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

AGA 12, Part 2 Performance Test Plan

Mark Hadley, Kristy Huston
Pacific Northwest National Laboratories

November 2006

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

Acknowledgements

The authors wish to thank Bill Rush and Aakash Shah of the Gas Technology Institute as well as the members of the NERC Control Systems Security Working Group and Sandia National Laboratory for their contributions towards the development of this test plan.

EXECUTIVE SUMMARY

Under the guidance and sponsorship of DOE's Office of Electricity Delivery and Energy Reliability, Pacific Northwest National Laboratory (PNNL) developed a test plan for AGA 12, Part 2 compliant devices. The test plan covers the following elements of performance and security.

- Performance (Telemetry, Control, and Polling Cycle) Tests
- Interoperability Tests
- Failover Tests
- Stress Tests

This test plan is intended to be usable in the future to test compliance of devices to the AGA 12, Part 2 Standard and to evaluate impact on a utilities operation.

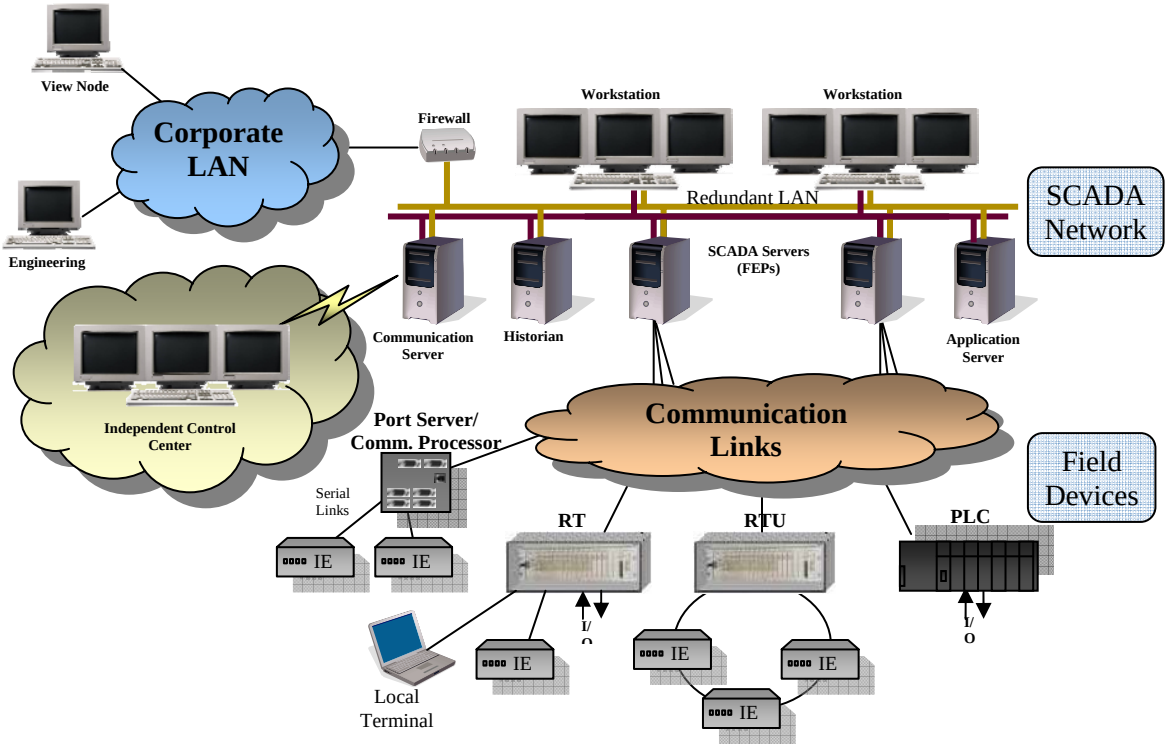
Three manufacturers of SCADA Cryptographic Modules (SCMs) agreed to submit their devices for testing.

- Safenet Mykotronx
- Thales eSecurity, Inc.
- Schweitzer Engineering Laboratories

TABLE OF CONTENTS

1. INTRODUCTION

Electric utilities utilize Supervisory Control and Data Acquisition (SCADA) or similar networks to monitor and manage electric distribution, transmission, and generation environments. The following diagram depicts a typical electric distribution environment used in the design of this test plan.



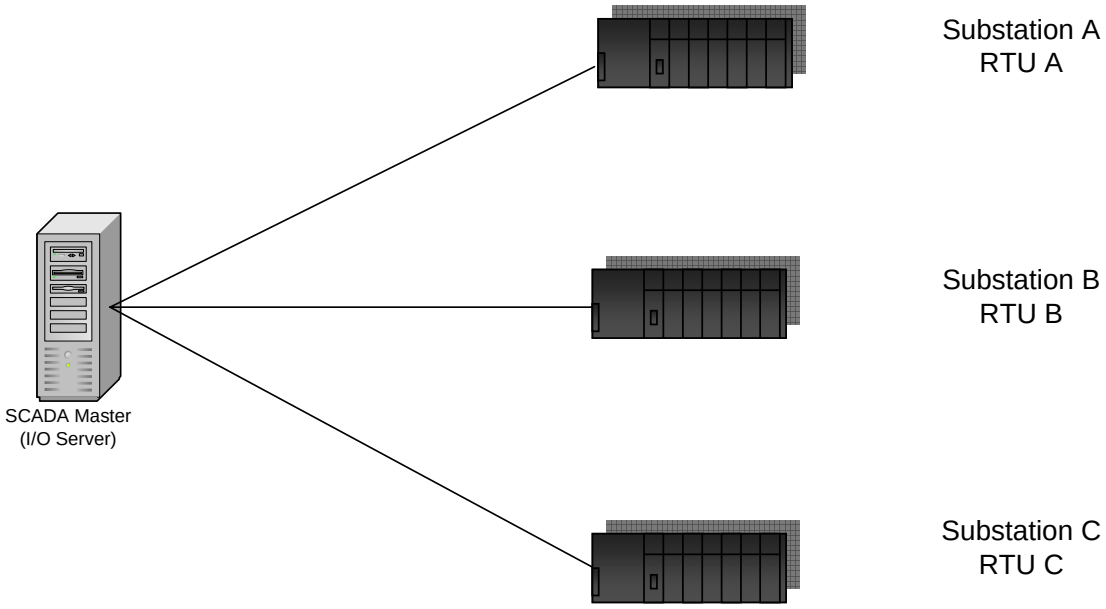
The SCADA Network is implemented in a redundant manner for larger utilities, and multiple types of Communication Links are used to network the control center to remote sites. Typical communication methods include analog or digital leased lines, SCADA radio, microwave, fiber, or dialup modems. The SCADA equipment and protocols were designed and implemented with availability and personnel safety in mind, and as a result security was not a consideration. Since the events of September 11th, it has become apparent that this approach leads to serious cyber vulnerabilities for our nation's SCADA infrastructures. The American Gas Association (AGA) 12-1 guideline addresses the need for increased cyber security of SCADA networks and introduces cryptographic modules (CM) to secure communication channels.

However, before introducing performance test methods, a discussion of SCADA in the electric sector is needed. The function of gathering data is known as telemetry, and this typically is performed in time-slice or round-robin configurations. In the time-slice model, a database or configuration file is used to manage the frequency various types of data are requested from a remote site. Each time slice may include a request for more than one type of data; for example status, analog, or accumulator. The following diagram depicts a two second time slice telemetry scheme. In this sample, type 1 data is requested every two seconds and type 2 data once per minute. At time slice 48, a delay of 100 MS is used between requests for the two types of data. SCADA protocols frequently contain the ability to retry communication if a response to a request is not received within expected time constraints. Time slice telemetry schemes do not utilize that function since the database is used to strictly control communication.

Relative Timing of Telemetry Requests

Function	Time Slice																													
	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58
Type 1	X		X		X		X		X		X		X		X		X		X		X		X		X		X		X	
Type 2																									X					

In a round-robin telemetry scheme, information from each remote device is requested in sequence and is depicted in the following diagram.



In this round-robin telemetry scheme, the Master first polls Substation A. After receiving the response from Substation A, Substation B is polled. Likewise, after the response is received from Substation B, Substation C is polled. After the response from Substation C is received, the process is repeated.

One final aspect of SCADA environments to consider is the communication rate. While the SCADA network can utilize high-speed communication media, it is more common to encounter serial communication in the 1200 to 19200 baud range. Systems are designed to maximize the amount of information that can be reliably transported over the communication media. It is common to find 75 to 80 percent of the band width utilized. Ideally, any security solution will not require the telemetry scheme to be modified or for a significant reduction in the amount of data available for decision making purposes.

2. PURPOSE

The purpose of this test plan is to evaluate the commercial versions of devices built to the American Gas Association (AGA) 12 Part 1 and Part 2 standard in a laboratory setting that simulates an electric utility's distribution environment. A variety of tests will be conducted using a representative assortment of equipment from the electric and gas industries. While both TCP/IP and serial based communication protocols are used in this industry, the focus of the test plan will be on serial communication.
The test plan is written with the following sections. The first section includes requirements and definitions. The second section includes a description of the test environment. The third section contains common elements for all tests, and the fourth section contains specific details about each testing area.

3. REQUIREMENT & DEFINITIONS

In order to measure the impact on latency in a consistent manner, the version of the AGA standard to which the commercial devices are developed should be identical. We will be testing devices to the most recent version of AGA 12 Part 2. The reason for this requirement is that newer versions of the AGA standard include additional data in the header. The addition of a time field, for example, will slightly increase latency. Latency will be calculated by measuring the time a round trip request and associated response take. The round trip will start with the first byte of the request and end with the last byte of the response. The performance of the environment will be measured prior to the introduction of vendor AGA devices. This baseline performance measurement will be used to show the impact upon communication vendor appliances introduce. The same cryptographic algorithms (i.e. AES-128 or SHA-1) will be used by each vendor.

3.1 What is not going to be tested?

Testing will not be done to verify compliance with IEEE Standard 1613-2003, IEEE Standard Environmental Testing Requirements for Communications Networking Devices in Electric Power Substations. We are not formally approving nor certifying any devices, but we will provide results, test environments, and methods for the suite of tests performed.

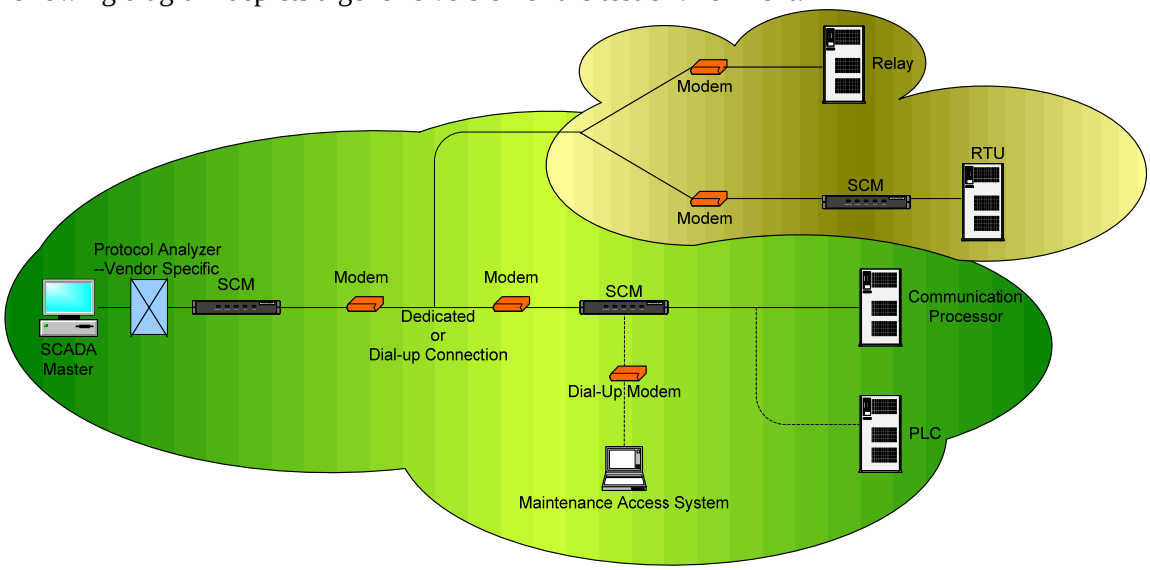
3.2 AGA Report No. 12

The AGA Report 12 (AGA-12) effort is being led by the Gas Technology Institute (GTI) under the auspices of the American Gas Association to establish a recommended practice for providing a secure SCADA system. Additional entities have provided direct financial support or funding of AGA-12 activities including the Federal Government's Technical Support Working Group (TSWG). In addition to being developed for and available to gas utilities, AGA-12 is intended to be available to and useful to other utilities including water and electric utilities.
AGA Report 12 is a series of reports.

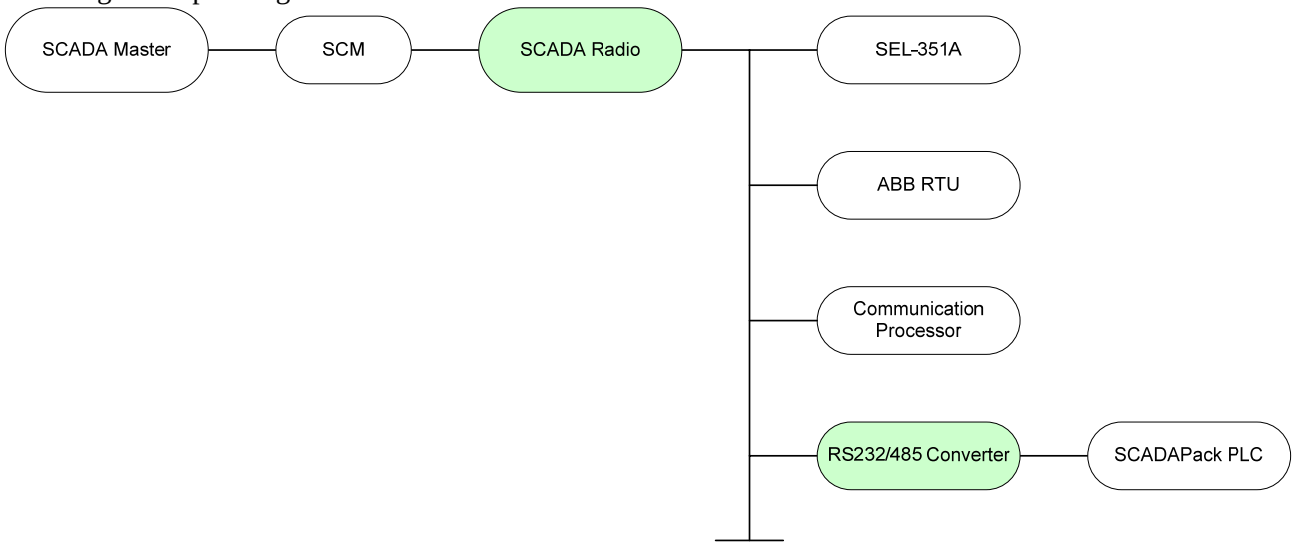
- Part 1 addresses the general recommendations that apply to other documents in the series. It has been widely reviewed and balloted successfully as a recommended practice and the American Gas Association is expected to publish it in early 2005.
- Part 2 address the cryptographic protocol needed to ensure a minimum level of interoperability between cryptographic modules built by different manufacturers and to achieve the performance required for the retrofit solution. We will be conducting tests of vendor devices against the draft version of AGA 12, Part 2.
- Part 3 and Part 4 are future documents that will address the IP-based network solution and the embedded solution respectively.

4. TEST ENVIRONMENT

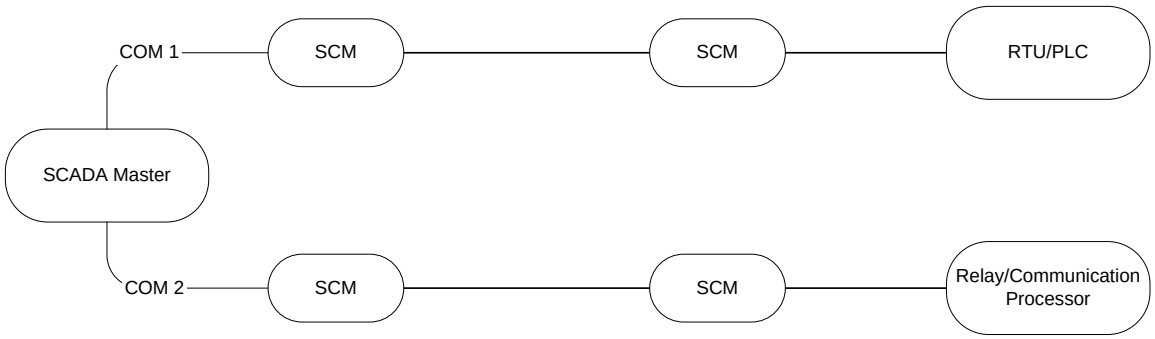
Five devices will be required to perform the full test suite. However, the majority of the tests will only require the use of three SCADA Cryptographic Modules (SCM) from each vendor. For example, failover of a master SCM device in a multi-drop network with three remotes IED's. Most communication in the electric and gas industries are performed over point to point connections, but some multi-drop communication networks are used. The laboratory environment will be based upon feedback from industry. The goal is to provide an environment that represents typical electrical industry installations. Hardware and software from electric industry vendors such as ABB, Areva, and SEL will be used. The following diagram depicts a generic version of the test environment:



This diagram depicts a generic SCADA Radio environment:



This diagram depicts a RS232 test environment:



4.1 Test Equipment

Following test equipment will be used throughout this test plan. If there is additional equipment needed it will be labelled per section.

- LabView / Standard Automation OPC Server
- Modbus Simulator
- Protocol analyzers from ASE-Systems and Frontline Test Equipment (Net Decoder) to decode DNP3, Modbus, and general serial traffic
- InTouch SCADA Master Software
- Triangle MicroWorks Protocol Test Harness and DNP3 simulator environment and SCADA Data Gateway product
- IEDs consisting of representative electric industry hardware from Telvent, SEL, Allen Bradley or other vendor
- WonderWare InControl virtual PLC
- Substation Explorer (for SEL)
- ASE2000 and NetDecoder protocol analyzers
- RS232 / RS485 converters
- Mykotronix
- Schweitzer
- Thales
- Arcom Vipers / Gold Standard
- SEL-351A relay, SEL-421 relay, Sage2300 RTU, and SCADAPack100 PLC
- Null modem cables
- Modems and modem cables
- Analog phone lines
- Wireless modems and modem cables

5. COMMON TEST ELEMENTS

- Testing will be done with length-based (DNP3) and timing-based (Modbus) protocols. Other protocols, such as Conitel, will be added as funding and time allow.

- Point-to-point serial connections will be implemented with null-modem cables, leased lines, and SCADA Radio modems.
- Multi-drop serial communications will be used with at most four remote nodes with wireless modems.
- Timed polling intervals:
  - 1 second
  - 2 seconds
  - 3 seconds
  - 5 seconds
- Round-robin polling where devices are polled in sequence with no timed delay between a response and the next request.
- Functionality tests run at:
  - 1200 baud
  - 2400 baud
  - 4800 baud
  - 9600 baud
  - 19200 baud
- Stress tests will measure the maximum throughput of the devices over serial communication channels as well as measure the smallest, most frequent polling rate possible at each baud rate.
- Each supported AGA Cipher Suite will be tested to measure the latency the different methods introduce to communication. The amount of data introduced by the hashing algorithms is configurable and will be held constant across cipher suites.
- Mixed-mode operation, where some remote IED's are protected by SCM's and others are not, will not be tested.
- Broadcast communication will be tested if supported by all vendor equipment.
- Data from each test will be gathered in a consistent manner and repeated to verify accuracy.
- Various communication methods within the protocol will be tested. For example, acknowledgement of user data and report by exception modes will be enabled for DNP3.
- Each test will be repeated with each vendor's solution.
- The term IED is used to indicate a serial device such as a relay, remote terminal unit, or programmable logic controller for simplicity.

5.1 Result Details

For each of the result sections the following will be captured:

- Approximate geographic distances between components.
- Communications protocols used on various links
- Make, model and/or type of the different kinds of communications equipment
- Version of the AGA standard supported by the vendor hardware
- Use of custom connectors and/or Null modems

- Host controller information
  - Make, Model, Processor and Operating System
  - Real-time control system host software used
- Slave device information (if applicable)
  - Make, model and/or type of all secured slave devices
- Communication parameters on various links
  - Baud rate
  - Stop bits
  - Parity bits
  - Full/half duplex
  - Flow control
  - Are communications parameters negotiated or ever changed?
- Any specific operating modes of the real-time control system
- Polling scheme (master poll, report-by-exception, etc.), timeouts, and polling rates (e.g. poll every second, as fast as possible, etc.)
- Types of polls and responses and average lengths. If the set of polls is recurring, record the poll/response lengths. If possible note the slave processing time for each poll the actual clear text commands and responses will be captured.

6. BASELINE TESTS

6.1 Introduction

Prior to measuring the impact commercial AGA devices have upon SCADA communication, normal communication times need to be identified for each protocol, baud rate, and device (relay, RTU, PLC) using a variety of telemetry and control commands. The purpose is to provide the baseline measurements without cryptographic hardware devices from which additional latency can be measured.

6.2 Background

The communication characteristics for “normal” operation needs to be identified before impacts upon communication can be measured. For example, one RTU may take 250 MS to process a request and prepare a response while another RTU may take 150 MS. These times need to be identified to accurately measure the amount of time a “round trip” communication takes. The baseline measurements need to be repeatable.

Two types of measurements will be recorded. The first will measure the amount of time a round-trip request and response take for both telemetry and control commands. The second will measure the number of polling cycles that can be completed over a given time duration. For reporting purposes, these results will be normalized to polling cycles per hour. All traffic will be captured for analysis and reference using a protocol analyzer. Additionally, degradation over time and normal traffic loss will be examined by repeating tests for longer durations of time.

6.3 Test Procedures

The communication configurations used in the baseline tests are patterned after the various environments implemented in electrical SCADA systems. The test steps identified below will be run over point to point

(RS232) and SCADA Radio communication environments. Telemetry tests will be conducted according to the scheduled intervals and round-robin methodologies described in section 4. Finally, the tests will be conducted over null-modem, dialup, and wireless communication networks. The data collection charts at the end of the test plan have been created for each combination of serial communication, polling methodology, and communication media as a reminder to the tester that all of the communication configurations should be tested.

6.3.1 Baseline Telemetry Test

6.3.1.1 Description

This test will measure the amount of time needed for both DNP3 and Modbus telemetry requests and associated responses at each baud rate indicated in section 4 over a null-modem connection.

6.3.1.2 Test setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the amount of time a round trip polling cycle requires. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate, the data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with the null modem environment, they will be run again using dialup and wireless modem configurations.

6.3.1.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which telemetry function(s) will be used and document the selection.

d. Configure the SCADA Master to initiate the telemetry requests.

e. Using the protocol analyzer, calculate the length of the telemetry request in bytes. Note that this is not the value of the length field in the DNP3 header, for example.

f. Calculate the time required to transmit the request in MS for the baud rate in use.

g. Using the protocol analyzer, calculate the length of the telemetry response in bytes.

h. Calculate the time required to transmit the response in MS.

i. Using the captured data, identify the time necessary for the polling cycle to complete and calculate the time required for the IED to process the request. This is round trip time minus the time from step F minus the time from step H.

j. Repeat steps e – i 3 more times to verify the IED processing time.

    a. Perform steps a through j for:

        1. Null modem environments.

        2. Leased line connections.

        3. SCADA Radio connections.

6.3.2 Baseline Control Test

6.3.2.1 Description

This test will measure the amount of time needed for both DNP3 and Modbus control requests and associated responses at each baud rate indicated in section 4 over a null-modem.

6.3.2.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the amount of time a round trip polling cycle requires. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate, the data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems.

6.3.2.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which control function(s) will be used and document the selection.

d. Configure the InTouch SCADA Master to initiate the control request.

e. Using the protocol analyzer, calculate the length of the control request in bytes. Note that this is not the value of the length field in the DNP3 header, for example.

f. Calculate the time required to transmit the request in MS for the baud rate in use.

g. Using the protocol analyzer, calculate the length of the control response in bytes.

h. Calculate the time required to transmit the response in MS.

i. Using the captured data, identify the time necessary for the polling cycle to complete and calculate the time required for the IED to process the request. This is round trip time minus the time from step F minus the time from step H.

j. Repeat steps e – i 3 more times to verify the IED processing time.

    a. Perform steps a through i for:

        1. Null modem environments.
        2. Leased line connections.
        3. SCADA Radio connections.

6.3.3 Baseline Polling Cycle Test

6.3.3.1 Description

This test will measure the number of polling cycles that can be completed for both DNP3 and Modbus telemetry requests and associated responses at each baud rate and polling frequency indicated in section 4 over both null modem, dialup, wireless connections. The captured data will be analyzed to identify the amount of traffic typically lost at each baud rate and polling frequency combination. Two baseline duration tests will be run. The first test will provide an accurate measurement for the number of telemetry requests and responses that can be completed in one hour. The 48-hour duration test will provide the stability baseline information and will provide the baseline for degradation over time measurements.

6.3.3.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems.

6.3.3.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which telemetry function(s) will be used and document the selection.

d. Configure the InTouch SCADA Master to initiate the telemetry request.

e. Using the protocol analyzer, capture traffic for one hour.

f. Analyze the traffic to determine the normal failure rate and polling cycles per hour.

g. Perform steps a through f for:

    1. Null modem environments.
    2. Leased line connections.
    3. SCADA Radio connections.

h. Repeat step e, only once, for 48 hours using a typical baud rate, polling interval, and communication network for your organization.

6.4 Baseline Test Results

- Excel Spreadsheet with summary test results, attached.

7. PERFORMANCE TESTS

7.1 Introduction

The purpose of SCM tests of a real-time process control system with cryptographic protection is described. These tests are to determine the impact of commercial SCM's on the functionality of a real-time SCADA system used in an electrical distribution environment. We will be conducting telemetry, control and polling tests with multiple vendors SCM's in place.

7.2 Background

SCM testing examines the extent to which your real-time control system hardware and software meet expected performance requirements. Examining the difference between the baseline measurements and the measurements with SCM's in place will provide latency data.

7.3 Test Procedures

The communication configurations used in these tests are patterned after the various environments implemented in electrical SCADA systems. The test steps identified below will be run over point to point (RS232) and SCADA Radio communication environments. Tests will be conducted according to the scheduled intervals and round-robin methodologies described in section 4. Finally, the tests will be conducted over null-modem, dialup, and wireless communication networks. The data collection charts at the end of the test plan have been created for each combination of serial communication, polling methodology, and communication media as a reminder to the tester that all of the communication configurations should be tested.

7.3.1 Telemetry Test

7.3.1.1 Description

This test will measure the amount of time needed for both DNP3 and Modbus telemetry requests and associated responses at each baud rate indicated in section 4 over both null-modem and dialup connections. Monitor and record the time it takes to request a command, acknowledge the command, and the response to the command for each baud rate and polling cycle.

7.3.1.2 Test setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the amount of time a round trip polling cycle requires. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate, the data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems.

7.3.1.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which telemetry function(s) will be used and document the selection.

d. Configure the InTouch SCADA Master to initiate the telemetry request.

e. Using the protocol analyzer, calculate the length of the telemetry request in bytes. Note that this is not the value of the length field in the DNP3 header, for example.

f. Calculate the time required to transmit the request in MS for the baud rate in use.

g. Using the protocol analyzer, calculate the length of the telemetry response in bytes.

h. Calculate the time required to transmit the response in MS.

i. Using the captured data, identify the time necessary for the polling cycle to complete and calculate the time required for the IED to process the request. This is round trip time minus the time from step F minus the time from step H.

j. Repeat steps e – i 3 more times to verify the IED processing time.

    a. Perform steps a through i for:

        1. Null modem environments.
        2. Leased line connections.
        3. SCADA Radio connections.

7.3.2 Control Test

7.3.2.1 Description

This test will measure the amount of time needed for both DNP3 and Modbus control requests and associated responses at each baud rate indicated in section 4 over a null-modem connection. Monitor and record the time it takes to request an action, acknowledge the action, and then response to the action for each baud rate and polling cycle.

7.3.2.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the amount of time a round trip polling cycle requires. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate, the data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems.

7.3.2.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which control function(s) will be used and document the selection.

d. Configure the InTouch SCADA Master to initiate the control request.

e. Using the protocol analyzer, calculate the length of the control request in bytes. Note that this is not the value of the length field in the DNP3 header, for example.

f. Calculate the time required to transmit the request in MS for the baud rate in use.

g. Using the protocol analyzer, calculate the length of the control response in bytes.

h. Calculate the time required to transmit the response in MS.

i. Using the captured data, identify the time necessary for the polling cycle to complete and calculate the time required for the IED to process the request. This is round trip time minus the time from step F minus the time from step H.

j. Repeat steps e – i 3 more times to verify the IED processing time.

    a. Perform steps a through j for:

        1. Null modem environments.
        2. Leased line connections.
        3. SCADA Radio connections.

7.3.3 Polling Cycle Test

7.3.3.1 Description

This test will measure the number of polling cycles that can be completed for both DNP3 and Modbus telemetry requests and associated responses at each baud rate and polling frequency indicated in section 4 over both null modem and dialup connections. The captured data will be analyzed to identify the amount of traffic typically lost at each baud rate and polling frequency combination.

7.3.3.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems.

7.3.3.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

c. Determine which telemetry function(s) will be used and document the selection.

d. Configure the InTouch SCADA Master to initiate the telemetry request.

e. Using the protocol analyzer, capture traffic for one hour.

f. Analyze the traffic to determine the normal failure rate and polling cycles per hour.

g. Repeat steps e and f.

i. Calculate the length of the telemetry request in bytes. Note that this is not the value of the length field in the DNP3 header, for example.

j. Perform steps a through i for:

    1. Null modem environments.
    2. Leased line connections.
    3. SCADA Radio connections.

k. Repeat step e, only once, for 48 hours using a typical baud rate, polling interval, and communication network for your organization.

7.4 Test Results

- Excel Spreadsheet with summary test results, attached.

8. INTEROPERABILITY TESTS

8.1 Introduction

The purpose of this test is to verify the interoperability of SCM's manufactured by different vendors to each other as well as interoperability with the AGA 12 Gold Standard. Interoperability is dependent upon the SCMS supporting the same version of the SCADASafe code. For example, an SCM supporting version 0.67 should interoperate with another SCM running the same version, but interoperability with an SCM running 0.72 will not work given changes in the protocol.

8.2 Background

Some cryptographic module designs adhere to standards that require interoperability. AGA 12 is one such standard. The following excerpt is from AGA 12, Part 1:

> AGA 12 enforces limited cryptographic interoperability by requiring all compliant components to exchange encrypted messages using at least one common cryptographic algorithm, and to exchange session keys using at least one common key exchange method. While operating within one session, AGA 12, Part 1 requires at least one mode in which the shared session key shall, as a minimum, be used for encryption and decryption of SCADA messages between cryptographic modules at the master station and the cryptographic modules at the remote locations.

In such cases, it is important for a real-time control system operator to verify that the cryptographic module indeed conforms to the standard and that it is interoperable. Interoperability tests can be conducted between two different vendor SCM's or between different SCM versions from the same vendor. In the case of AGA 12, a "gold standard" implementation[1] of the AGA 12, Part 2 cryptographic protocol is freely available on the web (http://scadasafe.sf.net). This implementation being in java can be

[1] Also known as the ScadaSafe implementation. This implementation was developed by Dr. Andrew Wright as part of Cisco Systems Critical Systems Assurance Group.

run on virtually any computer system with two serial ports. Tests can then be conducted to prove interoperability between the cryptographic module under test and the "gold standard." The test procedure described below will focus on testing AGA 12 interoperability using the "gold standard" but can easily be generalized for vendor products.

8.3 Test Procedures

The communication configurations used in these tests are patterned after the various environments implemented in electrical SCADA systems. The test steps identified below will be run over point to point (RS232) and SCADA Radio communication environments. Interoperability tests will be conducted according to the scheduled intervals and round-robin methodologies described in section 4. Finally, the tests will be conducted over null-modem, leased line, and wireless communication networks. The data collection charts at the end of the test plan have been created for each combination of serial communication, polling methodology, and communication media as a reminder to the tester that all of the communication configurations should be tested.

8.3.1 Multiple Vendor SCM Interoperability Test

8.3.1.1 Description

A mixture of products from vendors as well as the gold standard will be utilized in this test. Using the various test environments described in section 6, a single vendor solution will be re-configured to include SCMs from another vendor. The test scenarios will replace an SCM at either the master or remote location. The tests will identify basic interoperability and identify any configuration changes necessary for the mixed-vendor environment to operate. Performance in a multi-vendor environment for both DNP3 and Modbus telemetry requests and associated responses will be measured using section 6 as a guide. The captured data will be analyzed to identify any differences in performance, the amount of traffic typically lost at each baud rate and polling frequency combination, and ensure the various AGA modes function correctly. This test requires 3 SCM units from one vendor and one or more from a second. You can also do a 3-way test by incorporating the Gold Standard.

8.3.1.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems. (Shown in Figure 3)

8.3.1.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the SCM's and ensure compatibility between settings such that they could communicate with each other.

c. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

d. Determine which telemetry function will be used and document the selection.

e. Configure the InTouch SCADA Master to initiate the telemetry requests.

f. Verify that both SCM's function in both master as well as slave modes, and interoperability by sending messages back and forth.

g. Using the protocol analyzer, capture traffic for one hour.

h. Analyze the traffic to determine the normal failure rate and polling cycles per hour.

i. Record session negotiation, session timeouts, and session re-establishments.

j. Repeat steps a through f.

8.4 Interoperability Test Results

- Excel Spreadsheet with summary test results, attached.

9. FAILOVER TESTS

9.1 Introduction

The purpose, background and procedure for testing the functionality of the backup/failover system of a network protected by retrofit cryptographic modules are described.

9.2 Background

Many real-time process control networks have a backup/failover system that can be used if a component on the primary communications channel fails. The functionality of this system must be preserved when cryptographic protection is added. Three common types of backup systems exist: hot, warm and cold backups. A hot failover is not currently supported by the standard but may be provided by the vendor implementation. Failover of the SCM's is most accurately categorized as cold or warm, and the following tests will evaluate recovery from failure with that in mind. If hot failover is supported by the vendor, the feature will be tested as well.

The following test procedure will provide a series of simple steps to ensure that the backup system is completely functional once cryptographic protection is introduced.

9.3 Procedures

9.3.1 Vendor Specific SCM Test

9.3.1.1 Description

9.3.1.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems. (Shown in Figure 3)

9.3.1.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the SCM's and ensure compatibility between settings such that they could communicate with each other.

c. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

d. Verify that both SCM's function in both master as well as slave modes, and interoperability by sending messages back and forth.

e. Start telemetry requests.

f. Interrupt communication for 10 minutes to provide enough time for the session keys to become outdated.

g. Record results.

h. Repeat steps a through e.

i. Disable a key component on the primary channel, so the backup system is engaged.

j. Record results.

k. Repeat steps a through e.

l. Pull the power plug on a remote SCM.

m. Record results.

n. Repeat steps a through e.

o. This should be done in a multi-drop configuration with 3 remote nodes. We need to test recovery from a failed master SCM by backing up the configuration, disconnecting the master SCM, restoring the config to the unused SCM, wait 10 minutes, and plug the replacement SCM into the network. The data we capture here will address show us how much time is required to renegotiate multiple sessions simultaneously. This will tell us if the AGA devices will scale.

p. Repeat steps a through e.

q. Force a shift to the backup system.

r. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

s. Repeat steps a through e.

t. Force a shift back to the primary communications channel.

u. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

9.3.2 Multiple Vendor SCM Failover Test

9.3.2.1 Description

9.3.2.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems. (Shown in Figure 3)

9.3.2.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the SCM's and ensure compatibility between settings such that they could communicate with each other.

c. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

d. Verify that both SCM's function in both master as well as slave modes, and interoperability by sending messages back and forth.

e. Start telemetry requests.

f. Interrupt communication for 10 minutes to provide enough time for the session keys to become outdated.

g. Record results.

h. Repeat steps a through e.

i. Disable a key component on the primary channel, so the backup system is engaged.

j. Record results.

k. Repeat steps a through e.

l. Pull the power plug on a remote SCM.

m. Record results.

n. Repeat steps a through e.

o. This should be done in a multi-drop configuration with 3 remote nodes. We need to test recovery from a failed master SCM by backing up the configuration, disconnecting the master SCM, restoring the config to the unused SCM, wait 10 minutes, and plug the replacement SCM into the network. The data we capture here will address show us how much time is required to renegotiate multiple sessions simultaneously. This will tell us if the AGA devices will scale.

p. Repeat steps a through e.

q. Force a shift to the backup system.

r. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

s. Repeat steps a through e.

t. Force a shift back to the primary communications channel.

u. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

9.4 Failover Test Results

- Excel Spreadsheet with summary test results, attached.

10. STRESS TESTS

10.1 Introduction

The purpose of this test is to determine if the commercial AGA can remain functional under stressful conditions as well as measure the maximum throughput the device will support. The communication configurations used in these tests are patterned after the various environments implemented in electrical SCADA systems. The test steps identified below will be run over point to point (RS232) and multi-drop (RS485) communication environments. Tests will be conducted according to the scheduled intervals and round-robin methodologies described in section 4. Finally, the tests will be conducted over null-modem, dialup, and wireless communication networks. The data collection charts at the end of the test plan have been created for each combination of serial communication, polling methodology, and communication media as a reminder to the tester that all of the communication configurations should be tested.

10.2 Background

10.3 Test Procedures

10.3.1 Vendor Specific SCM Test

10.3.1.1 Description

10.3.1.2 Test Equipment

Noise generation equipment from SEL

10.3.1.3 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems. (Shown in Figure 3).

10.3.1.4 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the SCM's and ensure compatibility between settings such that they could communicate with each other.

c. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

d. Verify that both SCM's function in both master as well as slave modes, and interoperability by sending messages back and forth.

e. Start telemetry requests.

f. Decrease polling cycles until communication fails.

g. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

h. Repeat steps a through e.

i. Increase the amount of data processed.

j. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

k. Repeat steps a through e.

l. Increase communication rates.

m. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift. See if it handles flow control and congestion control.

n. Repeat steps a through e.

o. Add additional remote SCM.

p. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

q. Repeat steps a through e.

r. Inject noise into the communication path. This will "stress" the system's ability to communicate.

s. Record results.

10.3.2 Multiple Vendor SCM Performance Test

10.3.2.1 Description

10.3.2.2 Test Setup

The NetDecoder protocol analyzer will be used to capture SCADA traffic in order to accurately measure the number of polling cycles that can be completed on one hour. For each IED and protocol combination, the test steps specified below will be repeated for each baud rate and polling interval. The traffic data will be captured, and summary information entered into a spreadsheet. After the tests are conducted with null modem cables, they will be run again using dialup modems. (Shown in Figure 3)

10.3.2.3 Test Steps

a. Configure the test equipment and ensure it is functioning properly with the desired protocol.

b. Configure the SCM's and ensure compatibility between settings such that they could communicate with each other.

c. Configure the protocol analyzer to decode the specific protocol's traffic and capture the results with millisecond timestamps. The file created during the test will be archived and labelled for easy identification.

d. Verify that both SCM's function in both master as well as slave modes, and interoperability by sending messages back and forth.

e. Start telemetry requests.

f. Decrease polling cycles until communication fails.

g. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

h. Repeat steps a through e.

i. Increase the amount of data processed.

j. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

k. Repeat steps a through e.

l. Increase communication rates.

m. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift. See if it handles flow control and congestion control.

n. Repeat steps a through e.

o. Add additional remote SCM.

p. Record results. Ensure that communication is restored. If the backup system does not automatically poll all the slaves, poll each slave and ensure communication. Perform any other operations related to the backup system and ensure functionality. Also ensure proper communication by polling each slave, if the host system does not automatically do so. Record ALL steps you had to take to complete the shift.

10.4 Stress Test Results

- Excel Spreadsheet with summary test results, attached.

11. DEFINITION OF TERMS

Unless otherwise defined, definitions and acronyms are defined by IEEE 100, "The Authoritative Dictionary of IEEE Standard Terms," Seventh Edition.

Approved security function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either specified in an approved standard, or adopted in an approved standard and specified either in an annex of the approved standard or in a document referenced by the approved standard, or specified in the list of approved security functions.
Authentication	A process that establishes the origin of information, or validates an entity's identity.
Authorization	Access privileges granted to an entity; conveys an "official" sanction to perform a security function or activity.
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
Credentials	The means to associate access and use permission with a cryptographic value.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.
Cryptographic key component (key component)	One of two or more secret numbers that are combined to produce a key using split knowledge procedures.
Cryptographic Module (CM)	The set of hardware, software, and/or firmware contained within a cryptographic boundary that implements approved security functions (including cryptographic algorithms and key generation).
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
Cyber attack	Exploitation of the software vulnerabilities of information technology-based control components.
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
Domain	A grouping of roles, categories, credentials and policies with common security needs.
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key.
Firmware	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Hash function	A function that maps a bit string of arbitrary length to a fixed length bit string. With cryptographic hash functions, it is computationally infeasible to find any input that map to a pre-specified output, and It is computationally infeasible to find any two distinct inputs that map to the same output.
Intelligent Electronic Device (IED)	Any device incorporating one or more processors capable of receiving or sending data/control from/to an external source (e.g., electronic multifunction meters, digital relays, controllers).
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Maintenance port	The physical access mechanism (interface) on an IED or RTU through which a maintenance engineer can access data, and access or change settings and programs with the IED or RTU. The port is typically RS-232 (a standard for asynchronous serial data communications). The access may be controlled by several levels of passwords, For remote access via dial-up phone lines; an external or internal automatic answering modem is required.
Mixed mode	Pertaining to a communication arrangement where some devices on a shared communication channel are protected by cryptographic modules and some are not.
Multidrop	Pertaining to a communication arrangement where several devices share a communication channel. See [3]
Non-repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.
Operator (SCADA)	An individual in the utility control center that is responsible for on-line SCADA system control.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Plaintext	Unencrypted data with format additions or changes, such as framing or padding.
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Slave	A device that gathers data or performs control operations in response to requests from a master and sends response messages in return. It may also generate unsolicited responses.
Substation or station	The term, including its qualifier, is used to generically address all remote sites housing devices that control transmission and distribution of gas, electricity, water, wastewater, etc. Examples are electric power substations, pumping stations, compressor stations, and gate stations.
Supervisory control data acquisition system (SCADA and automatic control)	A system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station). The supervisory system may be combined with a data acquisition system, by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions.
Threat	Any circumstance or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure,

	modification of data or denial of service.
Throughput	The total capability of equipment to process or transmit data during a specified time period.
Utility	A generic term that, when qualified, identifies the business entity including all its operating and business functions; e.g., electric utility, gas utility, water utility, wastewater utility, pipeline utility.
Vulnerability	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

11.1 Definition of Acronyms

AES	Advanced Encryption Standard
AGA	American Gas Association
ALU	Arithmetic Logic Unit
AU	Address Unit
bps	bits per second
CKM	Cryptographic Key Management
CM	Cryptographic Module
CPU	Computer Processing Unit
CS	Cipher State
CTS	Clear To Send
DCE	DATA Communication Equipment
DHS	Department of Homeland Security
DMA	Direct Memory Access
DMS	Distribution Management System
DNP	Distributed Network Protocol
DOE	Department of Energy
DMA	Direct Memory Access
DSP	Digital Signal Processor
DSR	Data Set Ready
DTR	Data Terminal Ready
DTE	Data Terminal Equipment
DU	Data Unit
EMS	Energy Management System
FEP	Front End Processor
GTI	Gas Technology Institute
HSARPA	Homeland Security Advanced Research Project Agency
ID	Identification
IED	Intelligent Electronic Device
IT	Information Technology
IU	Instruction Unit
Kbps	Kilo bits per second

MCM	Maintenance Cryptographic Module
MPU	Main Processing Unit
PIN	Personal Identification Number
PU	Processing Unit
NETL	National Energy Technology Laboratory
NIST	National Institute of Science and Technology
RBAC	Role-based Access Control
RTS	Ready To Send
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCM	SCADA Cryptographic Module
SCMS	Secure Cryptographic Management System
SDK	Software Development Kit
SSDL	SCADA Security Development Laboratory
SSPP	Serial SCADA Protection Protocol
TI	Texas Instrument
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
WAN	Wide Area Network

12. REFERENCES

[1] AGA Report No. 12: Cryptographic Protection of SCADA Communications, Part 1, Background, Policies, and Test Plan.

[2] AGA Report No. 12: Cryptographic Protection of SCADA Communications, Part 2, The Retrofit Solution.

[3] E. Anderson, C. Beaver, T. Draelos, R. Schroeppel, M. Torgerson, "Manticore and CS Mode: Parallelizable Encryption with Joint Cipher-State Authentication," Sandia Report SAND2004-5113, October, 2004. Published in the Proc. of the 9th Australasian Conference on Information Security and Privacy (ACISP 2004), LNCS 3108, Springer-Verlag, July, 2004 as "ManTiCore: Encryption with Joint Cipher-State Authentication."

[4] IEEE 100 Authoritative Dictionary of IEEE Standard Terms, Seventh Edition.

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

doe.energy.gov/randd/css.htm