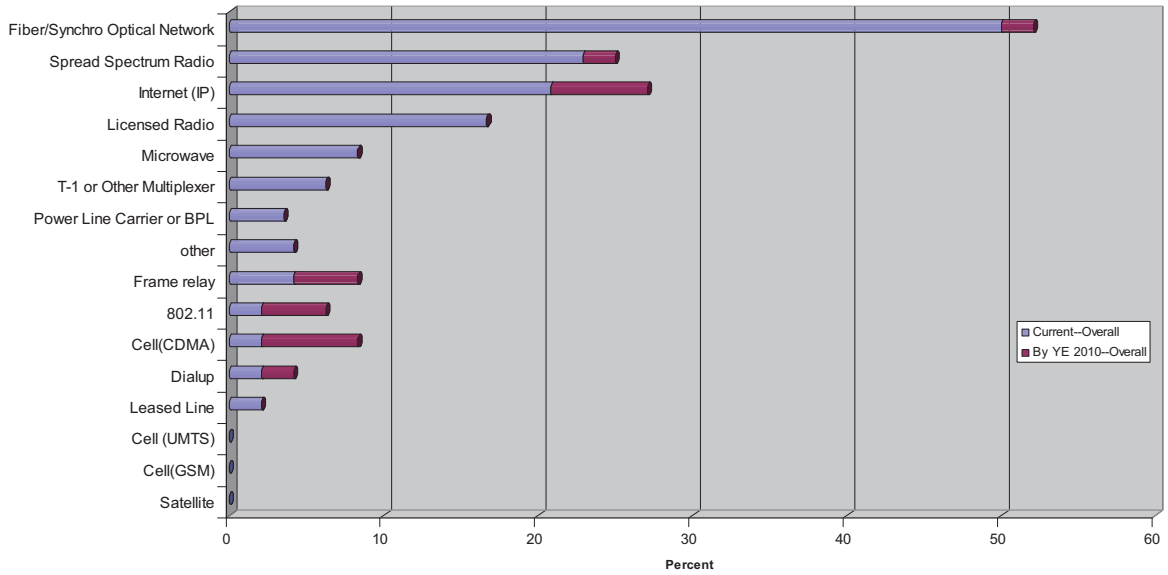



Figure 31. Substation-to-end device communications by type.

When broken down by entity type, as shown in Figure 32, all entities are most likely to use fiber for this purpose. For investor-owned utilities, Internet is the second most popular option; spread spectrum radio is second, most likely for both Public Power and cooperatives.

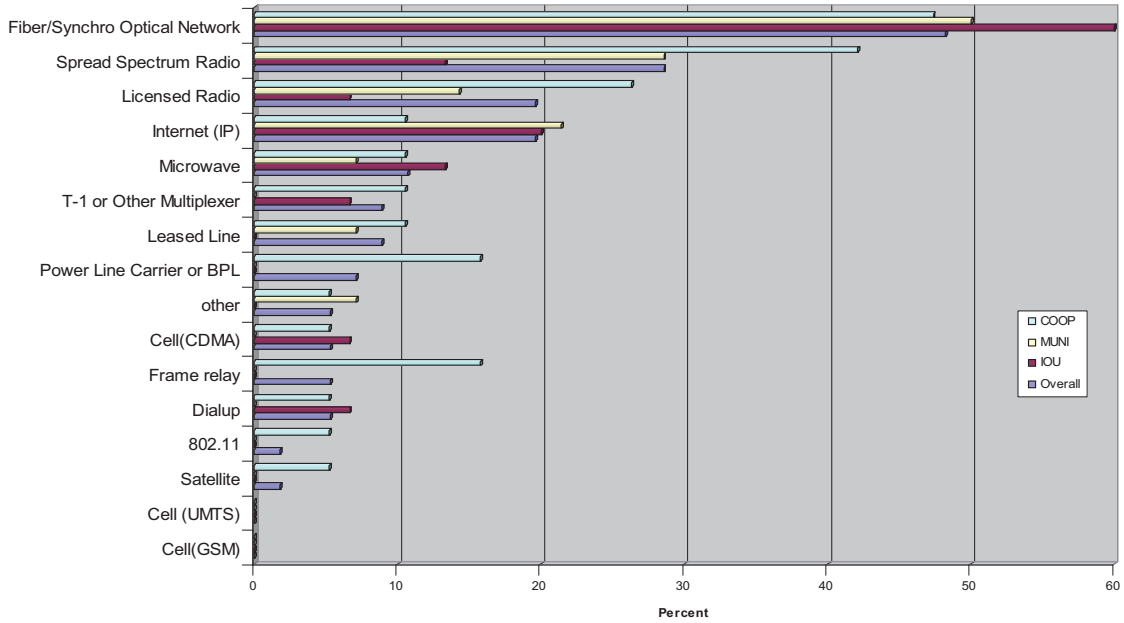



Figure 32. Communications-to-end devices by entity type.

### 5.4.5 Vendor Access to Substation

Figure 33 shows the usage of vendor communications by type. Communications circuits for external vendor access were indicated as being used by very few respondents. Of those who allow vendor access, dialup was by far the most commonly used communications type, followed by Internet and CDMA.

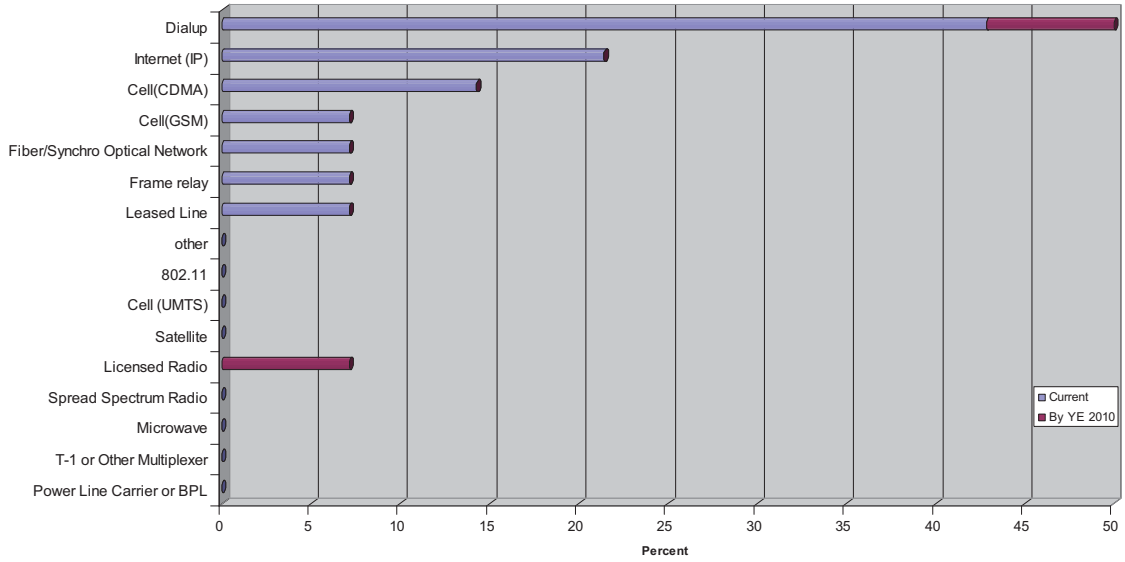



Figure 33. Vendor communications by type.

Broken down by entity, Figure 34 shows that there is almost no usage by investor-owned utilities for remote vendor access. Cooperatives are most likely to implement remote vendor access and use dialup and Internet/IP in almost equal proportions.

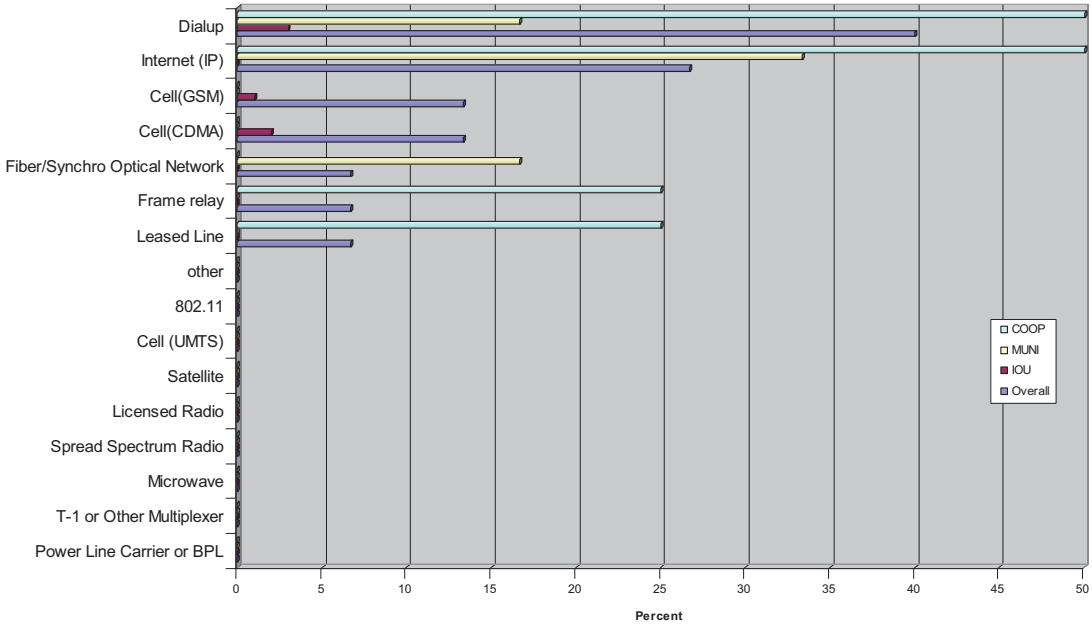



Figure 34. Vendor communications by entity type.

## 5.5 Protocol Usage

The NESA 2008 study asked respondents to indicate the protocols they use internal to the substation and from the substation to an external host. There may be some ambiguity in what is meant by an external host, but since host and master are often used interchangeably, one can assume that for the bulk of the respondents, this question refers to the substation-to-control center link. Figure 35 shows the survey responses to this question. Overall, the serial and LAN versions of DNP 3.0 tied for most popular at 44% each. "Other" was next most popular, indicating that proprietary protocols are still predominantly used. Also, there is no indication that International Electrotechnical Commission (IEC) 61850 is catching on in the U.S. IEC 61850 is an international standard protocol that was intended to improve interoperation of devices from different vendors for substation applications.

Concerning future plans to implement any of these protocols, DNP 3.0 LAN was indicated most often; if this proves correct, it will be the most commonly used protocol by 2010.

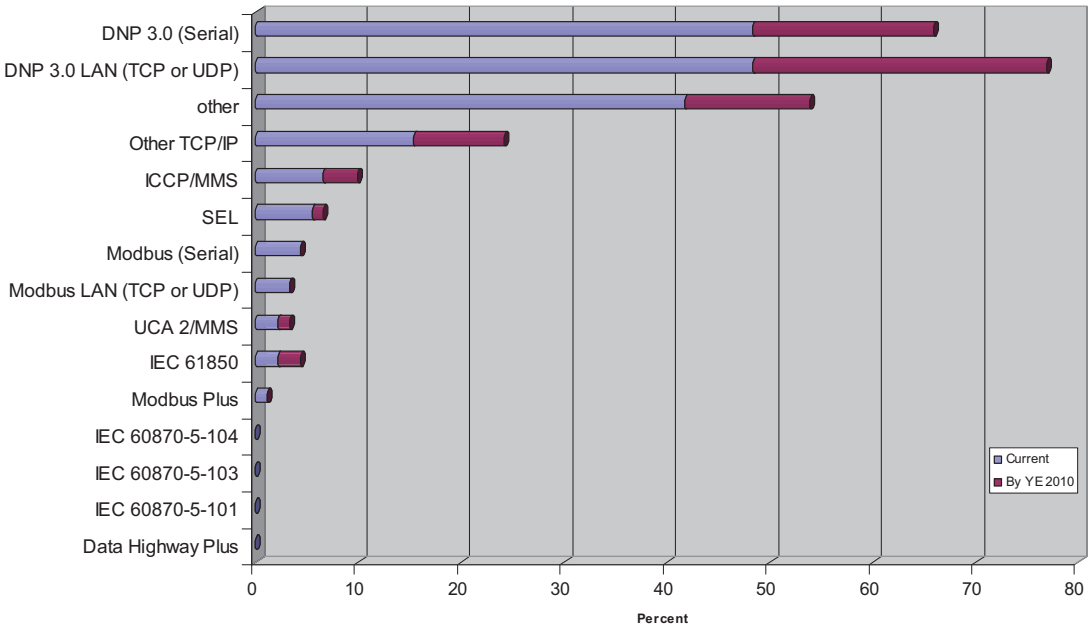



Figure 35. Current and future protocol usage among utilities.

When broken down by entity type, Figure 36 shows that the "other" column is still very much applicable to investor-owned utilities. Over 60% of them still use proprietary protocols, well outpacing the approximately 44% who indicate the use of DNP 3.0 LAN.

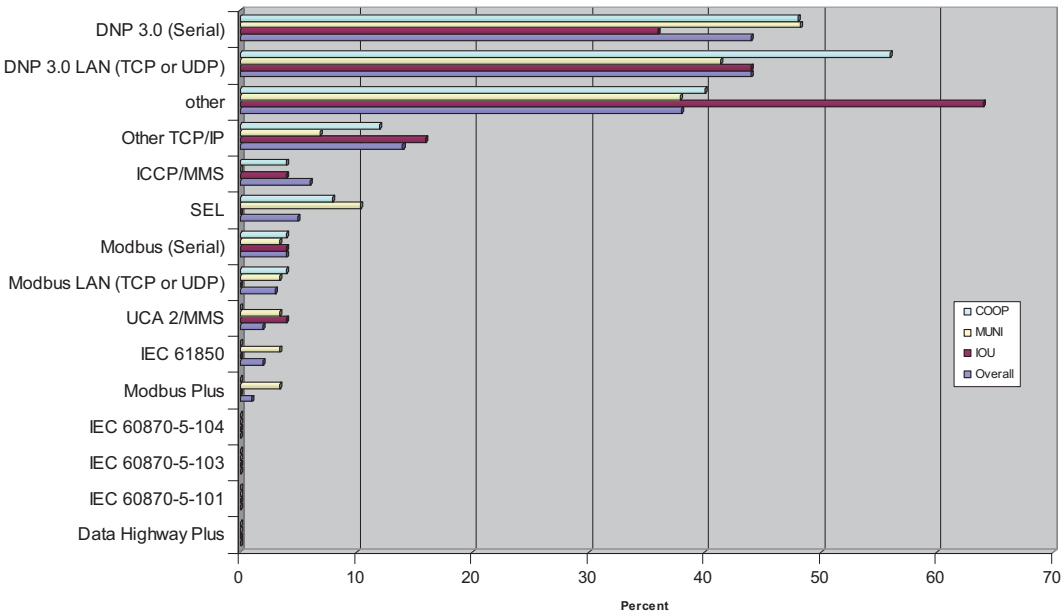



Figure 36. Protocol use by entity type.

## 5.6 Vendors of Communication Equipment

### 5.6.1 Leased Line

Of the 20 respondents who indicated a leased line vendor, the largest percentage of them (25%) indicated their local telephone or service provider. As shown in Figure 37, others indicated specific providers (Verizon [20%] and AT&T [15%]). Several other providers had one mention each.

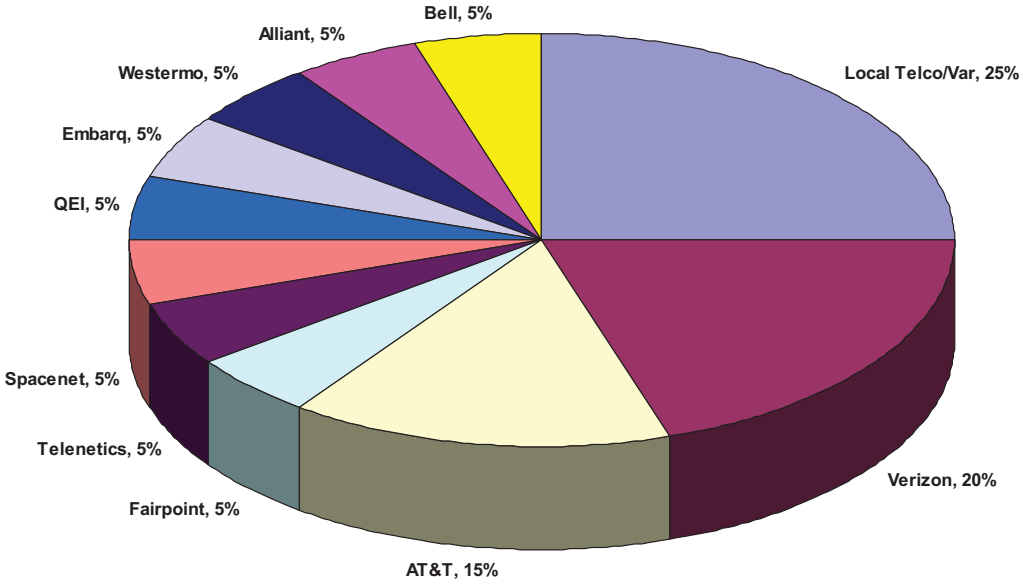



Figure 37. Vendors of communication equipment.

### 5.6.2 Fiber Optic

Of the 23 respondents in the NESA survey who indicated a vendor for their fiber optic communications system, there was a mix among manufacturers or installers of the actual fiber (e.g., Siecor/Corning, In-house) and manufacturers of the communications equipment that uses the fiber. Among equipment manufacturers, GE/Lentronix has the clear lead with 26% of the market; SEL and Cisco tied with the second-most mentions (see Figure 38).

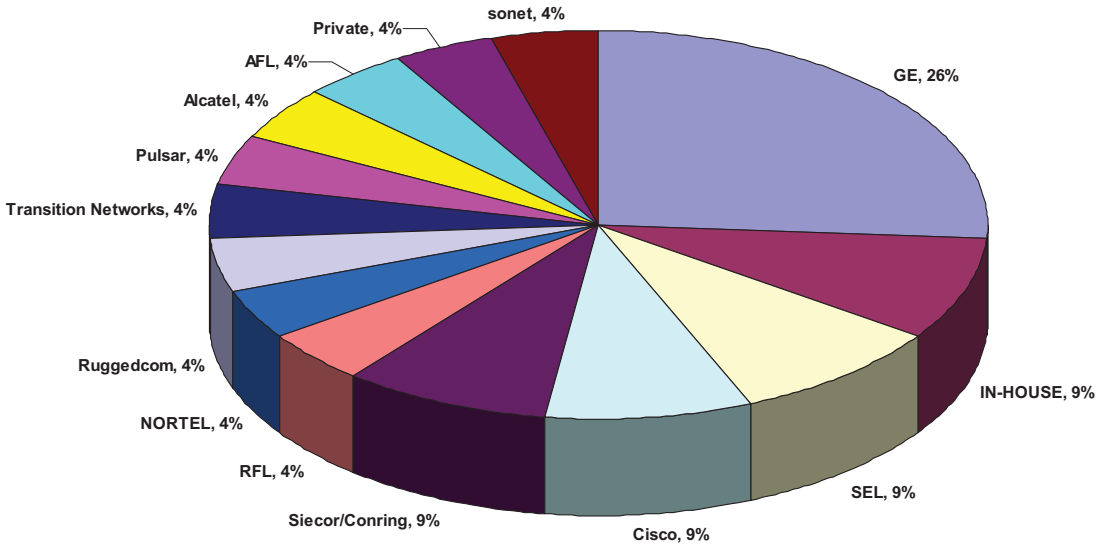



Figure 38. Vendors of fiber optic communications equipment.

### 5.6.3 Licensed Radio

Among the manufacturers of licensed radio equipment, Microwave Data Systems (MDS) has the clear majority. Of the 21 respondents to the survey, 17 indicated MDS as their manufacturer of choice. Motorola was a distant second with two mentions (see Figure 39).

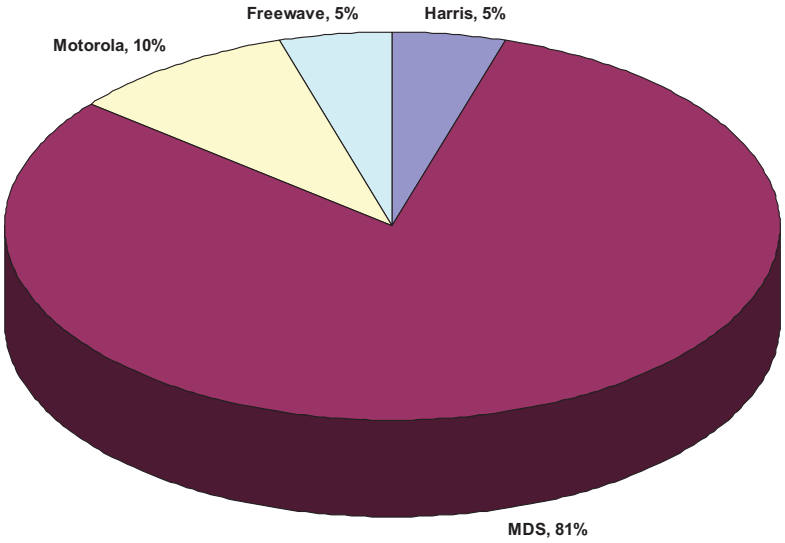



Figure 39. Vendors of licensed radio equipment.

### 5.6.4 Microwave

Among manufacturers of microwave equipment, Harris led with five mentions of 10 respondents. MDS was second with two mentions (see Figure 40).

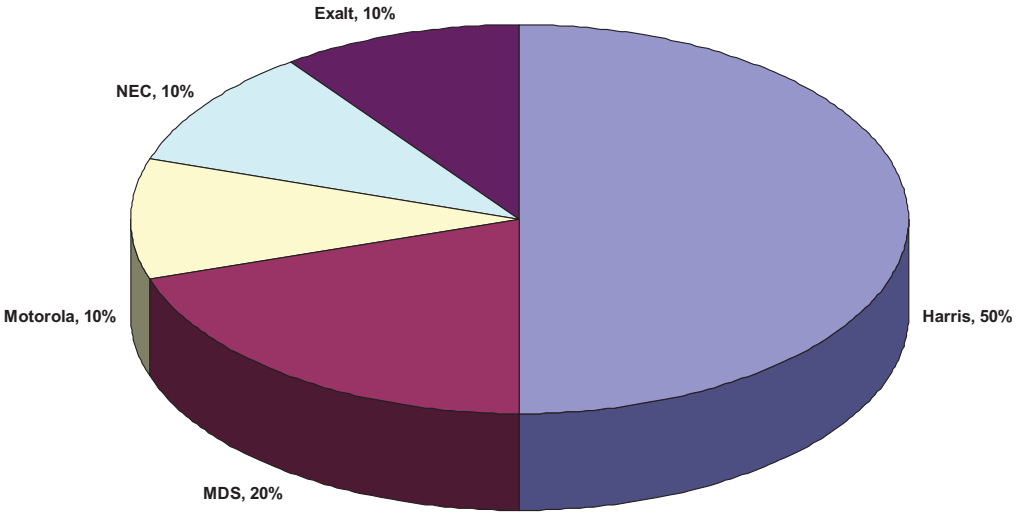



Figure 40. Vendors of microwave equipment.

### 5.6.5 Spread Spectrum

An exact copy of the licensed radio market, the unlicensed spread spectrum market is dominated by MDS among respondents. Motorola is a distant second (see Figure 41).

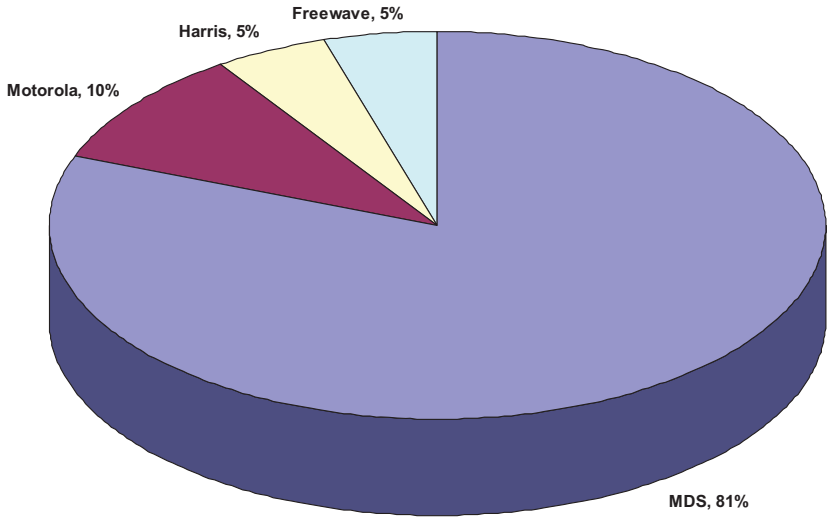



Figure 41. Vendors of spread spectrum equipment.

### 5.6.6 T-1

The response for T-1 multiplexer vendors appears to be split among the providers of the T-1 circuits and the manufacturers of the endpoint electronics. RFL, a manufacturer of T-1 multiplexers, led this category with six mentions of a total of 21 responses. Of the names mentioned by the rest of the respondents, Alcatel and Fujitsu are also equipment manufacturers. The rest appear to be service providers (see Figure 42).

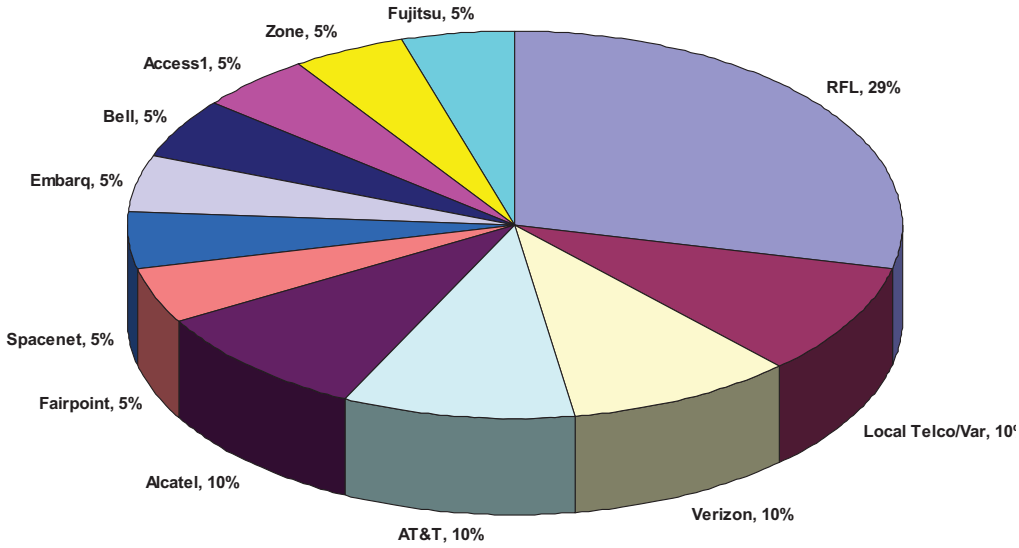



Figure 42. Vendors of T-1 multiplexers.

# 6. Substation Automation Case Studies

As part of this effort, INL visited five utilities. One of the goals of these visits was to better understand the utilities interpretation of the questions asked in the 2008 Substation Automation Market Survey study by Newton-Evans. Another goal was to get a "pulse" on the progression utilities are taking toward substation automation and their migration from older electro-mechanical relays and to digital relays. This will, in part, determine the extent that substations are vulnerable to remote cyber attacks.

## 6.1 General Observations

An important observation was that utilities visited had an excellent awareness of security measures that either are required or were considered "best practice." Some utilities that are not part of the "bulk electric system" still followed the CIP 002–009 standards as they thought they made sense and were good practice.

Another parallel observation was that all utilities were going through some sort of upgrade or new installation. As part of this process, security was an important factor in determining the best practice and selection of system or components.

## 6.2 Investor-owned Utility 1

### 6.2.1 Overview

The INL project team visited a large investor-owned utility serving over a million residential customers with additional commercial and industrial customers. The utility was in the progress of upgrading and building new substations to address the age of some of their substations and to accommodate ongoing growth.

### 6.2.2 Substation Communications

The investor-owned utility had over 200 substations within their area of responsibility. Figure 43 illustrates typical communications to substation. Typical substations had an SEL RTU and an SEL data concentrator. SCADA communications between the control center and the RTU were standardized using a proprietary protocol. The communication between the RTU and data concentrator used DNP 3.0. SCADA communications were used for gathering of SCADA-related information and also used for device control. A serial link between the control center and the typical substation was implemented. The serial link media was converted to fiber optics for communication back to the control center. The entity owned a majority of the fiber used for SCADA communications. These communications were over a dedicated fiber strictly for substation communications. In cases where they did not own it, the local service provider was used for serial communications. For these communications, encryption was used (using "Bump in the wire" technology). No third-party remote communication links or remote engineering access connections were available to DPCDs. Event collection and relay settings changes are performed locally at the substation.

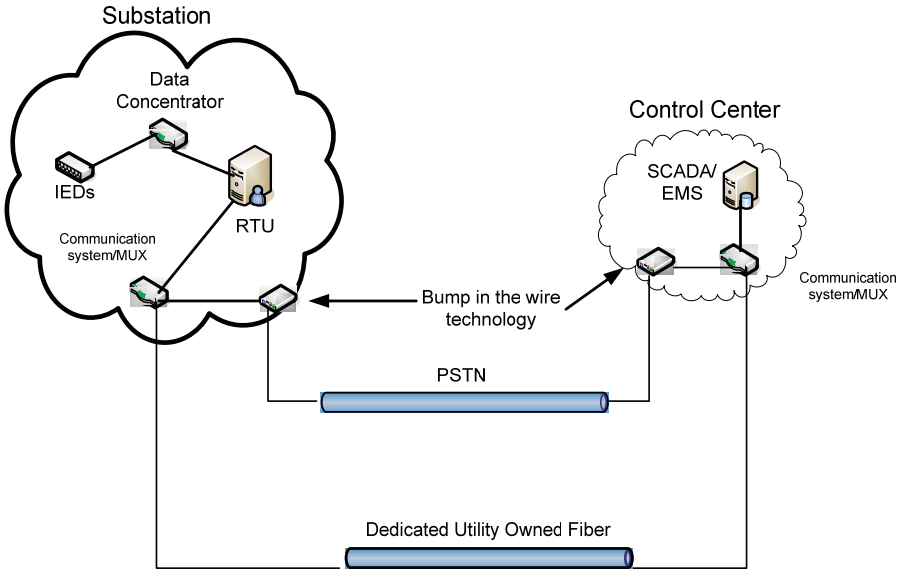



Figure 43. Typical communications to substation.

### 6.2.3 Substation Automation

Substation automation implementation consisted of relay integration, SCADA monitoring, and SCADA control. No substation Transmission Control Protocol (TCP)/IP LAN or local control station was used. No local SCADA at the substation was implemented, although manual local control of devices was in place. The entity was in the process of installing other distribution automation devices outside the substation. This technology area is relatively new in the market place and requires further research to fully understand any potential impacts to cyber vulnerability. This utility has standardized on SEL equipment for primary relay protection and control. They use GE as a redundant secondary relay protection and control. This is consistent with the results from the NESA 2008 Study. This study had SEL as the first in utilization and GE as second. The utility has a configuration management system along with a password management policy in place for security of all IEDs.

### 6.2.4 Substation Physical Security

The typical substation had a locked gate, locked door, door alarm, key card access, and camera for security measures.

## 6.3 Electric Cooperative 1

### 6.3.1 Overview

The INL project team visited an electric cooperative serving over a 100,000 residential customers with additional commercial and industrial customers. The utility was in the progress of upgrading and building new substations to address the age of some of their substations and to accommodate ongoing growth.

### 6.3.2 Substation Communications

The entity had over 25 substations within their area of responsibility. Communications between the control center and the substation RTU primarily consisted of collecting SCADA-related information and

performing SCADA control. SCADA communications to the RTU were standardized using the DNP 3.0 protocol. Figure 44 illustrates typical communications to substation for the electric cooperative. A serial-type link between the control center and the typical substation was implemented. The serial link media was converted to fiber optics for communication back to the control center. The entity owned all the fiber used for SCADA communications. These communications were over a dedicated fiber strictly for substation communications. In addition to the fiber media, the cooperative used microwave as part of a Synchronous Optical Network (SONET) loop. Neither third-party remote communication links nor remote engineering access were available to control DPCDs at the substation. The cooperative had recently installed digital cameras for substation security, which communicate back to the control center using a different communication system and different fibers.

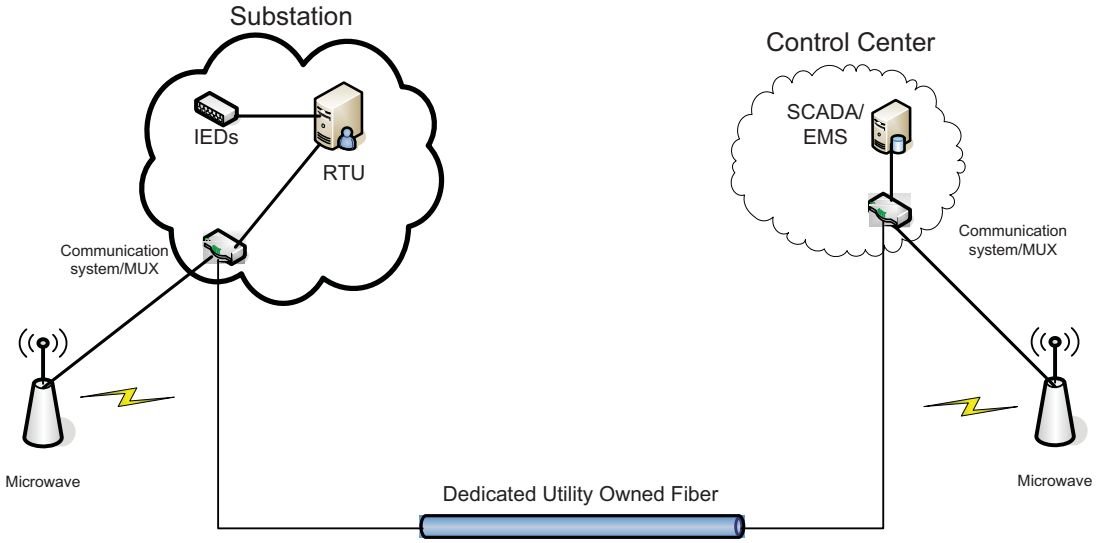



Figure 44. Communications to substation.

### 6.3.3 Substation Automation

Substation automation implementation consisted of relay integration, SCADA monitoring, and SCADA control. No substation TCP/IP LAN or local control station was utilized. No local SCADA at the substation was implemented, although manual local control of devices was in place.

The utility uses a Telvent RTU to collect SCADA information and perform SCADA control. This utility is standardized on ABB and GE equipment for primary and back up relay protection and control. This is consistent with the results from the 2008 Substation Automation NESA 2008 Study.

The utility has a configuration management system along with a password management policy in place for security of all IEDs.

### 6.3.4 Substation Physical Security

The typical substation had a locked gate, locked door, door alarm, key card access, and cameras for security measures.

## 6.4 Municipality

### 6.4.1 Overview

An INL project team visited a small municipal utility (serving approx 55,000 customers, 15 to 20 substations, 200 MW capacity). The host utility team consisted of individuals covering operation, maintenance, and control of the SCADA operation. This utility's control system was in the process of continual upgrade based on user demand and available funding.

Because the municipality has less than 200 MW generating capacity, the Western Electricity Coordination Council has exempted this utility from NERC CIP standards. However, this utility has taken the position to adhere as practical (within available funding) the NERC standards and has made plans to meet the majority of the CIP standards in the near future. This utility is not considered a Bulk Electric System (BES) provider nor is its system considered part of the BES.

### 6.4.2 Substation Communications

Typical substations have a primary and secondary form of communication. The primary communications link is via Ethernet over fiber optic media. Equipment at the substations is equipped to use multimode fiber versus the trunk single mode fiber and requires conversion boxes at each substation. Normal city data communications are available by using a hub that attaches directly to a single mode fiber that ultimately connects back into the backbone equipment. The second communication method is a backup radio communications link rated at 19,200 baud. The radio communications link is a redundant system using two separate frequencies, but future plans may be to abandon the radio link. Inside the substation, this utility uses serial links to connect their protective relays to their RTUs. The municipality owns and maintains the fiber optic media for the communications backbone and for the substations communication. The municipality does have one leased line on the PSTN from the local service provider communicating to one of their substations. No bump in the wire technology is currently being used for this application. See Figure 45 for a typical substation architecture.

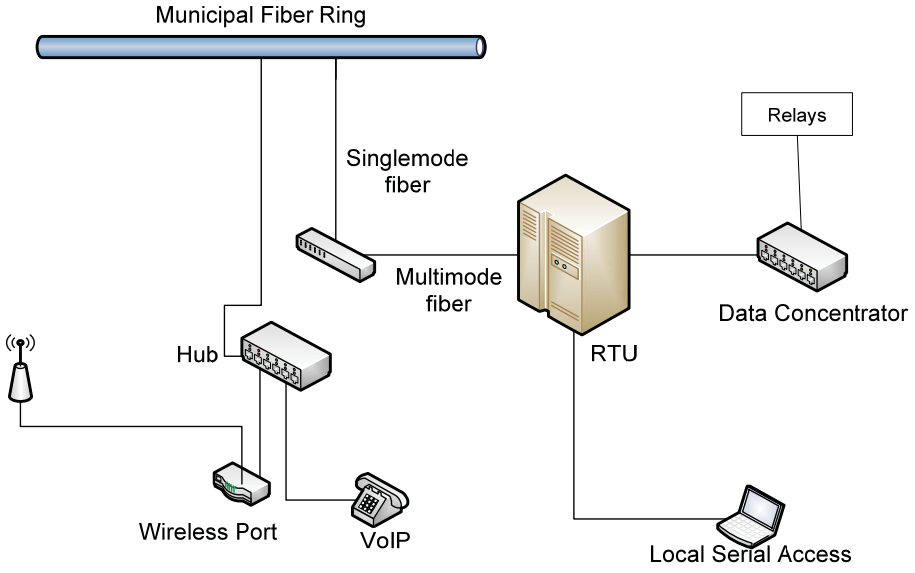



Figure 45. Typical substation control building.

The municipality primary IT service is protected by firewalls. The power utility does not plan for intrusion detection system at this time for the SCADA portion of the network. No firewalls are within the city network separating SCADA traffic from business traffic. The utility has future upgrade plans to harden the SCADA system isolating it from outside business traffic and installing a SCADA firewall, isolating the SCADA LAN from the business LAN. Open communication links to the SCADA system are minimized, but known links exist. These links are primarily managers requiring real-time data displays of system operation. Plans are not finalized at this time.

VoIP is utilized to reduce additional telephone infrastructure, also allowing vendor system updates to be available by this source. VoIP may be considered another access vector. Other business sectors (such as police) also use the substation for remote access to the city network via wireless access ports.

### 6.4.3 Substation Automation

With respect to substation automation equipment, this utility uses RTUs that utilize the DNP 3.0 protocol to communicate with the SCADA master. A DNP 3.0 serial link connects the RTU to protective relays. This utility is standardized on SEL equipment for relaying and data concentration, which is consistent with the findings of the 2008 survey. Neither the relays nor the data concentrator have external engineering/maintenance connections. Event collection and settings changes are done locally. Other utilities have equipment in the two substations that connect this utility to the BES, but their equipment is separate and uses separate communications links.

SCADA system data traffic is not completely isolated from normal business data traffic, sharing the fiber optic data bus backbone throughout the municipality. Separation is accomplished by domain separation. The SCADA network runs on a protected portion of the overall bandwidth, which is similar to a virtual private network. The utility is developing additional plans to further isolate and enhance security on the SCADA side.

### 6.4.4 Substation Physical Security

Substation physical security consists of locked gated chain link fencing topped with three-strand barbed wire, and the control building has a locked door to control entry. The future plan is to install door alarms and exterior cameras because the fiber is already installed. In some cases protective relays are installed in the breakers in the yard. In the substation the INL team visited, the relays were in the control house. Breaker doors in the yard had no locks on them, which would allow anyone who could get past the outer fence to manually operate any of the breakers. Utility personnel have recognized this and are planning to install locks in the near future.

## 6.5 Investor-owned Utility 2

### 6.5.1 Overview

The INL project team visited a large investor-owned utility serving over a million residential customers with additional commercial, industrial, and government customers. The host utility consisted of a team of various disciplines. In general, the utility is experiencing growth and are in the process of addressing associated issues. In addition to addressing growth, they have short and long-range plans to upgrade substation communications.

### 6.5.2 Substation Communications

The investor-owned utility currently has approximately 500 transmission and distribution substations. Typical substation communications include three communication links. The first is a serial link used for SCADA monitoring and control and communicates using a Satellite Very Small Aperture Terminal system. The second is a modem connected to an IED used to download event reports. The modem uses the local service provider Telcom system. The third is a power line carrier used for relay protection. Other types of communications are used in specific isolated applications such as microwave, 900 MHz wireless, leased line, and CDMA/Global System for Mobile Communications (GSM).

Plans to upgrade substation communications to Ethernet links are in the making. Higher priority substations will be converted first. The communication link is anticipated to be with the local service provider.

The SCADA link uses a proprietary protocol for its monitoring and control. The SCADA communications link talks between the control center and a Telvent RTU. Some use of the protocol DNP3 exists between a data concentrator and the RTU. See Figure 46 for a simplified communications architecture.

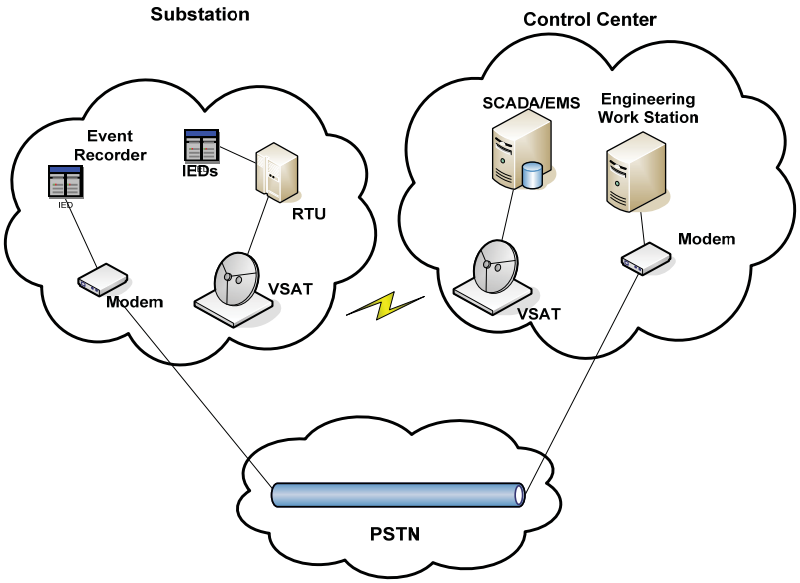



Figure 46. Simplified communications architecture.

### 6.5.3 Substation Automation

Substation automation implementation consisted of relay integration and SCADA monitoring and control. No substation TCP/IP LAN or local control station was utilized. No local SCADA at the substation was implemented, although, manual local control of devices was in place. Plans were also discussed to make the grid "smarter." This includes pilot programs and testing of such devices that perform distribution automation, substation automation, and automatic meter reading.

Use of DPCDs was about 20 to 40% for existing substations and 100% for all new substations. Protection and control was implemented through one device. Redundant protection is implemented in the transmission system, and some transmission has redundant communications. The utility used SEL as the primary vendor for relay protection and control.

### 6.5.4 Substation Physical Security

The typical substation had a locked gate and in some locations had two locked gates to go through for vehicular access. Upon completion of an Ethernet-network for substation communications, digital security cameras will be evaluated.

## 6.6 Electric Cooperative 2

### 6.6.1 Overview

The INL project team visited an electric cooperative serving over 50,000 residential customers with additional commercial and industrial customers. The host utility consisted of a substation lead. The cooperative performed only distribution as transmission assets were owned by their provider. The cooperative had approximately 20 substations that were relatively small in size.

### 6.6.2 Substation Communications

The entity used fiber optic cable as their main communication media. Some 900 MHz system is latent and used if backup is necessary. The fiber optic cable is in a ring topology and has redundant paths. In some areas, the cooperative has agreements to use other entity's fibers in exchange for use of their fibers. There are two communication links to each of the substations. The communication hub acts as a terminal server for serial communications and some IP ports for Ethernet communications. Serial communication was used for SCADA monitoring and control of the Telvent RTU. The Ethernet communication was for engineering access for the same RTU. All communication hubs were located within the substation or control center and were the responsibility of the cooperative. No outside provider was used for communications. See Figure 47 for a simplified communications diagram.

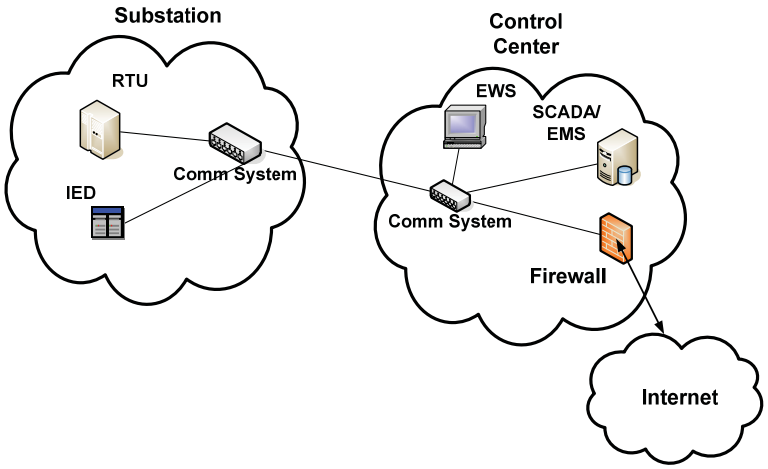



Figure 47. Simplified communications diagram.

The cooperative had a fully operational automatic meter reading system that communicated from the substation to the remote meters. This used the vendor-specific power line communication system. Once the data was in each substation, the IP network was used to transmit these data to a centralized location. The data is utilized for billing and outage management. A firewall was used for isolation of Enterprise network traffic from Internet traffic.

There were no third-party or remote communication links to the DPCDs at the substations, with the exception of a neighboring utility having a remote communication link for meter reading.

### 6.6.3 Substation Automation

Substation automation implementation consisted of relay integration, SCADA monitoring, and control. No local SCADA at the substation was implemented, although, manual local control of devices was in place.

The cooperative used Telvent RTU to collect SCADA information and perform SCADA control. This utility was standardized on ABB and GE for relay protection and control. They have standardized separate protection and control for operation of their devices.

Approximately 60 to 80% of the relay protection is performed through DPCDs. Automatic reclosing is implemented in most distribution system breakers.

### 6.6.4 Substation Physical Security

The typical substation had a locked gate, locked door, and door alarms for security measures. A pilot program was in process for testing digital cameras at each substation.

## 6.7 Observations from Utility/Substation Visits

The personnel that the INL team visited at each utility had very good awareness of security measures and the need for them. The two investor-owned utilities were the only utilities that fell under North American Electric Reliability Corporation (NERC) CIP regulations, but the others have implemented security measures on their own. With a couple of exceptions, all had a password management plan in place and use strong passwords on their RTUs and IEDs. One of the cooperatives intentionally decided to not provide remote access to their protective relays, believing that the added risk was not worth the benefit, even though they had their own fiber optic network. One of the investor-owned utilities chose not to provide network capability to their substations, even though they had their own fiber as well, citing added security risk. The investor-owned utilities both use proprietary serial protocols; one made reference to gaining some “security through obscurity.”

Most of the utilities we visited indicated a desire to have more information available regarding information on security of substation automation. This was particularly true of the investor-owned utility preparing for a major upgrade of its communications system. In general, it did appear that there were more challenges related to implementing network-based systems as opposed to serial. Configuration and segmentation of networks, as well as the application of firewalls seem to be issues of particular interest and need.

# 7. STANDARDS AND RECOMMENDATIONS

This section briefly discusses the applicability of standards to electrical substations in regard to providing security to critical assets. The intent here is not to reiterate the NERC CIP 2–9 standards[3] nor is it to review previously documented NERC guidelines. It is merely a statement of methodology specifically targeted to electrical substation security measures.

## 7.1 Bulk Electric System

In order to determine the applicability of NERC CIP 002 through 009 standards to electrical substations, it must first be determined if the electrical substation supports "reliable operation of the BES."[3] After this determination is made by the utility, identification of the critical cyber assets is made, as described in CIP-002.

In cases where CIP standards do not apply, due diligence in protecting company's assets only makes good business sense. Appropriate levels of physical security and cyber security should be implemented using a risk assessment methodology. In determining the appropriate levels of security, some utilities are using the CIP standards as a minimum or in addition to their company standards. INL has anecdotal information that some entities are complying with the CIP standards even if they do not support operation of the BES in anticipation that they will apply in the future.

Generally, substations that perform transmission functions are required to be compliant with the CIP standards, while substations that perform more distribution functions are generally exempt from the CIP standards. Specific compliance is handled on an individual substation or entity basis.

## 7.2 Other Standards

Many other organizations have standards applicable to electrical substations. These include but are not limited to:

- IEEE 1402, "Guide for Electric Power Substation Physical and Electronic Security"
- IEEE P802.11I, "Standard for IT Telecommunications and Information Exchange Between Systems"
- IEEE C37.1, "Guide for SCADA and Automation Systems"
- IEEE 1686, "Substation IEDs Cyber Security Capabilities"
- IEEE 1615, "Recommended Practice for Network Communications in Electric Power Substations."

# 8. GENERAL RECOMMENDATIONS FOR SUBSTATION SECURITY

Given the potential consequences and gaps in security identified in this report, it is clear that there is still work to be accomplished to achieve an acceptable level of security with respect to substation automation. The needed security improvements will require not just a commitment from utilities, but a coordinated effort among utilities, manufacturers, service providers, regulators, and others. The sections that follow contain recommendations of actions necessary to aid in this effort.

## 8.1 Recommended Practices

Some recommended practices have been written by DOE NSTB, Department of Homeland Security CSSP, or other entities that apply to substation automation systems. These include:

- "Recommended Practice for Securing Control System Modems," Department of Homeland Security, January 2008.
- "Wireless Recommended Practice," Electric Power Research Institute et al., 2009.

However, no recommended practice document focuses on substation automation devices, communication types, and specific mitigation strategies for substations. Therefore, the INL team recommends that a subsequent document be generated, "Recommended Practices for Securing Substation Automation Devices." A second recommendation for this effort would be the generation of procurement language for substation automation, similar to existing language written for the SCADA/EMS systems.[8]

## 8.2 Vendor Assessments

Through NSTB and other program efforts, several substation automation devices have been assessed for their level of cyber security. In every case, cyber vulnerabilities have been found. Work is ongoing with vendors to mitigate these vulnerabilities. However, most of the work has been focused on answering specific questions for specific projects, so there has been no comprehensive effort to assess the majority of substation automation devices and the communications devices they rely on.

Assessments of the most commonly used substation automation devices, including RTUs and protective relays in particular, should be performed. In addition, the products of the major vendors of communications equipment should also be assessed.

## 8.3 Onsite Assessments

Based on INL onsite visits and other contacts with utilities, there is a desire and a need to know more about implementation of substation automation security. Onsite assessments provide real-world practical solutions for industry partners. Onsite assessment recommendations:

1. Perform at least one full hands-on onsite assessment with a utility that has already implemented substation automation at Levels 3 and/or 4 to determine the component and systemic vulnerabilities that are present.
2. Support utilities in the process of upgrading their substations specifically in the area of cyber security, to help them through some of the security issues and learn what issues arise in these cases. These lessons learned could be rolled into a substation automation recommended practice document for others to use as they implement substation automation systems.
3. Include the communication provider for leased line systems in one substation automation assessment. The pervasive attitude that serial, non-routable communications are relatively secure is based on the

assumption that the provider's system is secure. This assumption should be validated by including an assessment on the security of the provider's network.

## 8.4 Training

Most of the utility personnel who were visited as part of this effort indicated an interest in training opportunities that include increasing awareness of potential substation vulnerabilities, methods of detecting intrusions or attacks, and ways of recovering from attacks. One of the issues with substation automation is that, as opposed to control center security, engineers often make more of the decisions in terms of security rather than IT personnel, especially in non-networked environments. Engineers often are not as aware of security issues and implementation tradeoffs. Providing training opportunities, whether in live classes or online tutorials or both, would be of great help. In some cases, INL could adapt training programs already in place to meet these needs. Other training programs may need to be developed, but would be worthwhile to help increase the general knowledge and awareness of engineers with respect to security.

# 9. SUBSTATION TECHNOLOGIES

## 9.1 Substation Overview

Substations are classified as either transmission or distribution according to their voltage level and purpose. Transmission substations' primary purpose is to transmit or "wheel" large amounts of power from one location to another. To keep electrical energy losses to a minimum, their voltage levels are relatively high compared to distribution substations. Common transmission voltage levels are 230 kV, 345 kV, 500 kV and 765 kV. Voltages of 115 to 161 kV are technically considered transmission level, but are often labeled sub-transmission because most lines of these voltages are relatively short.

Distribution substations have as their primary purpose to provide power at a voltage level where it can be transmitted the "last mile" to the load and utilized. Distribution substations step voltage down from transmission or sub-transmission levels to distribution voltage levels. These levels are often in the 5 to 15 kV range, but can be as high as 69 kV.

Common devices that can be found in both transmission and distribution substations are described and shown in Table 2. Substation devices. Photos of equipment are of transmission level devices; distribution devices are typically smaller and have shorter insulators.

Table 2. Substation devices.

| | |
|---|---|
| **Circuit breakers** are high-speed switches that are designed to open automatically in the case of an overload or short circuit event. Unlike most low voltage breakers, medium and high-voltage breakers in substations typically rely on external devices (i.e., protective relays) to sense these conditions. They also can be used for routine switching, or reconfiguration, of power lines, transformers, and loads in and out of service. Opening a breaker causes a large energy arc within the breaker. Because of the high temperature (>20,000°C) of the arc that must be extinguished when opening a circuit at medium and high voltages, breakers must be maintained or replaced after several hundred operations. | <br>Gas Circuit Breaker<br>(www.abb.com) |
| **Power transformers** change power from one voltage level to another voltage level. Transformers can range in size from 1 to 5 MVA in smaller distribution substations to several hundred MVA in larger transmission substations. Transformers are often the most expensive components in a substation and have the longest replacement lead times. A large power transformer can cost well over $1M and take a year to order.<br>Power transformers, especially at the distribution level, often contain LTCs. LTCs adjust the secondary voltage of the transformer by mechanically changing the transformer's turns ratio in small steps. LTCs usually can regulate the voltage by ± 10%, in steps of 1% or less. | <br>Power Transformer<br>(www.abb.com) |

Table 2. (continued).

| | |
|---|---|
| **Phase-shifting transformers** are used to regulate power flow between two substations. They are usually installed on tie lines between utilities and are used to control the import or export of power between utilities. | <br>Phase Shifting Transformer<br>(www.abb.com) |
| **Capacitor banks** are used to support voltage, maximize power transfer between substations, and inject reactive power to the system without relying on rotating machinery (i.e., generators or synchronous condensers). In transmission applications capacitor banks are most often installed in series with the line, whereas in distribution applications they are often installed in a shunt configuration. Shunt applications usually require that the capacitor bank be switched in and out so that they are on only when required (i.e., when the load is great enough to cause the voltage to sag). | <br>Series Capacitor Bank<br>(www.nokiancapacitors.fi/) |
| **Disconnect switches** are slower speed switches that are used to isolate equipment like breakers or transformers for maintenance. In most cases, a disconnect switch is installed on either side of a breaker; a bypass disconnect switch may bypass the breaker when it is not in service. Disconnect switches usually cannot be opened under load, so their associated breaker must be opened first. | <br>Disconnect Switch<br>(http://www.southernstatesllc.com) |
| **Instrument transformers** provide signals that can be measured by protective relays, meters, fault recorders, etc. Potential transformers take the transmission or distribution voltage and transform it to low voltage, usually 120 V. Current transformers reduce the line current by a standard ratio such that the secondary current is on the order of a few amps; the most common secondary ranges are 0 to 5 A or 0 to 1 A. | <br>Potential Transformer<br>(www.abb.com) |

# 10. REFERENCES


1. Newton-Evans Research Company, "The World Market for Substation Automation and Integration Programs in Electric Utilities 2008–2010," Volume 1, North American Market, September 2008.
2. SearchSecurity, "What is HSPD-7?" HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003), replaces earlier PDD-63 (Presidential Decision Directive No. 63 issued by President Clinton May 1998). The primary intent of HSPD-7 is to prevent the exploitation, incapacitation, or destruction of all critical infrastructures and key resources of the government and economic sector. The secondary goal is to foster the development of methods and technologies that can minimize the impact if an adverse event occurs. Federal departments and agencies have been instructed to work with state and local governments, and with the private sector to accomplish the objectives laid out in this directive, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1144956,00.html, Web page accessed February 2009.
3. NERC Standards CIP-002 through CIP-009, http://www.nerc.com/page.php?cid=2|20, May 2006.

   CIP-002-1 – Cyber Security – Critical Cyber Asset Identification

   CIP-003-1 – Cyber Security – Security Management Controls

   CIP-004-1 – Cyber Security – Personnel and Training

   CIP-005 -1 Cyber Security – Electronic Security perimeter(s)

   CIP-006 -1 Cyber Security – Physical Security of Critical Cyber Assets

   CIP-007 -1 Cyber Security – Systems Security Management

   CIP-008 -1 Cyber Security – Incident Reporting and Response Planning

   CIP-009 -1 Cyber Security – Electronic Recovery Plans for Critical Cyber Assets.
4. Energetics Incorporated, "Roadmap to Secure Control Systems in the Energy Sector," January 2006.
5. INL, "Cyber Security Procurement Language for Control Systems," INL/EXT-06-11516, http://www.msisac.org/scada/documents/4march08scadaprocure.pdf, February 2008.