PNNL-17117

Pacific Northwest
National Laboratory
Operated by Battelle for the
U.S. Department of Energy

AGA-12, Part 2 Performance Test Results

M.D. Hadley
K.A. Huston
T.W. Edgar

August 2007

Prepared for
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

AGA-12, Part 2 Performance Test Results

M.D. Hadley
K.A. Huston
T.W. Edgar

August 2007

Prepared for
the U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

The Pacific Northwest National Laboratory (PNNL) was tasked to evaluate the performance of devices conforming to the American Gas Association 12 (AGA-12), Part 2 standard as a contribution to the U.S. Department of Energy's National Supervisory Control and Data Acquisition (SCADA) Test Bed Program. The method of investigation used in this task was based on the AGA-12, Part 2 Performance Test Plan.

AGA-12 is designed to be a four part standard. Part 2 is the technical description of the serial SCADA protection protocol (SSPP) for cryptographically protecting existing serial SCADA communications. Part 2 is the technical standard to which vendors and developers would build an AGA-12 compliant cryptographic module. In addition, it identifies the various operating modes for the SSPP, the SSPP protocol layers, and the additional information that will be added to the original SCADA message to encrypt and provide message authentication. It is this additional information that adds latency, i.e, delay, to serial communications.

While the gas industry and the electric industry both use SCADA systems, the manner in which they are used differs dramatically. Common telemetry schemes in the gas industry request information from remote sites typically every 60 to 90 seconds. Telemetry environments in the electric industry collect more data more frequently. It is common in the electric industry to make multiple requests every 2 to 4 seconds.

The purpose of the performance tests undertaken in this task was to measure vendor products developed to the AGA-12 standard, when operated in SCADA environments patterned after those of the electric industry. This report presents performance test data to assist other organizations evaluating AGA-12 technology, but does not attempt to quantify whether the performance will be acceptable for their particular application.

The performance test identified that all AGA-12 vendor devices add latency to the transmission of SCADA communications. The impact is greatest in low-bandwidth environments with frequent telemetry requests. In addition, the performance impact is greater on timing-based protocols (such as Modbus) than length-based protocols (such as distributed network protocol DNP3). In round-robin telemetry environments, this impact cascades across requests, accumulating additional latency for each request and response pair.

The manner in which control commands function differs by SCADA protocol. The use of AGA-12 vendor devices will impact the amount of time required for a control command to be enacted by the field device. This increase in time should be carefully considered by each respective user organization when evaluating the application of AGA-12 devices.

Acknowledgements

The authors extend their gratitude to the following individuals and organizations for their assistance in developing the AGA-12 test plan, providing cryptographic modules to be tested, and providing technical support during testing activities.

North American Electric Reliability Corporation (NERC) Control Systems Security Working Group
Paul Blombgren, SafeNet Mykotronx
Juan Asenjo, Thales e-Security
Bill Rush and Aakash Shah, Gas Technology Institute
Dr. Andrew Wright, Cisco

Acronyms and Definitions

Acronym	Definition
AES	Advanced encryption standard specified in FIPS PUB 197
AGA	American Gas Association
CM	Cryptographic module
CTR	Counter (as used in the block cipher function)
CTS	Clear to send
DNP	Distributed network protocol
FD	Field devices
GTI	Gas Technology Institute
I/O	Input/output
HMAC	Keyed-hashed message authentication code
NERC	North American Electric Reliability Corporation
PCPH	Polling cycles per hour
PE	Position embedding
PLC	Programmable logic controller
PNNL	Pacific Northwest National Laboratory
RSD	Relative standard deviation
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SCM	SCADA cryptographic module; used interchangeably with CM
SHA	Secure hash algorithm
SSPP	Serial SCADA protection protocol

SQL	Structured query language
USB	Universal serial bus

Contents

Figures

Tables

1.0 Introduction

The Pacific Northwest National Laboratory (PNNL)[1] evaluated the performance of devices conforming to AGA-12, Part 2 as a task in the U.S. Department of Energy's National SCADA Test Bed Program. This report summarizes these performance test results and lessons learned during the testing of vendor devices built to this evolving standard.

1.1 AGA - 12 Background

AGA-12 was developed by and for the oil/gas industry. Compared to the electric power industry, these environments utilize less-demanding telemetry schemes in their SCADA systems both in terms of the number of requests per hour and the amount of data gathered. The following excerpt from the "**Protecting SCADA Communications Fact Sheet"** (Gas Technology Institute 2004) on the Gas Technology Institute (GTI) web site identifies the purpose of the AGA-12 standard:

The objective of the AGA-12 standard is to secure SCADA communications against possible tampering by terrorists, competitors, or hackers. The goals are to develop the technology to be applicable to most – if not all – SCADA communication systems.

Additional insight is provided by the following extract from AGA-12, Part 1: Cryptographic Protection of SCADA Communications: Background, Policies, and Test Plan:

"In the process of developing the report, the AGA-12 Task Group decided that a comprehensive SCADA encryption methodology required a two-pronged approach starting with the development of a solid foundation of corporate policy for addressing cyber security; followed by the reinforcement of specific procedures necessary for retrofitting cryptographic modules to existing SCADA systems. The group recognized that a comprehensive program required installation of hardware and software that is supported by operating procedures and appropriate corporate policies. Experience shows that if a cryptographic system is compromised, it is more often due to poor policies and operating procedures than to an assault on the cryptographic system itself" (NIST 2002). To implement this methodology and remain in sequence with AGA's other reports, the AGA Task Group decided to split the AGA-12 report into parts and number them as follows:

- AGA-12, Part 1: Cryptographic Protection of SCADA Communications: Background, Policies and Test Plan

[1] Pacific Northwest National Laboratory is a multi-program laboratory operated by Battelle Memorial Institute for the United States Department of Energy under Contract DE-AC05-76RL01830.

- AGA-12, Part 2: Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications

- AGA-12, Part 3: Cryptographic Protection of SCADA Communications: Protection of Networked Systems

- AGA-12, Part 4: Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components

AGA-12, Part 2 is the technical description of the serial SCADA protection protocol (SSPP) for cryptographically protecting existing serial SCADA communications. Currently it is in draft form at revision 0.7.44. It identifies the various operating modes for the SSPP, the SSPP protocol layers, and the additional information that will be added to the original SCADA message to encrypt and provide message authentication. This additional information requirement will add latency to serial communication environments. In particular, Part 2 is the technical standard to which vendors and developers would build an AGA-12 compliant cryptographic module.

1.2 Study Motivation

Industry representatives, asset owners, cryptographic module vendors, the Gas Technology Institute, AGA, and the NERC Control System Security Working Group have all expressed interest in unbiased testing of the performance and cryptographic review of the AGA-12 modules. This knowledge will permit the determination of whether AGA-12 devices could be implemented by the electric power industry in a more demanding communication environment than that of the oil/gas industry for which the AGA-12 standard was designed.

While the natural gas industry and the electric industry both use SCADA systems, the manner in which they are used differs dramatically. Common telemetry schemes in the gas industry request information from remote sites on the order of every 60 to 90 seconds. Telemetry environments in the electric industry collect more data more frequently. It is common in the electric industry to make multiple requests every 2 to 4 seconds.

The introduction of cryptographic modules into a SCADA system will impact its performance. The impact can vary in many different ways and can introduce system configuration problems as well as new points of failure. Issues that need to be addressed include the system impact and consequences of device failures, the types of failure that can occur, the means by which communications can be restored and whether or not failures are predictable. Cryptographic modules can also impact the performance of a SCADA system by introducing latency to communication. Additional issues include how much latency is introduced into a telemetry request and how much longer a control command will take to enact. Situational awareness based on the amount of system data will be reduced in proportion to the amount of system latency introduced.

The AGA-12 links to the roadmap goal to develop and integrate protective measures. The specific milestone is widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost effective to deploy. More information is available at http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secuire_Control_Systems_in_the_Energy_Sector.pdf

1.3 Report Organization

The purpose of this report is to present performance test data to assist organizations evaluating AGA-12 technology and does not attempt to quantify whether the performance will be acceptable for their particular application. The following test results do not include vendor names; the results have been redacted. A consistent naming convention is used from this point forward. The term SCADA cryptographic module (SCM) is used interchangeably with cryptographic module (CM). The products of different vendors are indicated numerically. Thus, SCM-1 refers to cryptographic modules from one vendor and SCM-2 represents those of the other vendor. Likewise, FD-1, FD-2, and FD-3 represent field devices (FDs) used in the tests.

The intended audience for the report includes asset owners, industry groups, and vendors. The desired response by industry would be collaboration to improve findings, discussion regarding the appropriate and acceptable use of cryptographic solutions, and testing of new and enhanced products in the future.

This report is written for two audiences with differing technical expertise. After common Introduction and Approach sections, results are divided into High-level Results and Detailed Results segments. The High-level Results segment provides general information regarding the performance impact of AGA cryptographic modules upon serial SCADA communication patterned after the electric industry. The Detailed Results segment provides greater depth and views into baseline and cryptographically protected communication. Finally, a Performance Summary section concludes the report.

2.0 Approach

The method of investigation was based on the AGA-12, Part 2 Performance Test Plan. This plan provides detailed instructions for placing protocol analyzers to measure communication performance, conducting baseline tests to measure normal serial communication characteristics, and placing the AGA-12 cryptographic modules. The telemetry environments identified in the test plan are based upon those used in electric utilities. The protocols, communication media, and communication rates are all indicated in the test plan. In addition, the unit of measure "polling cycles per hour" (PCPH) is defined as a measure of the number of telemetry requests and responses that can be complete within a 60-minute period. This new unit of measure is used to provide a cumulative insight into the impact cryptographic modules have on data visibility.

The measurement of field device variability provided is based on repeated sampling of the same registers/object on the same field device using the same communication media, baud rate, protocol, and telemetry request. Tests were repeated at different times, and random samples were taken to ensure that a bias in results was not reported. The repeated tests showed little variability from one test to another. Given this apparent consistency of field device communication behavior, the estimate of variability is calculated from one data set sample to all data sets.

Key points of the test procedure are:

- Establish baseline to determine the time required for a single request and response to complete

- Establish baseline to determine the number of polling cycles per hour that can be completed

- Introduce AGA-12 cryptographic modules into the SCADA environment

- Measure the time required for the identical request and response to complete

- Identify any increase in the time.

The test facility at PNNL used to conduct the performance tests was comprised of the following hardware, software, and telemetry equipment:

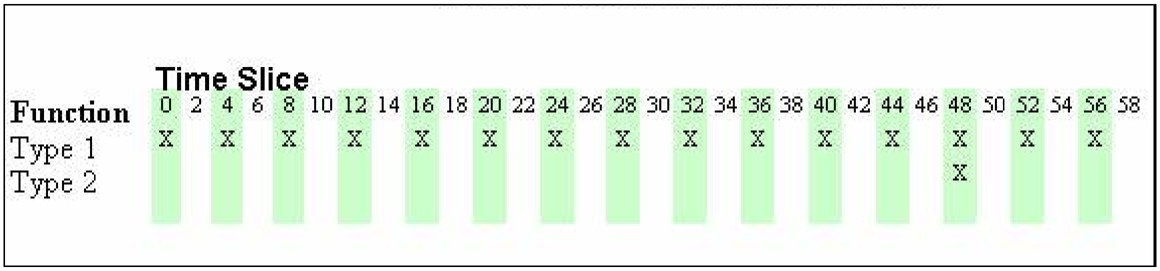
- NetDecoder protocol analyzer software, cables, and serial adapters
- Null-modem cables
- MultiTech MultiModem-IND MT5634IND analog
- SCADA Radios ELPRO 905U-D 900 MHz unlicensed
- Triangle MicroWorks SCADA Data Gateway
- Wonderware

- Dell PowerEdge 1850
- SEL-351A relay
- SCADAPack 100 programmable logic controller (PLC)
- Sage2300 remote terminal unit (RTU).

This equipment was operated at communication rates of 1200, 2400, 4800, 9600, and 19,200 baud and polling frequencies of 1, 2, 3, and 5 seconds.

2.1 Telemetry Scenario

Figure 1 illustrates a typical telemetry environment for the electric power industry. The environment implemented for the performance testing was patterned after this approach. It should be noted that at relative time slice 48, a 100-mS delay is used between requests. Telemetry differs between the electric industry and the gas/oil industry. The electric industry typically gathers more data points more frequently, and the timeliness of information is more critical for supporting situation awareness in the control room.



	Time Slice																													
Function	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					

Figure 1. Relative timing of telemetry requests

For the PNNL performance testing activities, two types of data were requested. At 1-, 2-, 3-, or 5-second intervals, DNP Class 1 or Class 3 data was requested, and at 5-minute intervals, DNP Class 0 data was requested.[2] For Modbus, three separate registers were requested during each time-slice interval. The ability to request the equivalent of DNP's Class 0 data is not available for the Modbus protocol. Round-robin tests were conducted using multiple serial ports instead of one because of limitations in vendor SCMs and the DNP input/output (I/O) server software.

2.2 Differences Between Planned and Actual Tests

The original test plan contained several tests that could not be conducted with available hardware and software products. Where possible, a new testing methodology was

[2] Class data is determined within the Outstation. Class 0 is reserved for static data objects (static data reflects the current value of the data in the Outstation). Classes 1, 2, and 3 are reserved for event data objects (objects created as a result of data changes in the Outstation or some other stimulant). The user can determine which data objects are associated with each class.

implemented to conduct the tests. By utilizing the vendor-provided partial implementation of the standard in this analysis, we cannot definitively determine the comprehensive impact upon communication. Details of the actual testing are as follows:

- Both SCM-1 and SCM-2 devices only support a subset of the cipher suites in the AGA-12, Part 2 guideline to be used for securing the transmission of data. Both vendors support:

    - 1) Cipher suite 1 operating in counter- (CTR-) mode with holdback. This suite uses a 128-bit advanced encryption standard (AES) key and CTR-mode in the encryption of the SCADA message as well as a secure hash algorithm (SHA-1) keyed-hashed message authentication code (HMAC) for authentication and error detection

    - 2) Cipher suite 2 operating in position embedding- (PE-) mode with no holdback. This suite uses a 128-bit AES key and PE-mode in the encryption of the SCADA message as well as a SHA-1 HMAC for authentication and error detection.

    - 3) Cipher suite 3 (hash only). This suite uses a SHA-1 hash on the data. These cipher suites provide no data privacy or authentication; only error detection is provided. Consequently, only cipher suites 1 and 2 were included in the testing.

  Each cipher suite and HMAC mode defined in the Part 2 standard may introduce different amounts of latency into SCADA communications. A complete view of the potential latency impact is not available as a result of limited vendor implementation.

- SCM-1 devices do not support point to multi-point round-robin SCADA radio configurations for the DNP protocol. Two serial ports were used to simulate the environment one would encounter during typical point to multi-point environments.

  One testing objective was to utilize SCADA radio or RS-485 networks to replicate a common industry implementation of point to multi-point communication configurations. In these environments, a single communication port on the SCADA I/O server is associated with multiple remote devices. Because vendor products were limited, multiple communication ports on the I/O server were utilized to simulate industry implementations. The test results were not adversely impacted by this limitation.

- SCM-1 devices would not function at 1200 baud in the test environment.

  By not supporting the complete bandwidth test range, vendor SCM-1 devices could not be completely tested. While data is missing, the impact upon the report is minimal. The latency impact tends to be liner in nature, implying that a good estimate will be to double the latency measured at 2400 baud.

- Interoperability between SCM-1 and SCM-2 devices could not be tested because each vendor built their device to a different version of the evolving AGA-12, Part 2 standard.

  Interoperability testing between vendor products could not be completed because vendor products were built to different versions of the AGA-12 Part 2 standard. However, each vendor product successfully interoperated with the AGA-12 Gold Standard[3] built to an identical version of the standard. This work demonstrated that each vendor accurately implemented the AGA-12 version to which their product was built. The authors anticipate that vendor product interoperability would occur if strict adherence to the AGA-12 standard was followed. The impact on the test report is minimal.

- The devices to generate noise onto the communication line were not available as part of stress testing activities.

  Adding noise into the communication channel would identify quality of service issues for AGA-12 vendor products. A noisy communication environment introduces communication problems (missing data) for normal SCADA communications. Noise introduced in the cryptographically protected communication could compound the impact. The lack of this testing does provide a significant adverse impact upon test results.

[3] Arcom Viper Gold Standard is a test platform for ensuring interoperability of vendor products. The developers of the AGA-12 standard also created a software implementation in Java designed to run on the Arcom Viper industrial computer with the Arcom Embedded Linux operating system.

3.0 High-Level Results

Before measuring the impact vendor SCMs have on SCADA communication, a series of baseline tests were conducted per the test plan. Four areas are summarized in this high-level section: 1) impact on a single telemetry request, 2) impact on the number of telemetry requests that can be made during 1 hour, 3) impact on round-robin telemetry environments, and 4) impact on control. Each of the following charts is based on the DNP protocol, given its widespread use in the electric industry. Also note that these results are based on the best performing vendor SCMs for the particular test.

The addition of vendor SCMs will add some latency to a telemetry request and response. The amount of latency is dependent on many factors including baud rate (number of signal level changes per second), original message length, and which AGA-12 cryptographic cipher suite is used. Figure 2 displays the additional milliseconds (mS) of latency added to the transmission time of a typical telemetry request and response at various baud rates. For example, at 2400 baud, 416 mS (or approximately four tenths of 1 second) are added. As the baud rate increases, latency drops to 38 mS in this example.

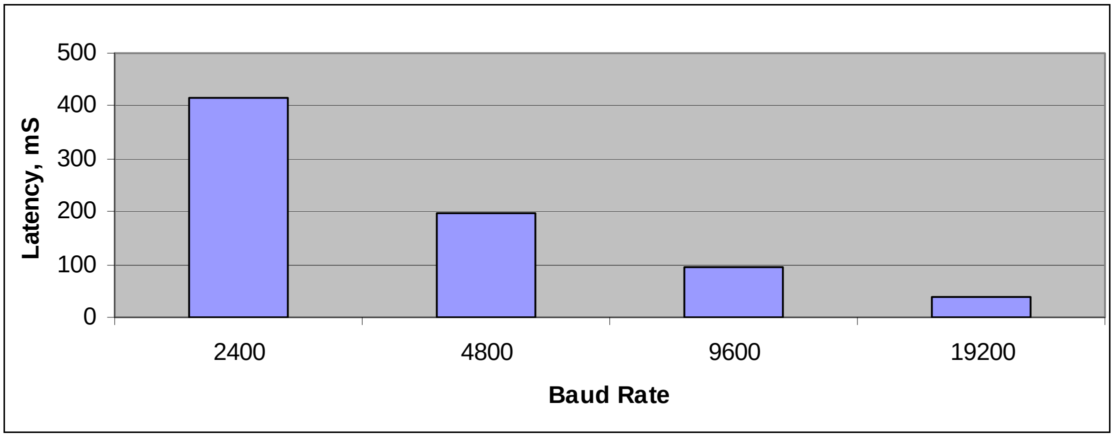


Figure 2. Additional latency for a single telemetry request and response versus baud rate

Time-slice telemetry environments may be impacted when AGA-12 cryptographic modules are introduced. The level of impact is dependent on the amount of unused bandwidth available in the organization’s operational SCADA communication. If ample bandwidth is available, the impact may be negligible. In environments where bandwidth is 70 or 80 percent utilized, a loss of data can be expected. Figure 3 displays this impact by showing the percentage of baseline, or normal, time-slice communication after AGA-12 devices have been added to the communication path for 1 hour. Note that, as the baud rate or time-slice window increases, the impact is less. Each bar represents the percentage of baseline communication. At 1200 baud and 1 second polling, 69% of the baseline telemetry data is received by the I/O server. This improves for our test environment to essentially 100% for the remainder of the time-slice configurations.

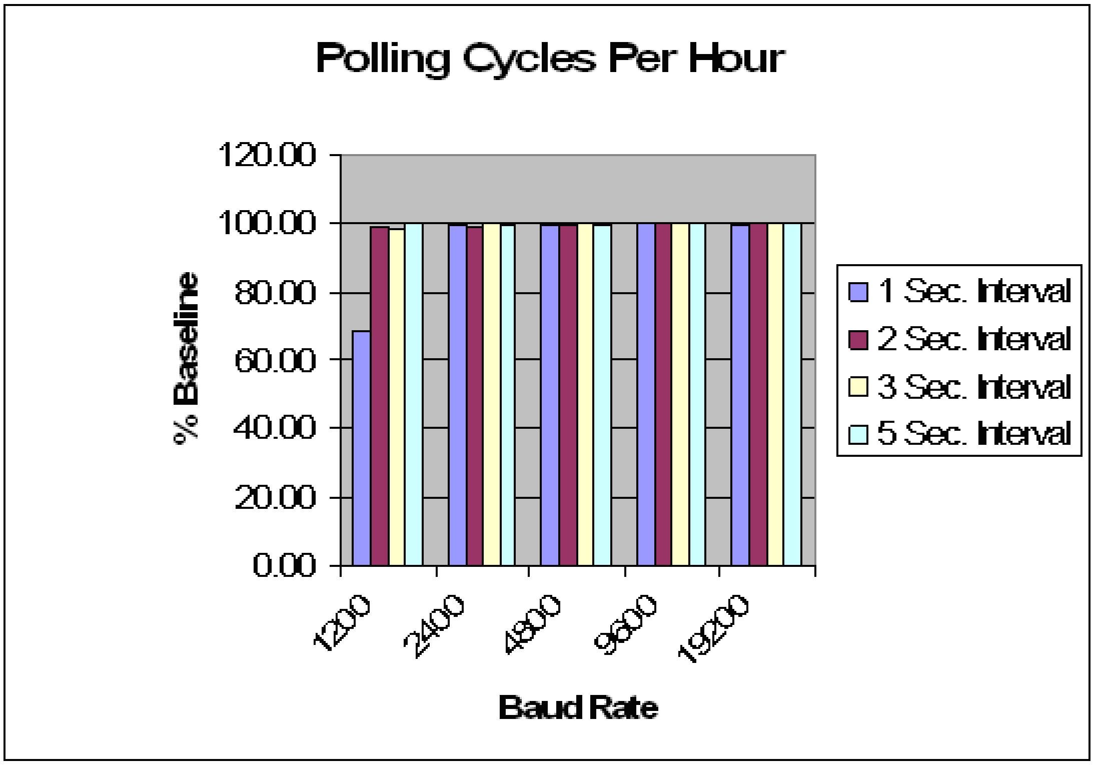


Figure 3. Percent of baseline achieved versus baud rate for a range of polling frequencies

Round-robin telemetry environments will be impacted to a larger extent than time-sliced telemetry environments when AGA-12 cryptographic modules are introduced. The additional time required for each telemetry request and response is magnified over the course of 1 hour, day, or month. Figure 4 displays this impact by showing the percent of baseline, or normal, round-robin communication after AGA-12 devices have been added to the communication path for 1 hour. Note that as the baud rate increases, the impact is less. Each bar represents the percent of baseline communication. At 1200 baud, only 38% of the baseline telemetry data is received by the I/O server. This improves as the baud rate increases to 74% for a communication rate of 19200.

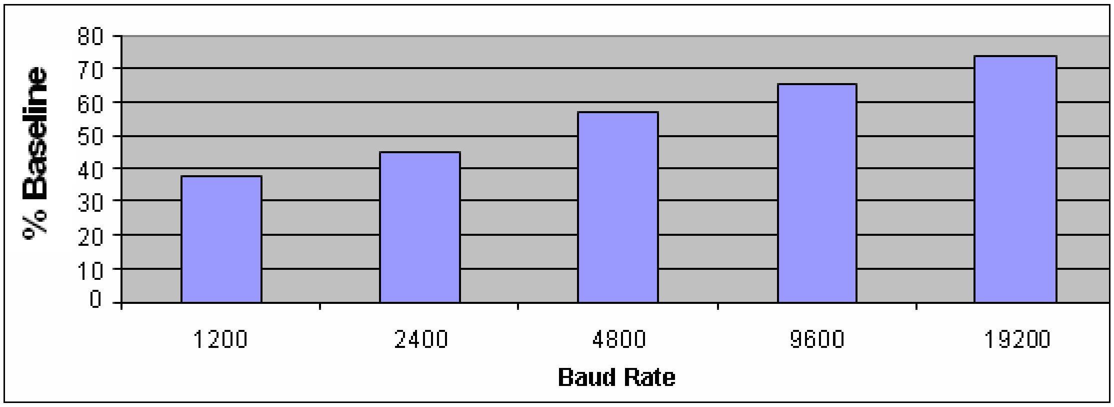


Figure 4. SCM impact on round-robin telemetry as a percentage of baseline versus baud rate

Finally, the impact of AGA-12 cryptographic modules on control messages needs to be explored. Personnel safety and the ability to react quickly to transients on the electric system are of primary concern. The relevant issue is whether AGA-12 devices create delays in the transmission of control messages. Figure 5 illustrates, as with telemetry requests, that the latency increase is dependent primarily upon baud rate. The method used with DNP is called “select before operate”. This method utilizes two messages from the I/O server to enact the change on the field device. At 2400 baud, almost 1 complete second is added to the baseline control time. At 19200 baud, the additional latency is only 62 mS.

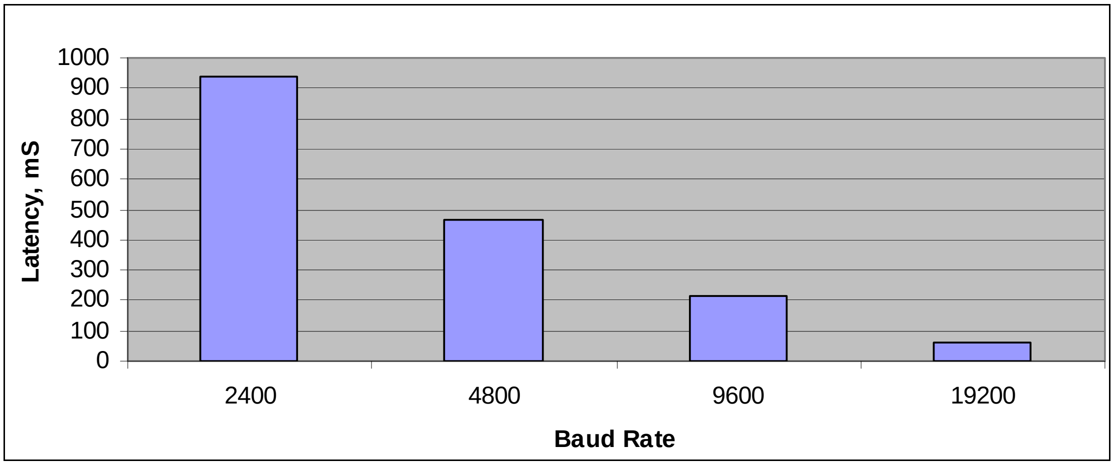


Figure 5. Additional latency in mS versus baud rate for a control request and response

4.0 Detailed Results

The following tables and charts were generated using data from the tests defined above. Data were captured using NetDecoder, Triangle MicroWorks SCADA Data Gateway, or custom applications and were imported into a structured query language (SQL) database and/or Excel for analysis. Instead of including a graph/chart for each test configuration option, a representative sample is included in each category below to illustrate the main findings. The use of multiple charts/graphs to illustrate the same point was determined to be repetitive. Additional reports or views of the test data can be provided upon request.

4.1 Sample Data

Before moving into the analysis section, it is important to discuss the format of the captured data. Each of the methods used to capture data employ a different level of sensitivity. For example, some products create a time stamp for the message, others time stamp each byte of data, and each solution utilizes a different level of sensitivity. Table 1 summarizes the time stamp characteristics of the available methods.

Table 1. Time Stamp Characteristics of Available Methods

Method	Time Stamp Detail	Sensitivity	Notes
SCADA Data Gateway	Message	Millisecond	Generates DNP traffic
NetDecoder	Byte or message	Tenth of a millisecond (1/10000 of 1 second)	Asynchronous serial data was captured and converted to DNP or Modbus to provide more detailed views of the data
Custom Application	Message	Millisecond	Uses Microsoft performance measurement tools for round-robin testing

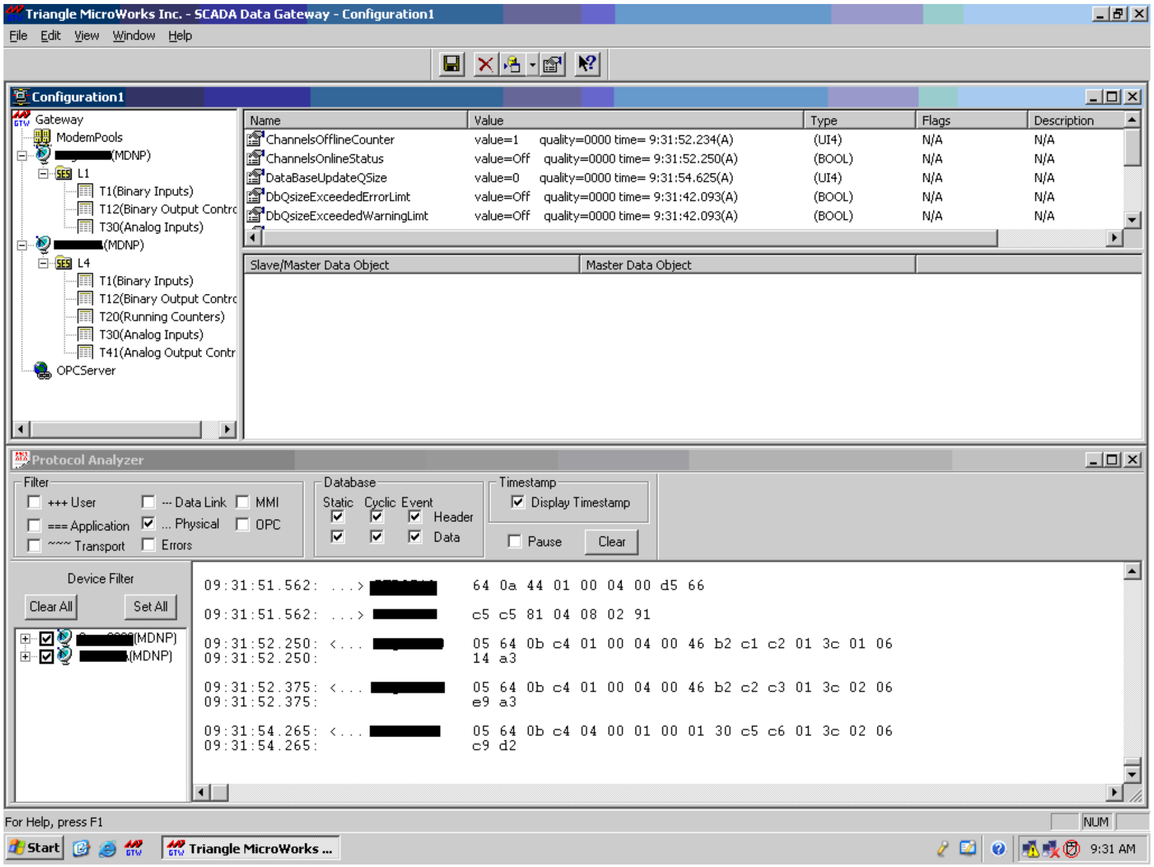
Data from all tests were catalogued, stored for future reference, and imported into a SQL database to assist with analysis. Microsoft Excel and MATLAB®[4] were also used for analysis and graphing. Sample data captures from the products used are contained below.

4.1.1 Triangle MicroWorks SCADA Data Gateway

Figure 6, from the SCADA Data Gateway, provides a status window containing telemetry requests for both the FD-1 and the FD-2. Note that the time contains two digits for the hour, two for the minute, two for the second, and three for microseconds. The upper-left

[4] Registered trademark of The MathWorks, Natick, MA.

panel is used to configure the telemetry environment, including the frequency, classes of data, mode of operation, and communication parameters.



Name	Value	Type	Flags	Description
ChannelsOfflineCounter	value=1 quality=0000 time= 9:31:52.234(A)	(UI4)	N/A	N/A
ChannelsOnlineStatus	value=Off quality=0000 time= 9:31:52.250(A)	(BOOL)	N/A	N/A
DataBaseUpdateQSize	value=0 quality=0000 time= 9:31:54.625(A)	(UI4)	N/A	N/A
DbQsizeExceededErrorLimt	value=Off quality=0000 time= 9:31:42.093(A)	(BOOL)	N/A	N/A
DbQsizeExceededWarningLimt	value=Off quality=0000 time= 9:31:42.093(A)	(BOOL)	N/A	N/A

Slave/Master Data Object	Master Data Object

Filter: ☐ +++ User ☐ --- Data Link ☐ MMI ☐ === Application ☑ ... Physical ☐ OPC ☐ ~~~ Transport ☐ Errors

Database: Static Cyclic Event ☑ ☑ ☑ Header ☑ ☑ ☑ Data

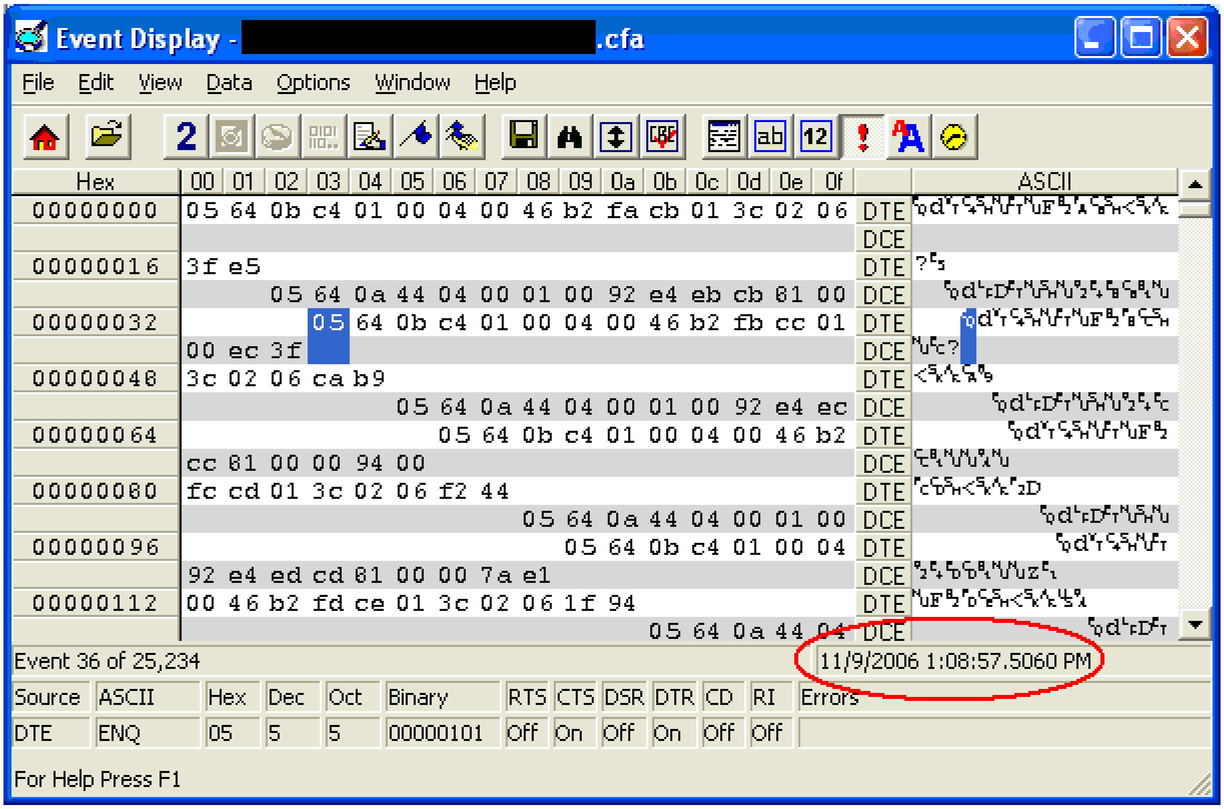
Timestamp: ☑ Display Timestamp ☐ Pause Clear

```
09:31:51.562:  ...>  [redacted]   64 0a 44 01 00 04 00 d5 66

09:31:51.562:  ...>  [redacted]   c5 c5 81 04 08 02 91

09:31:52.250:  <...  [redacted]   05 64 0b c4 01 00 04 00 46 b2 c1 c2 01 3c 01 06
09:31:52.250:                     14 a3

09:31:52.375:  <...  [redacted]   05 64 0b c4 01 00 04 00 46 b2 c2 c3 01 3c 02 06
09:31:52.375:                     e9 a3

09:31:54.265:  <...  [redacted]   05 64 0b c4 04 00 01 00 01 30 c5 c6 01 3c 02 06
09:31:54.265:                     c9 d2
```

Figure 6. Sample data set from Triangle MicroWorks SCADA Data Gateway

4.1.2 NetDecoder Data Capture of Telemetry Request

NetDecoder was used for two views of the data – raw asynchronous data or framed protocol data. Multiple samples of the information are contained in the following screens. The first screen (Figure 7) depicts a request for Class 1 data to the FD-2. Note the value of the time stamp in the screen identified in the red circle (1:08:57.5060). This is the time associated with the first byte of the telemetry request.



Event Display - [redacted].cfa
File Edit View Data Options Window Help

```
Hex       00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f       ASCII
00000000  05 64 0b c4 01 00 04 00 46 b2 fa cb 01 3c 02 06  DTE
                                                           DCE
00000016  3f e5                                            DTE
                05 64 0a 44 04 00 01 00 92 e4 eb cb 81 00  DCE
00000032           05 64 0b c4 01 00 04 00 46 b2 fb cc 01  DTE
          00 ec 3f                                         DCE
00000048  3c 02 06 ca b9                                   DTE
                         05 64 0a 44 04 00 01 00 92 e4 ec  DCE
00000064                    05 64 0b c4 01 00 04 00 46 b2  DTE
          cc 81 00 00 94 00                                DCE
00000080  fc cd 01 3c 02 06 f2 44                          DTE
                                  05 64 0a 44 04 00 01 00  DCE
00000096                             05 64 0b c4 01 00 04  DTE
          92 e4 ed cd 81 00 00 7a e1                       DCE
00000112  00 46 b2 fd ce 01 3c 02 06 1f 94                 DTE
                                                05 64 0a 44 04  DCE
```

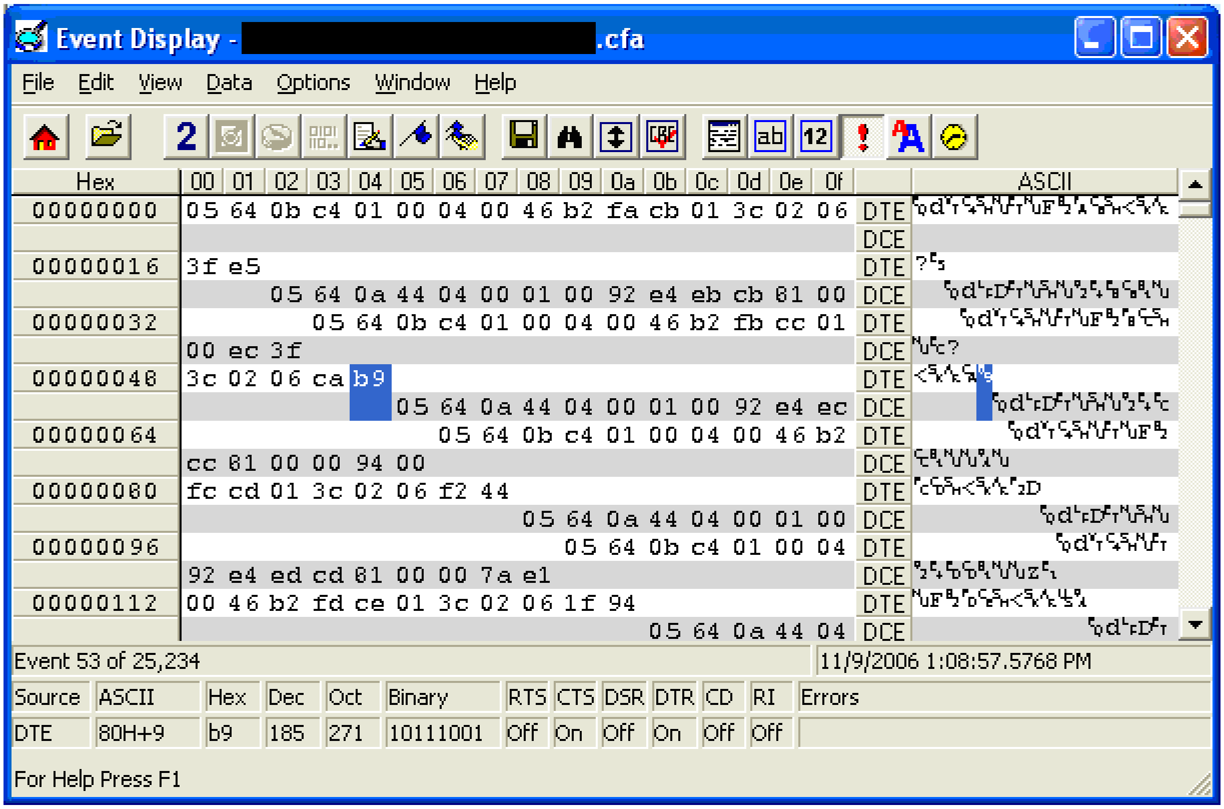
Event 36 of 25,234 | 11/9/2006 1:08:57.5060 PM

Source	ASCII	Hex	Dec	Oct	Binary	RTS	CTS	DSR	DTR	CD	RI	Errors
DTE	ENQ	05	5	5	00000101	Off	On	Off	On	Off	Off	

For Help Press F1

Figure 7. Depicts a request for Class 1 data to the FD-2

Figure 8 contains the last byte of the telemetry request. The time stamp of the last byte is 1:08:57.5768, meaning that 0.0708 seconds elapsed between the first and last bytes of the message. This particular data was generated using 3-second polling at 2400 baud over null-modem communication media.



Event Display - [redacted].cfa

```
Hex       00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f       ASCII
00000000  05 64 0b c4 01 00 04 00 46 b2 fa cb 01 3c 02 06  DTE
                                                           DCE
00000016  3f e5                                            DTE
                05 64 0a 44 04 00 01 00 92 e4 eb cb 81 00  DCE
00000032           05 64 0b c4 01 00 04 00 46 b2 fb cc 01  DTE
          00 ec 3f                                         DCE
00000048  3c 02 06 ca b9                                   DTE
                         05 64 0a 44 04 00 01 00 92 e4 ec  DCE
00000064                    05 64 0b c4 01 00 04 00 46 b2  DTE
          cc 81 00 00 94 00                                DCE
00000080  fc cd 01 3c 02 06 f2 44                          DTE
                                  05 64 0a 44 04 00 01 00  DCE
00000096                             05 64 0b c4 01 00 04  DTE
          92 e4 ed cd 81 00 00 7a e1                       DCE
00000112  00 46 b2 fd ce 01 3c 02 06 1f 94                 DTE
                                           05 64 0a 44 04  DCE
```

Event 53 of 25,234 — 11/9/2006 1:08:57.5768 PM

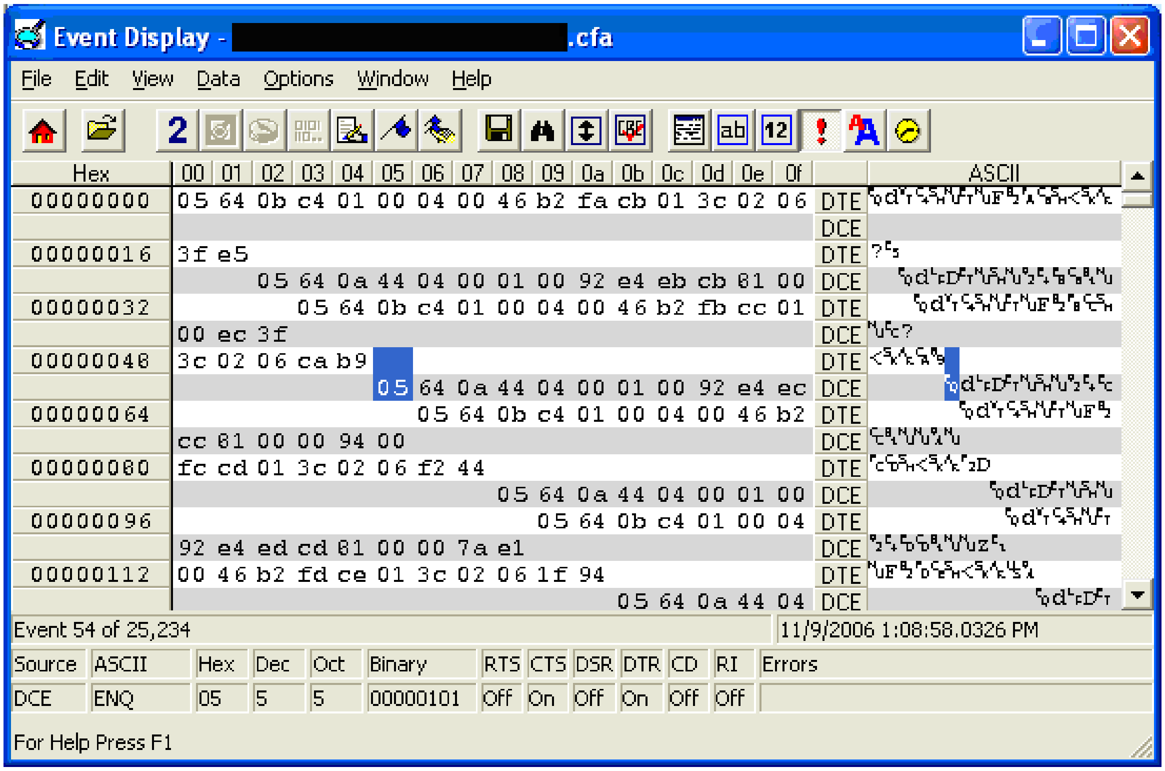
Source	ASCII	Hex	Dec	Oct	Binary	RTS	CTS	DSR	DTR	CD	RI	Errors
DTE	80H+9	b9	185	271	10111001	Off	On	Off	On	Off	Off	

For Help Press F1

Figure 8. Screen containing last byte of the telemetry request.

4.1.3 NetDecoder Data Capture of Telemetry Response

Figure 9 depicts the response from the FD-2. The first byte of the response contains a time stamp of 1:08:58.0326, meaning that the time between the last byte of the request and the first byte of the response is 0.0558 seconds.



```
Hex       00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f      ASCII
00000000  05 64 0b c4 01 00 04 00 46 b2 fa cb 01 3c 02 06  DTE
                                                           DCE
00000016  3f e5                                            DTE
                05 64 0a 44 04 00 01 00 92 e4 eb cb 81 00  DCE
00000032           05 64 0b c4 01 00 04 00 46 b2 fb cc 01  DTE
          00 ec 3f                                         DCE
00000048  3c 02 06 ca b9                                   DTE
                         05 64 0a 44 04 00 01 00 92 e4 ec  DCE
00000064                    05 64 0b c4 01 00 04 00 46 b2  DTE
          cc 81 00 00 94 00                                DCE
00000080  fc cd 01 3c 02 06 f2 44                          DTE
                                  05 64 0a 44 04 00 01 00  DCE
00000096                             05 64 0b c4 01 00 04  DTE
          92 e4 ed cd 81 00 00 7a e1                       DCE
00000112  00 46 b2 fd ce 01 3c 02 06 1f 94                 DTE
                                            05 64 0a 44 04 DCE
```

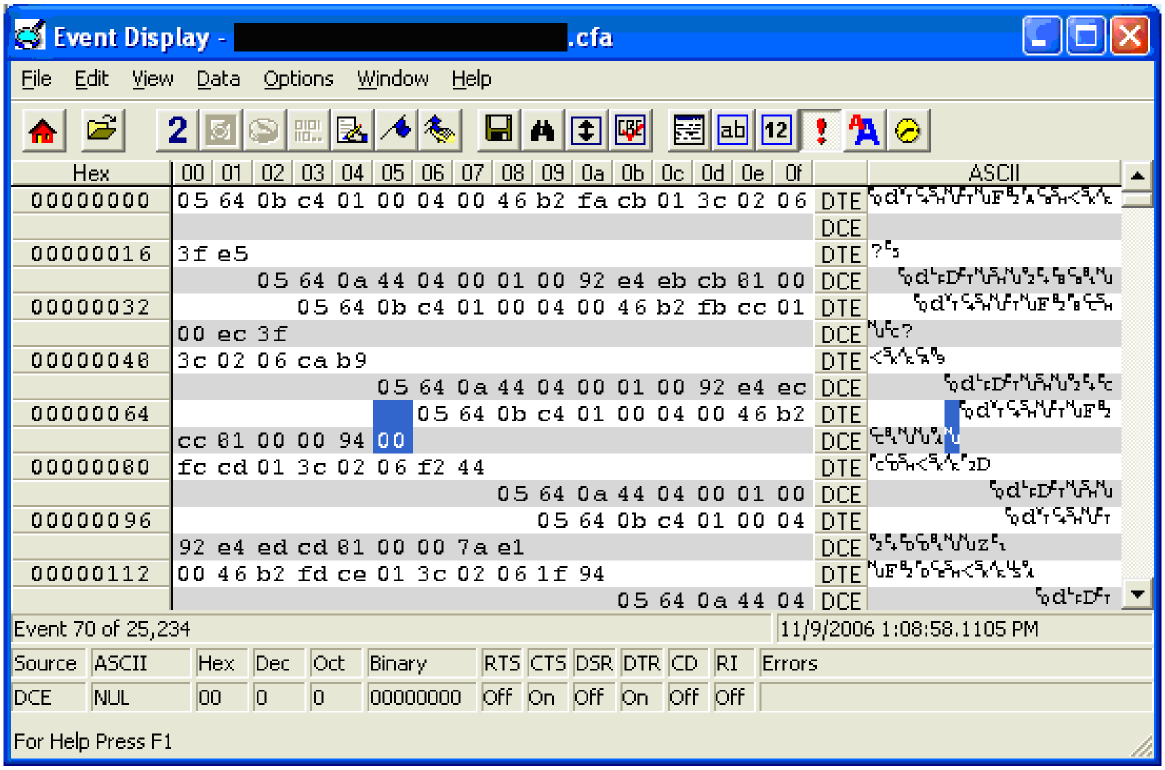
Event 54 of 25,234 | 11/9/2006 1:08:58.0326 PM

Source	ASCII	Hex	Dec	Oct	Binary	RTS	CTS	DSR	DTR	CD	RI	Errors
DCE	ENQ	05	5	5	00000101	Off	On	Off	On	Off	Off	

For Help Press F1

Figure 9. Screen containing the response from the FD-2

Figure 10 contains the last byte of the response. The time stamp of the last byte is 1:08:58.1105, meaning that 0.0779 seconds elapsed between the first and last bytes of the response message. This particular data was generated using 3-second polling at 2400 baud over null-modem communication media.



```
Hex       00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f       ASCII
00000000  05 64 0b c4 01 00 04 00 46 b2 fa cb 01 3c 02 06  DTE
                                                           DCE
00000016  3f e5                                            DTE
                05 64 0a 44 04 00 01 00 92 e4 eb cb 81 00  DCE
00000032           05 64 0b c4 01 00 04 00 46 b2 fb cc 01  DTE
          00 ec 3f                                         DCE
00000048  3c 02 06 ca b9                                   DTE
                         05 64 0a 44 04 00 01 00 92 e4 ec  DCE
00000064                    05 64 0b c4 01 00 04 00 46 b2  DTE
          cc 81 00 00 94 00                                DCE
00000080  fc cd 01 3c 02 06 f2 44                          DTE
                                  05 64 0a 44 04 00 01 00  DCE
00000096                             05 64 0b c4 01 00 04  DTE
          92 e4 ed cd 81 00 00 7a e1                       DCE
00000112  00 46 b2 fd ce 01 3c 02 06 1f 94                 DTE
                                        05 64 0a 44 04     DCE
```

Event 70 of 25,234 | 11/9/2006 1:08:58.1105 PM

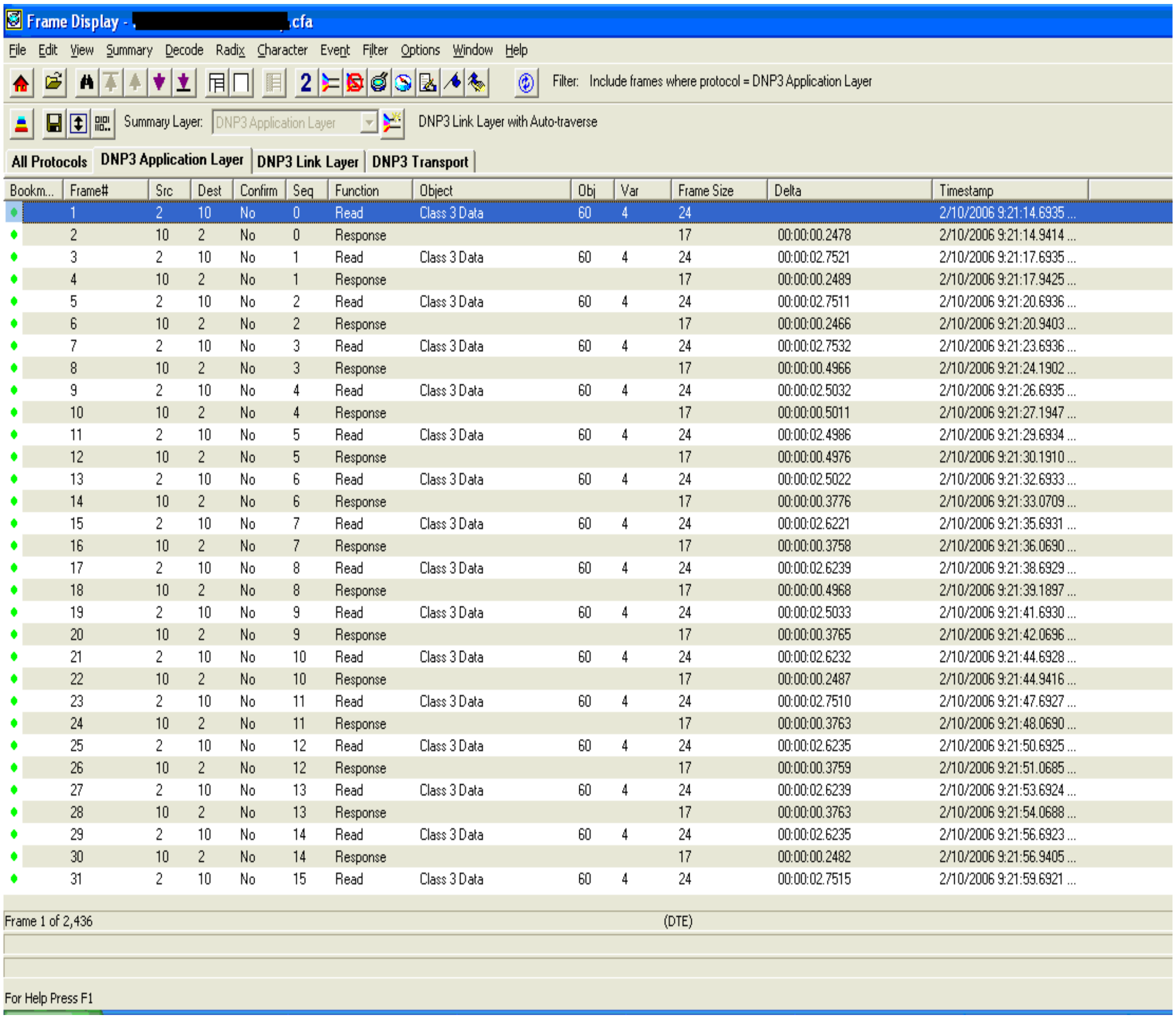
Source	ASCII	Hex	Dec	Oct	Binary	RTS	CTS	DSR	DTR	CD	RI	Errors
DCE	NUL	00	0	0	00000000	Off	On	Off	On	Off	Off	

For Help Press F1

Figure 10. Screen containing last byte of response

4.2 Decoder DNP Data View

When the data is reframed for the protocol in use, a different view is made available. The following screen (Figure 11) shows Class 3 data being requested at 2400 baud over a null-modem cable at 3-second intervals from the FD-1. This view interprets the hexadecimal data, making source, destination, function, and other attributes easily readable. Note the delta values associated with the response. This value is the difference between the first byte of the request and the first byte of the response and is used to generate graphs in MATLAB showing the variability in vendor response times to identical requests and the charts used in the Baseline and Performance Testing sections.



File Edit View Summary Decode Radix Character Event Filter Options Window Help
All Protocols
DNP3 Application Layer
DNP3 Link Layer
DNP3 Transport

Frame Display - [redacted].cfa

Filter: Include frames where protocol = DNP3 Application Layer

Summary Layer: DNP3 Application Layer

DNP3 Link Layer with Auto-traverse

Bookm...	Frame#	Src	Dest	Confirm	Seq	Function	Object	Obj	Var	Frame Size	Delta	Timestamp
◆	1	2	10	No	0	Read	Class 3 Data	60	4	24		2/10/2006 9:21:14.6935 ...
◆	2	10	2	No	0	Response				17	00:00:00.2478	2/10/2006 9:21:14.9414 ...
◆	3	2	10	No	1	Read	Class 3 Data	60	4	24	00:00:02.7521	2/10/2006 9:21:17.6935 ...
◆	4	10	2	No	1	Response				17	00:00:00.2489	2/10/2006 9:21:17.9425 ...
◆	5	2	10	No	2	Read	Class 3 Data	60	4	24	00:00:02.7511	2/10/2006 9:21:20.6936 ...
◆	6	10	2	No	2	Response				17	00:00:00.2466	2/10/2006 9:21:20.9403 ...
◆	7	2	10	No	3	Read	Class 3 Data	60	4	24	00:00:02.7532	2/10/2006 9:21:23.6936 ...
◆	8	10	2	No	3	Response				17	00:00:00.4966	2/10/2006 9:21:24.1902 ...
◆	9	2	10	No	4	Read	Class 3 Data	60	4	24	00:00:02.5032	2/10/2006 9:21:26.6935 ...
◆	10	10	2	No	4	Response				17	00:00:00.5011	2/10/2006 9:21:27.1947 ...
◆	11	2	10	No	5	Read	Class 3 Data	60	4	24	00:00:02.4986	2/10/2006 9:21:29.6934 ...
◆	12	10	2	No	5	Response				17	00:00:00.4976	2/10/2006 9:21:30.1910 ...
◆	13	2	10	No	6	Read	Class 3 Data	60	4	24	00:00:02.5022	2/10/2006 9:21:32.6933 ...
◆	14	10	2	No	6	Response				17	00:00:00.3776	2/10/2006 9:21:33.0709 ...
◆	15	2	10	No	7	Read	Class 3 Data	60	4	24	00:00:02.6221	2/10/2006 9:21:35.6931 ...
◆	16	10	2	No	7	Response				17	00:00:00.3758	2/10/2006 9:21:36.0690 ...
◆	17	2	10	No	8	Read	Class 3 Data	60	4	24	00:00:02.6239	2/10/2006 9:21:38.6929 ...
◆	18	10	2	No	8	Response				17	00:00:00.4968	2/10/2006 9:21:39.1897 ...
◆	19	2	10	No	9	Read	Class 3 Data	60	4	24	00:00:02.5033	2/10/2006 9:21:41.6930 ...
◆	20	10	2	No	9	Response				17	00:00:00.3765	2/10/2006 9:21:42.0696 ...
◆	21	2	10	No	10	Read	Class 3 Data	60	4	24	00:00:02.6232	2/10/2006 9:21:44.6928 ...
◆	22	10	2	No	10	Response				17	00:00:00.2487	2/10/2006 9:21:44.9416 ...
◆	23	2	10	No	11	Read	Class 3 Data	60	4	24	00:00:02.7510	2/10/2006 9:21:47.6927 ...
◆	24	10	2	No	11	Response				17	00:00:00.3763	2/10/2006 9:21:48.0690 ...
◆	25	2	10	No	12	Read	Class 3 Data	60	4	24	00:00:02.6235	2/10/2006 9:21:50.6925 ...
◆	26	10	2	No	12	Response				17	00:00:00.3759	2/10/2006 9:21:51.0685 ...
◆	27	2	10	No	13	Read	Class 3 Data	60	4	24	00:00:02.6239	2/10/2006 9:21:53.6924 ...
◆	28	10	2	No	13	Response				17	00:00:00.3763	2/10/2006 9:21:54.0688 ...
◆	29	2	10	No	14	Read	Class 3 Data	60	4	24	00:00:02.6235	2/10/2006 9:21:56.6923 ...
◆	30	10	2	No	14	Response				17	00:00:00.2482	2/10/2006 9:21:56.9405 ...
◆	31	2	10	No	15	Read	Class 3 Data	60	4	24	00:00:02.7515	2/10/2006 9:21:59.6921 ...

Frame 1 of 2,436 (DTE)

For Help Press F1

Figure 11. Screen containing Class 3 data from FD-1 being requested at 2400 baud

4.3 Custom Application to Support Round-robin Testing

The third product used for the tests was a custom application to support round-robin testing. While part of the DNP protocol, the SCADA Data Gateway product does not support the round-robin telemetry method. Therefore, a custom application was written to submit telemetry requests in this manner and to time stamp the last byte of the request and the first byte of the response. The difference between these two values was recorded, making the impact that the vendor SCMs introduce easily measurable. In addition, the total telemetry requests per hour was calculated using the log file. The round-robin telemetry request methodology used is shown in Figure 12.

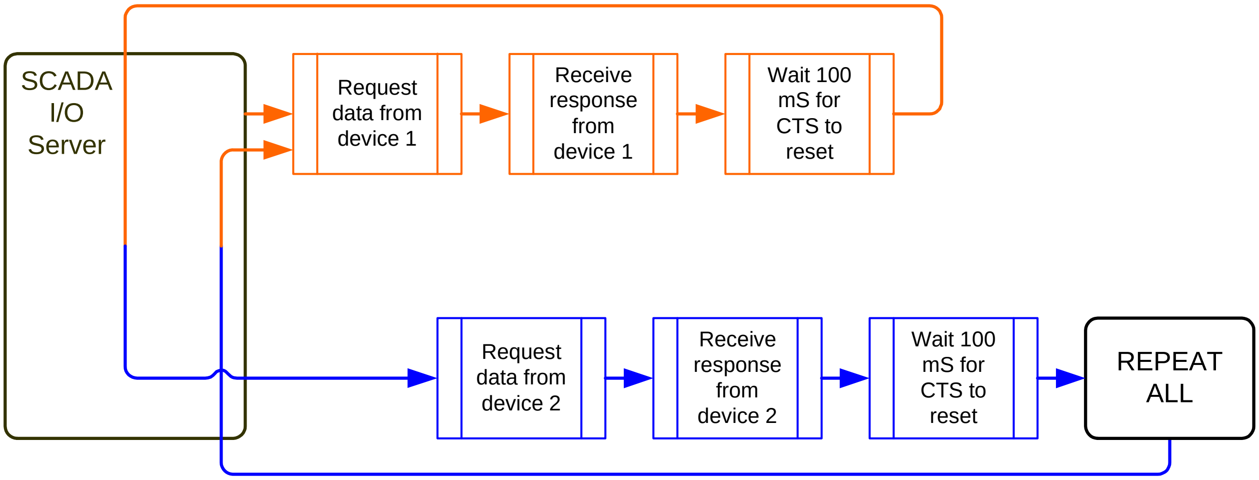
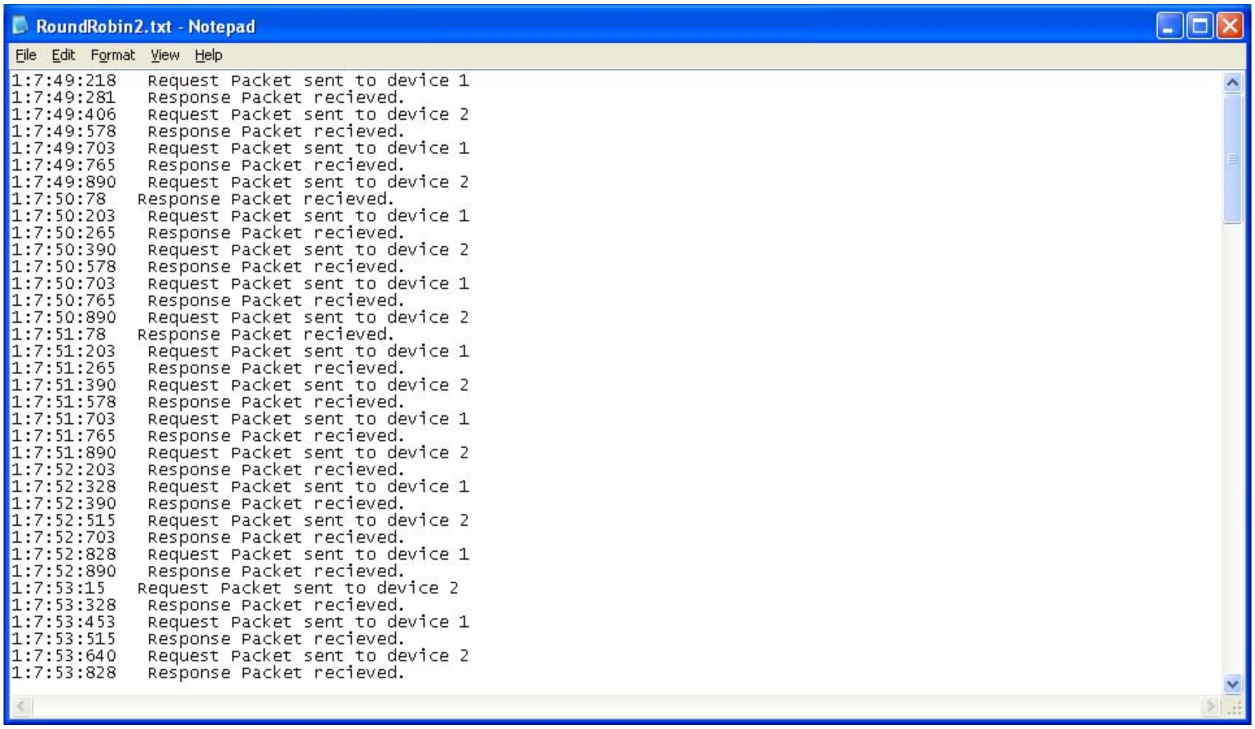

SCADA I/O Server
Request data from device 1
Receive response from device 1
Wait 100 mS for CTS to reset
Request data from device 2
Receive response from device 2
Wait 100 mS for CTS to reset
REPEAT ALL

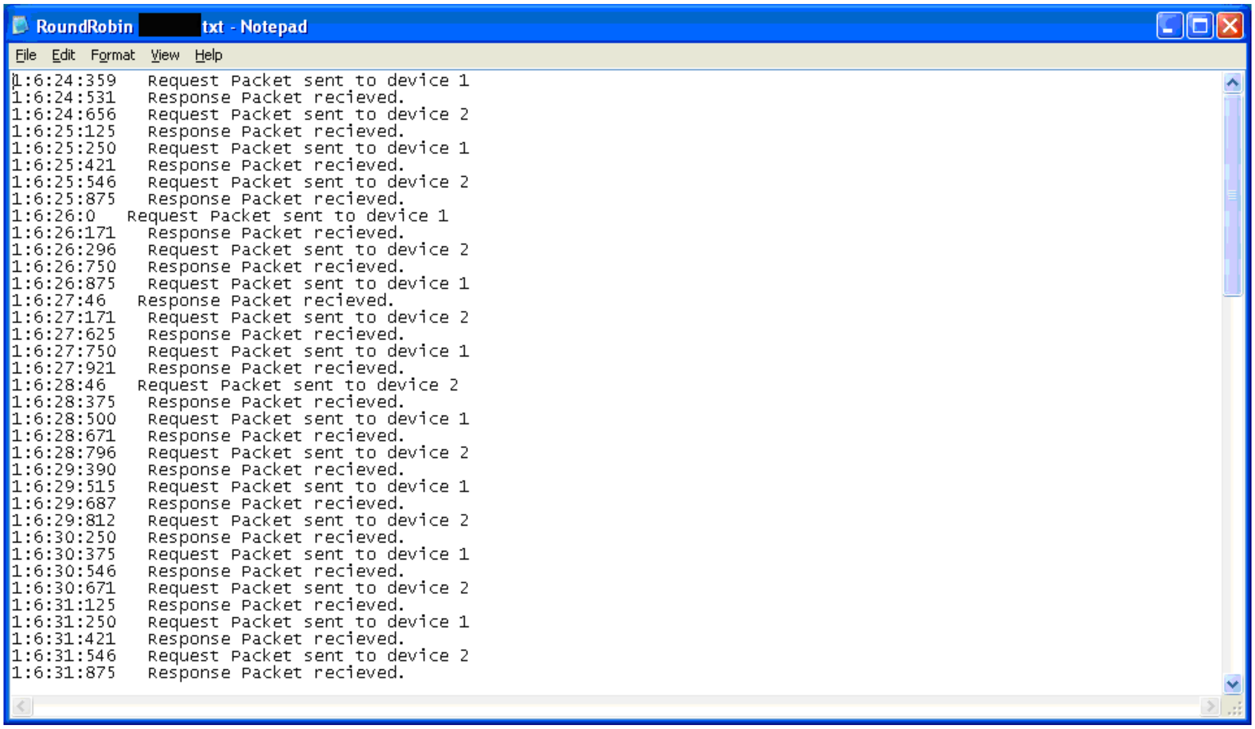
Figure 12. Round-robin telemetry request methodology

Sample log files from the custom application are included for reference. The communication rate for this test is 9600 baud. The first screen (Figure 13a) contains of baseline round-robin results and the second (Figure 13b) contains the SCM-protected communication results.



```
1:7:49:218   Request Packet sent to device 1
1:7:49:281   Response Packet recieved.
1:7:49:406   Request Packet sent to device 2
1:7:49:578   Response Packet recieved.
1:7:49:703   Request Packet sent to device 1
1:7:49:765   Response Packet recieved.
1:7:49:890   Request Packet sent to device 2
1:7:50:78   Response Packet recieved.
1:7:50:203   Request Packet sent to device 1
1:7:50:265   Response Packet recieved.
1:7:50:390   Request Packet sent to device 2
1:7:50:578   Response Packet recieved.
1:7:50:703   Request Packet sent to device 1
1:7:50:765   Response Packet recieved.
1:7:50:890   Request Packet sent to device 2
1:7:51:78   Response Packet recieved.
1:7:51:203   Request Packet sent to device 1
1:7:51:265   Response Packet recieved.
1:7:51:390   Request Packet sent to device 2
1:7:51:578   Response Packet recieved.
1:7:51:703   Request Packet sent to device 1
1:7:51:765   Response Packet recieved.
1:7:51:890   Request Packet sent to device 2
1:7:52:203   Response Packet recieved.
1:7:52:328   Request Packet sent to device 1
1:7:52:390   Response Packet recieved.
1:7:52:515   Request Packet sent to device 2
1:7:52:703   Response Packet recieved.
1:7:52:828   Request Packet sent to device 1
1:7:52:890   Response Packet recieved.
1:7:53:15   Request Packet sent to device 2
1:7:53:328   Response Packet recieved.
1:7:53:453   Request Packet sent to device 1
1:7:53:515   Response Packet recieved.
1:7:53:640   Request Packet sent to device 2
1:7:53:828   Response Packet recieved.
```

(a) Baseline


RoundRobin [redacted] txt - Notepad
File Edit Format View Help

```
1:6:24:359   Request Packet sent to device 1
1:6:24:531   Response Packet recieved.
1:6:24:656   Request Packet sent to device 2
1:6:25:125   Response Packet recieved.
1:6:25:250   Request Packet sent to device 1
1:6:25:421   Response Packet recieved.
1:6:25:546   Request Packet sent to device 2
1:6:25:875   Response Packet recieved.
1:6:26:0   Request Packet sent to device 1
1:6:26:171   Response Packet recieved.
1:6:26:296   Request Packet sent to device 2
1:6:26:750   Response Packet recieved.
1:6:26:875   Request Packet sent to device 1
1:6:27:46   Response Packet recieved.
1:6:27:171   Request Packet sent to device 2
1:6:27:625   Response Packet recieved.
1:6:27:750   Request Packet sent to device 1
1:6:27:921   Response Packet recieved.
1:6:28:46   Request Packet sent to device 2
1:6:28:375   Response Packet recieved.
1:6:28:500   Request Packet sent to device 1
1:6:28:671   Response Packet recieved.
1:6:28:796   Request Packet sent to device 2
1:6:29:390   Response Packet recieved.
1:6:29:515   Request Packet sent to device 1
1:6:29:687   Response Packet recieved.
1:6:29:812   Request Packet sent to device 2
1:6:30:250   Response Packet recieved.
1:6:30:375   Request Packet sent to device 1
1:6:30:546   Response Packet recieved.
1:6:30:671   Request Packet sent to device 2
1:6:31:125   Response Packet recieved.
1:6:31:250   Request Packet sent to device 1
1:6:31:421   Response Packet recieved.
1:6:31:546   Request Packet sent to device 2
1:6:31:875   Response Packet recieved.
```

(b) SCM-protected communication

Figure 13. Round-robin results

4.4 Baseline Communication

Before the impact upon telemetry and control requests can be identified, the normal or baseline communication of representative electric system equipment had to be determined. The following results are based upon 1 hour's worth of data instead of the small sample specified in the AGA-12, Part 2 Performance Test Plan because of the observed variability in response times.

During laboratory testing, leased line analog modem and null-modem communication configurations returned comparable numbers. Performance in operational environments may differ between these two implementations for a number of reasons including distance, quality of communication media, and interference. However, given that the laboratory measurements are comparable, null-modem communication will be used from this point forward to present results.

A spreadsheet will be used to summarize the baseline communication characteristics for each field device. The columns within Table 2 represent the following:

Baud The communication rate used for the performance test

Frequency Indicates how often telemetry requests were made for the performance test

PCPH Polling cycles per hour

Min Minimum measured time between the first byte of the request and the first byte of the response

Max Maximum measured time between the first byte of the request and the first byte of the response

Average The average measured time between the first byte of the request and the first byte of the response

Stdev The standard deviation of the measured time between the first byte of the request and the first byte of the response for all measurements

Rel Stdev The relative standard deviation is a percentage calculated by dividing the Stdev by the Average. The higher the relative standard deviation, the more variability that exists for the field device.

Table 2. DNP Baseline with FD-1

Null-Modem Connection							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second	3383	0.2957	1.2542	0.4406	0.1015	23.03
	2 second	1730	0.2665	1.2506	0.4419	0.1258	28.47
	3 second	1168	0.2883	1.37	0.4294	0.1101	25.65
	5 second	697	0.2764	1.4966	0.4111	0.1348	32.79
2400	1 second	3506	0.1706	0.9734	0.3189	0.1119	35.10
	2 second	1767	0.1958	0.9336	0.3827	0.1026	26.82
	3 second	1176	0.1983	0.8792	0.2936	0.0792	26.96
	5 second	709	0.1876	0.8826	0.2943	0.0964	32.74
4800	1 second	3546	0.149	0.8881	0.2965	0.0966	32.59
	2 second	1782	0.12	0.92	0.2656	0.0967	36.41
	3 second	1189	0.1885	0.8269	0.2853	0.0827	28.97
	5 second	709	0.1464	0.8982	0.2985	0.0969	32.47
9600	1 second	3560	0.119	0.8111	0.2249	0.0891	39.63
	2 second	1789	0.1083	0.8018	0.239	0.0842	35.23
	3 second	1189	0.129	0.742	0.3334	0.1072	32.1471
	5 second	721	0.1005	0.6811	0.2584	0.0899	34.7903
19200	1 second	3569	0.0893	0.9642	0.2871	0.1054	36.73
	2 second	1789	0.1016	0.8041	0.2505	0.0968	38.6215
	3 second	1200	0.0874	0.7836	0.1952	0.0852	43.6245
	5 second	721	0.1073	0.7951	0.2597	0.0963	37.0661

Figure 14 was created in MATLAB and is included to help visualize the data in Table 2. The chart is based upon telemetry requests at 2400 baud with a 3-second polling frequency. This combination was selected to demonstrate variability with a manageable data set. Other baud rate and polling frequency combinations will produce a similar histogram. Each of the blue vertical dotted lines represents baseline measurements, and the height of each bar indicates the number of measurements taken at the time interval on the x-axis. Each of the green solid vertical lines represents SCM-2 protected communication.

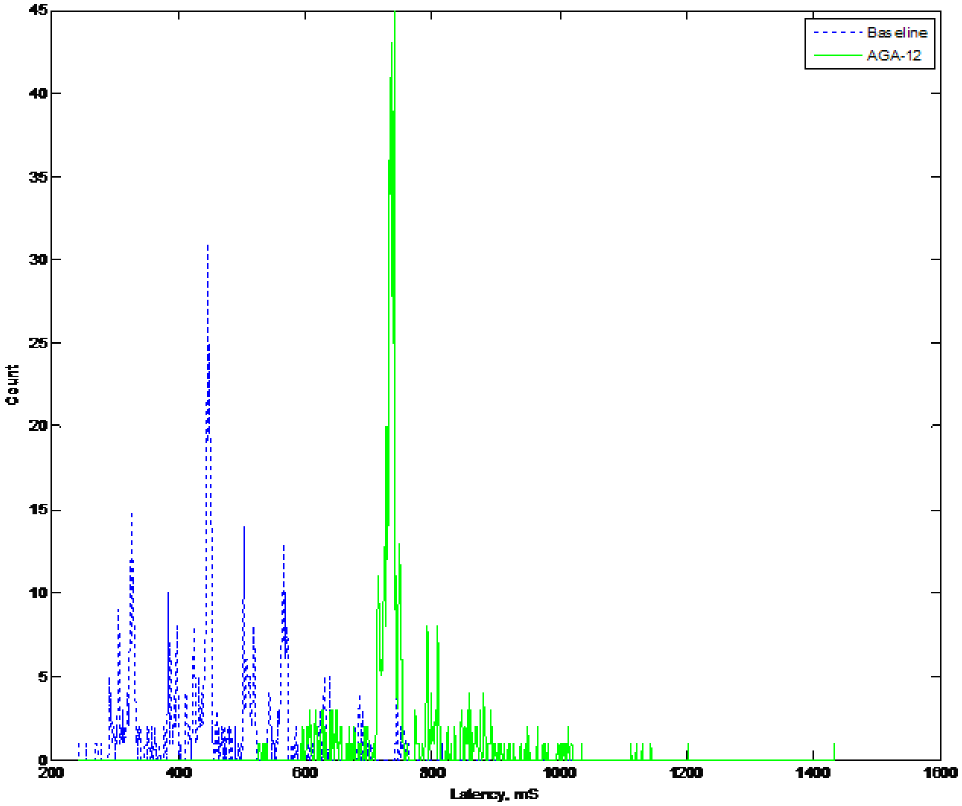


Figure 14. Histrogram of baseline and SCM-2 protected data for FD-1

Table 3 contains the data from which the histogram in Figure 15 is created using MATLAB. Note that the FD-2 is extremely consistent in response time at each baud. As a result, the small sample size identified in the test plan will be used to measure the latency that SCMs introduce.

Table 3. CNP Baseline with FD-2

Null-Modem Connection							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second	3600	0.1697	0.1922	0.1708	0.001	0.5871
	2 second	1800	0.1696	0.1936	0.1708	0.0013	0.7411
	3 second	1200	0.1696	0.1764	0.1708	0.0005	0.2767
	5 second	720	0.1699	0.1915	0.1708	0.0011	0.6451
2400	1 second	3600	0.0944	0.1188	0.0954	0.0011	1.1277
	2 second	1800	0.0945	0.1087	0.0955	0.0007	0.6818
	3 second	1200	0.0945	0.1009	0.0954	0.0004	0.4497
	5 second	720	0.0945	0.1161	0.0954	0.0015	1.5597
4800	1 second	3600	0.0568	0.0805	0.0577	0.0011	1.8582
	2 second	1800	0.0569	0.0745	0.0577	0.0008	1.3772
	3 second	1200	0.0568	0.0728	0.0577	0.0008	1.4331
	5 second	720	0.0568	0.0826	0.0577	0.0018	3.1091
9600	1 second	3600	0.038	0.0585	0.0388	0.0008	1.9694
	2 second	1800	0.038	0.0624	0.0389	0.0012	3.0205
	3 second	1200	0.038	0.0575	0.0388	0.0011	2.9396
	5 second	720	0.0381	0.0458	0.0388	0.0006	1.5599
19200	1 second	3600	0.0286	0.0535	0.0294	0.0011	3.6018
	2 second	1800	0.0286	0.051	0.0294	0.0009	2.9915
	3 second	1200	0.0286	0.0408	0.0294	0.0007	2.3467
	5 second	720	0.0286	0.0514	0.0294	0.0011	3.8561

The chart is based on telemetry requests at 2400 baud with a 3-second polling frequency. Again, this combination was selected to demonstrate variability with a manageable data set. Other baud rate and polling frequency combinations will produce a similar histogram. Each of the vertical bars represents baseline measurements, and the height of each bar indicates the number of measurements taken at the time interval on the x-axis. This histogram does not contain SCM-protected communication values because of scaling issues within MATLAB.

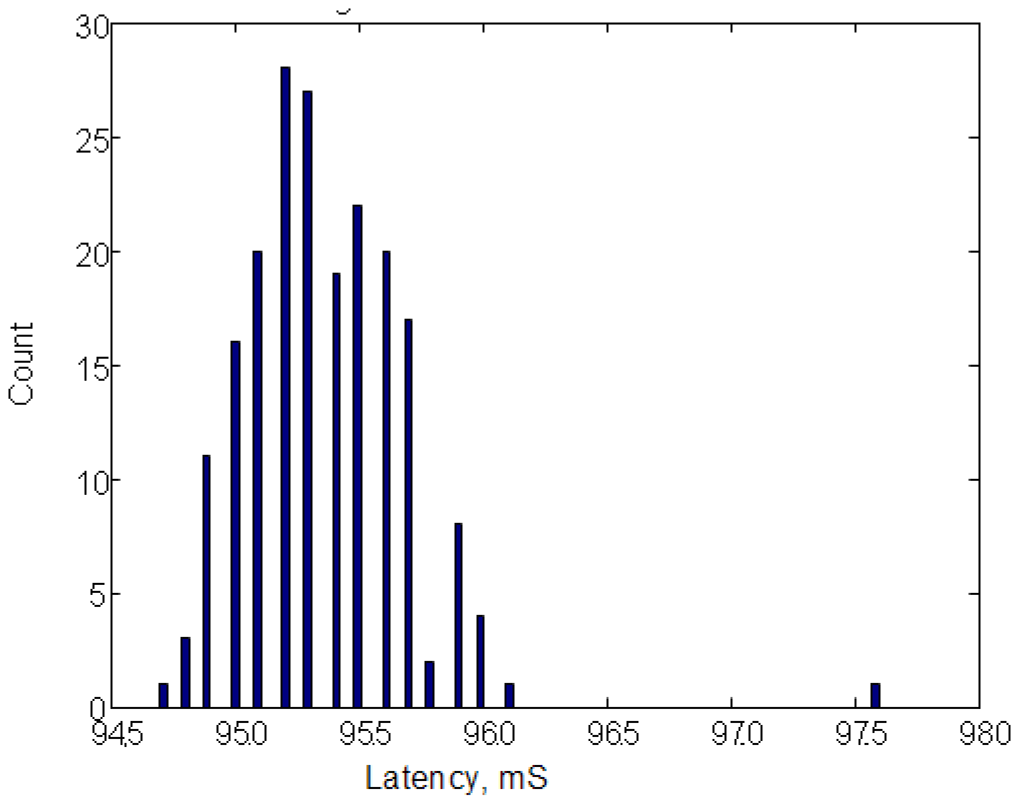


Figure 15. Histogram of baseline FD-2 communication

Table 4 contains the data from which Figure 16 was created in MATLAB. The chart is based upon telemetry requests at 2400 baud with a 3-second polling frequency. Again, this combination was selected to demonstrate variability with a manageable data set. Other baud rate and polling frequency combinations will produce a similar histogram. Each of the vertical bars represents baseline measurements, and the height of each bar indicates the number of measurements taken at the time interval on the x-axis. Because Modbus does not contain an equivalent to a DNP Class 0 request, three separate registers were polled during each polling cycle. Note that the communication characteristics for the FD-3 differ from both the FD-1 and FD-2.

Table 4. Modbus base FD-3 communication data

Null-Modem Connection							
Note - each polling cycle contains three requests: coils, discrete, and holding register							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second	10800	0.1032	0.1095	0.1056	0.0015	1.4409
	2 second	5400	0.1032	0.1127	0.1061	0.0019	1.8309
	3 second	3600	0.1031	0.1124	0.1062	0.0021	1.9776
	5 second	2160	0.1031	0.1122	0.1058	0.0017	1.6209
2400	1 second	10800	0.0529	0.0625	0.0556	0.0019	3.4351
	2 second	5400	0.0529	0.0618	0.0555	0.0017	3.0693
	3 second	3600	0.0529	0.0623	0.0556	0.0018	3.2444
	5 second	2160	0.0529	0.0623	0.0556	0.0018	3.2422
4800	1 second	10800	0.0278	0.0371	0.0304	0.0017	5.7145
	2 second	5400	0.0278	0.0362	0.0303	0.0016	5.4273
	3 second	3600	0.0278	0.0363	0.0305	0.0017	5.6222
	5 second	2160	0.0278	0.0371	0.0304	0.0017	5.5674
9600	1 second	10800	0.0152	0.0248	0.0177	0.0015	8.7075
	2 second	5400	0.0152	0.0247	0.0178	0.0016	8.7377
	3 second	3600	0.0152	0.0241	0.0179	0.0017	9.6476
	5 second	2160	0.0152	0.0242	0.0179	0.0018	9.8389
19200	1 second	10800	0.009	0.0174	0.0116	0.0018	15.4885
	2 second	5400	0.009	0.0179	0.0117	0.0018	15.3503
	3 second	3600	0.009	0.0185	0.0116	0.0018	15.2407
	5 second	2160	0.009	0.0182	0.0116	0.0018	15.1107

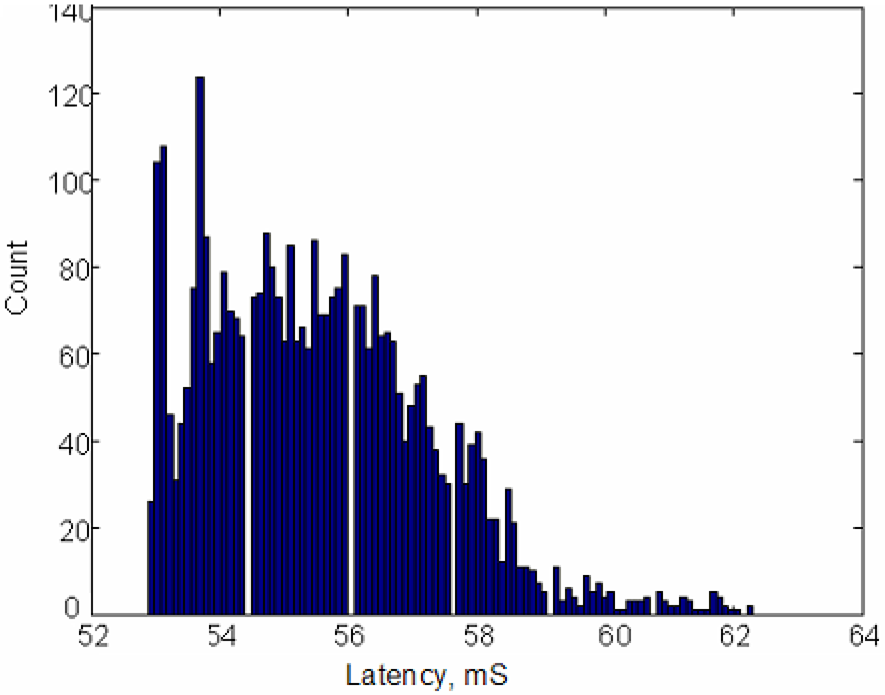


Figure 16. Histogram of baseline Modbus communication for FD-3

4.5 SCM-Protected Communication

The introduction of vendor CMs onto a serial communication channel will add latency to communication. The impact on an organization is dependent upon many factors including baud rate, communication media, telemetry scheme, field device selection, and the version of the AGA-12 standard to which the CM is built. This report does not draw conclusions regarding the applicability or usefulness of vendor CMs on a utilities infrastructure. The purpose is to show the impact on communication in various situations.

Table 5 contains the data from which the histogram in Figure 17 (a duplicate of Figure 14 presented earlier) is created. The chart shows both the baseline and latency SCM-2 has on communication with the FD-1 at 2400 baud and 3-second polling. The blue dotted lines represent baseline communication while the green solid lines represent CM protected communication. The shift to the right depicted by the black bars is the additional latency. The SCM-2 devices used the PE mode, and the height of each bar represents the number of measurements taken at the time interval represented on the x-axis. Table 5 contains PE mode measurement averages for the SCM-2 and the FD-1.

Table 5. PE mode measurement averages for SCM-2 and FD-1

DNP Measurements DNP PE Mode with SCM-2 and FD-1 Null-Modem Connection							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second	2260	0.0391	1.6166	1.3006	0.1238	9.5163
	2 second	1738	0.1089	1.6336	1.2714	0.1296	10.1904
	3 second	1145	0.8720	1.6997	1.2932	0.1129	8.728
	5 second	710	0.0144	1.6829	1.3138	0.1712	13.031
2400	1 second	3487	0.436	1.1337	0.832	0.1108	13.3168
	2 second	1753	0.436	1.1447	0.8391	0.1013	12.0688
	3 second	1200	0.436	1.1949	0.8391	0.1019	12.1474
	5 second	710	0.436	1.1367	0.824	0.1108	13.4507
4800	1 second	3323	0.3731	0.8893	0.5453	0.0977	17.9167
	2 second	1763	0.4394	0.9317	0.5648	0.097	17.1838
	3 second	1112	0.3832	0.9381	0.5856	0.0978	16.6990
	5 second	678	0.3701	0.8999	0.6029	0.0978	16.2289
9600	1 second						
	2 second	1758	0.2289	0.7597	0.4617	0.1126	24.3977
	3 second	1178	0.2433	0.8152	0.4628	0.1084	23.4212
	5 second	710	0.2538	0.8673	0.4568	0.0999	21.8721
19200	1 second						
	2 second	1776	0.1998	0.6539	0.3655	0.0997	27.283
	3 second	1178	0.1948	6504	0.3834	0.1032	26.9204
	5 second	720	0.2381	0.6771	0.3635	0.0885	24.3467

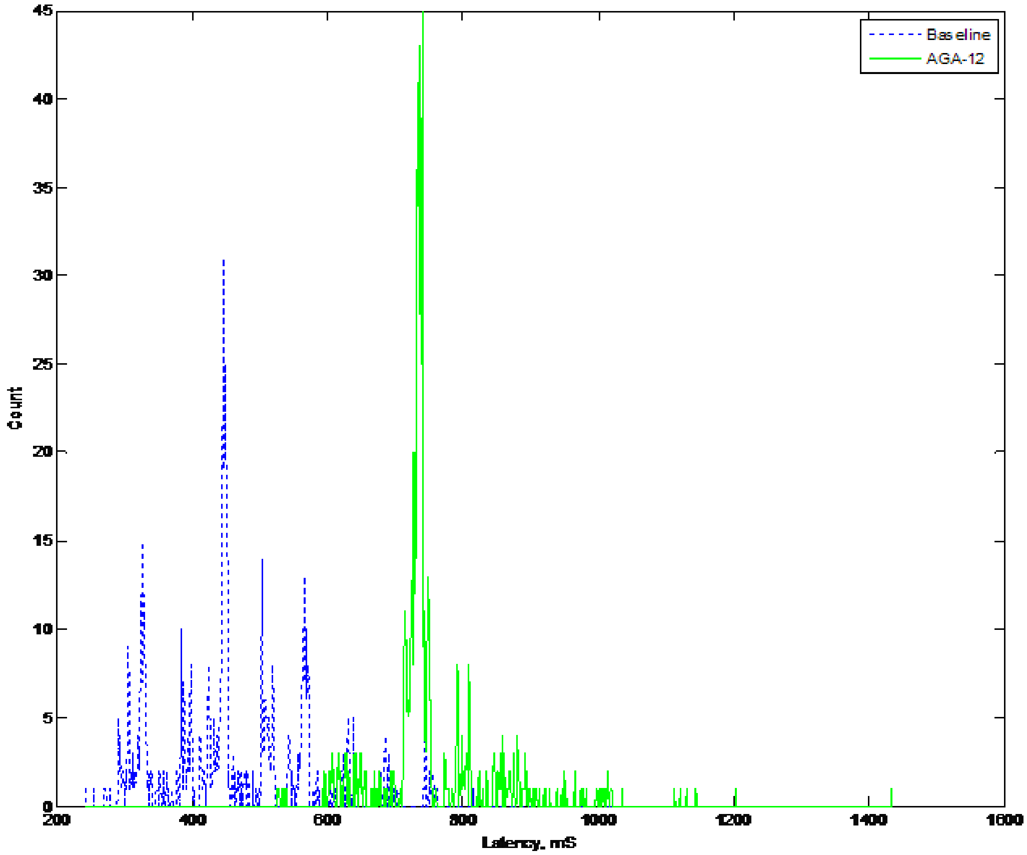


Figure 17. Histogram of baseline and SCM-2 protected data for FD-1

Table 6 and Figure 18 summarize the impact that SCM-1 has on serial communication. Table 6 displays all CTR mode communication data, and the histogram again uses 2400 baud communication with 3-second polling. The vertical bars represent SCM-1 protected communication using CTR mode, and the height of each bar represents the number of measurements taken at the time interval represented on the x-axis. Figure 19 shows the baseline, PE mode, and CTR mode communication averages at 2400 baud. Note that minimal performance difference between PE and CTR modes.

Table 6. DNP SCM-1 cipher suite 2 FD-2

Null-Modem Connection							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second						
	2 second						
	3 second						
	5 second						
2400	1 second	3463	0.5261	0.5494	0.5271	0.0012	0.2263
	2 second	1795	0.5262	0.5488	0.5271	0.0013	0.2501
	3 second	1200	0.5263	0.5321	0.5271	0.0008	0.1492
	5 second	720	0.5263	0.5439	0.5272	0.0015	0.2864
4800	1 second	3600	0.2750	0.2977	0.2758	0.0010	0.3522
	2 second	1800	0.2751	0.2957	0.2758	0.0011	0.3981
	3 second	1200	0.2750	0.2851	0.2758	0.0007	0.2621
	5 second	713	0.2751	0.2785	0.2758	0.0005	0.1760
9600	1 second	3600	0.1494	0.1717	0.1501	0.0010	0.6380
	2 second	1800	0.1494	0.1726	0.1501	0.0009	0.6278
	3 second	1200	0.1494	0.1605	0.1500	0.0006	0.4100
	5 second	720	0.1494	0.1661	0.1501	0.0010	0.6753
19200	1 second	3600	0.0864	0.1048	0.0871	0.0008	0.8738
	2 second	1800	0.0865	0.1094	0.0871	0.0011	1.2341
	3 second	1200	0.0864	0.0985	0.0871	0.0007	0.8478
	5 second	713	0.0865	0.1098	0.0872	0.0015	1.7437

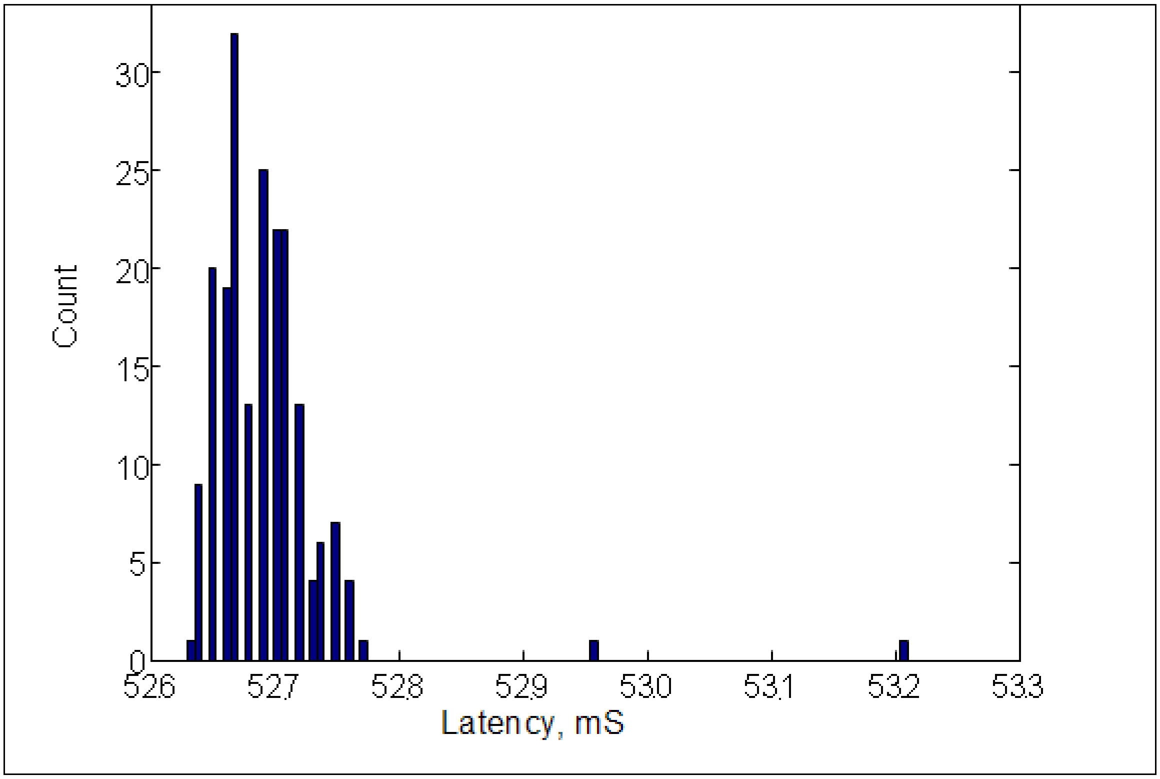


Figure 18. Histogram of SCM-1 protected data for FD-2

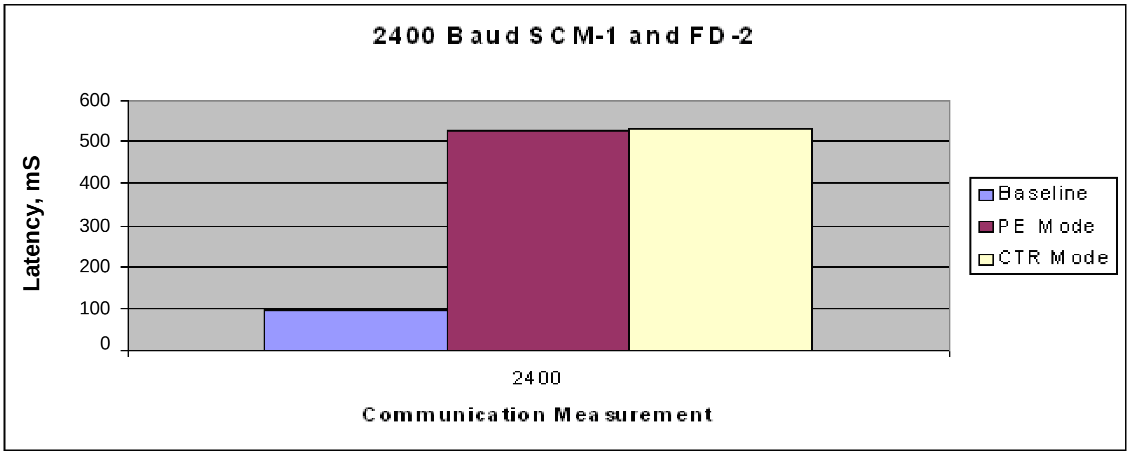


Figure 19. Baseline, PE mode and CTR communication averages at 2400 baud

4.5.1 Modbus Measurements

Table 7 contains the data from which the histogram in Figure 20 is created using MATLAB. The histogram is based on telemetry requests at 2400 baud with a 3-second polling frequency. Again, this combination was selected to demonstrate variability with a manageable data set. Other baud rate and polling frequency combinations will produce a similar histogram. Each of the vertical bars represents baseline measurements, and the

Table 7. Modbus SCM-2 PE mode with FD-3

Null-Modem Connection							
Note - each PC contains 3 requests. Coils, Discrete, and Holding Register							
Baud	**Frequency**	**PCPH**	**Min**	**Max**	**Average**	**Stdev**	**Rel Stdev**
1200	1 second	1512	2.2049	2.5257	2.2931	0.0264	0.0115
	2 second	1512	2.2186	2.5073	2.2934	0.024	0.0104
	3 second	1509	2.0241	2.4969	2.2951	0.0286	0.0125
	5 second	1008	2.2115	2.5183	2.2931	0.0255	0.0111
2400	1 second	3003	1.0605	1.234	1.1386	0.0279	0.0245
	2 second	3003	1.0561	1.2215	1.1388	0.0292	0.0257
	3 second	3006	1.0563	1.2171	1.1385	0.0285	0.0251
	5 second	2160	0.8181	1.3714	1.1128	0.0657	0.059
4800	1 second	5220	0.455	0.7958	0.6442	0.0382	0.0593
	2 second	5223	0.4657	0.7862	0.6431	0.0396	0.0616
	3 second	3600	0.4377	0.7412	0.6048	0.0577	0.0955
	5 second	2160	0.4334	0.7351	0.6089	0.059	0.0968
9600	1 second	9879	0.2415	0.5369	0.3254	0.0384	0.118
	2 second	5400	0.237	0.5088	0.3242	0.0399	0.1232
	3 second	3597	0.2413	0.5007	0.3228	0.0388	0.1201
	5 second	2160	0.2427	0.5041	0.3174	0.0371	0.1169
19200	1 second	10697	0.1281	0.2975	0.1964	0.027	0.1375
	2 second	5384	0.1265	0.2944	0.1947	0.0268	0.1379
	3 second	3592	0.1283	0.2862	0.1927	0.0265	0.1376
	5 second	2158	0.1287	0.2824	0.1955	0.0253	0.1293

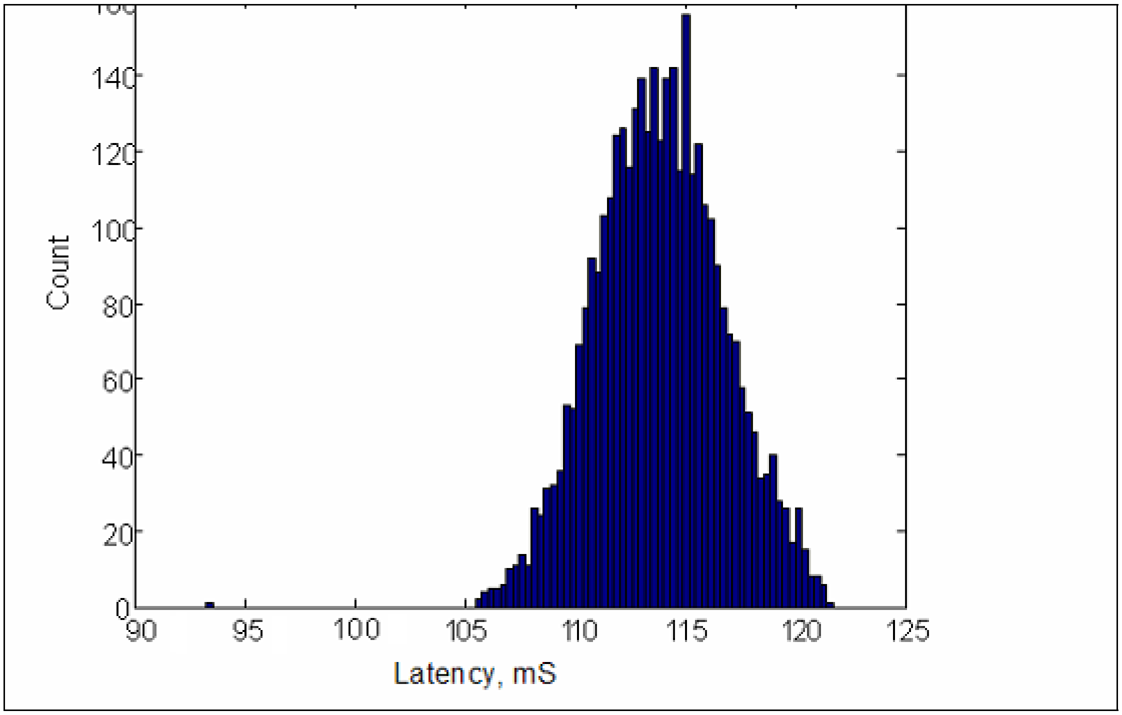


Figure 20. Histogram of SCM-2 protected Modbus communication for FD-3

height of each bar indicates the number of measurements taken at the time interval on the x-axis. Because Modbus does not contain an equivalent to a DNP Class 0 request, three separate registers were polled during each polling cycle. Note that the communication characteristics for the FD-3 differ from both the FD-1 and FD-2. This is because each field device vendor product is unique. The processor, operating system, available memory, and serial port drivers are specific to the vendor product. In addition, the design of the field device may provide varying levels of importance to communication and SCADA services. For example, one vendor may utilize 50% of the processor for communications while another utilizes 90%. The combination of all of these factors results in unique communication patterns for the tested field device.

4.5.2 Single Telemetry Request Tests

The introduction of SCM-1 or SCM-2 into a communication stream increases the amount of time required for a single telemetry request and response to complete. Figures 21 and 22 depict the impact on a single DNP request using the average response time as recorded by NetDecoder. Given the variability in a small sample size, the chart is based on the entire sample for the FD-1. The small sample size is used for the FD-2. The baseline request to the field device is represented by the blue bar, PE communication times are represented by the red bar, and the yellow bar represents CTR mode. As baud rate increases, the impact upon communication decreases.

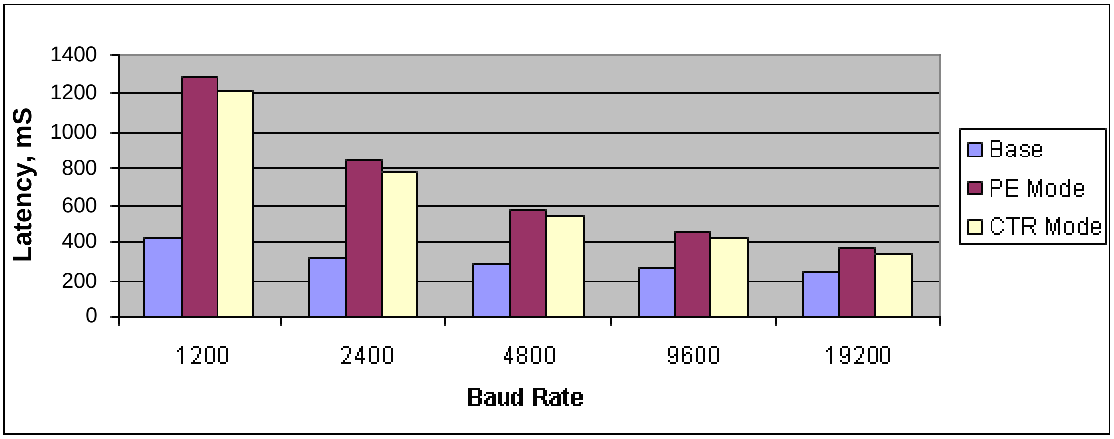


Figure 21. Average communication time for DNP telemetry request SCM-2 and FD-1

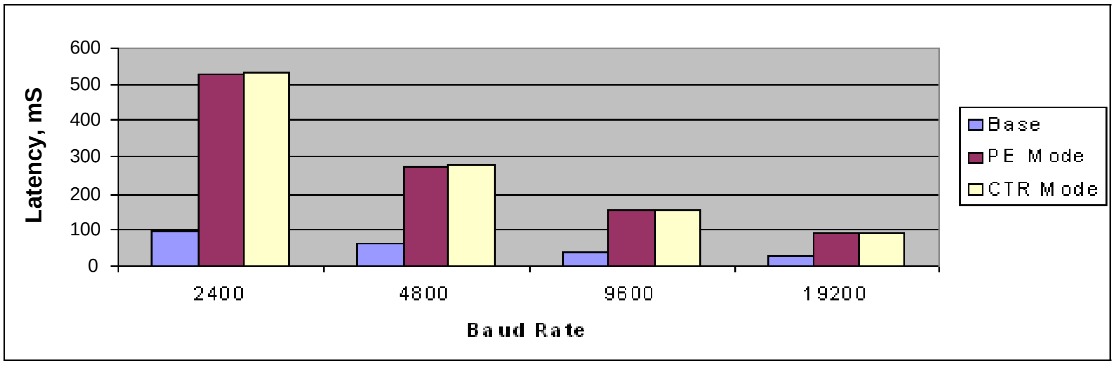


Figure 22. Average communication time for DNP telemetry request SCM-1 and FD-2

4.5.3 Polling Cycles per Hour Tests

Figures 23 and 24 represent the impact SCMs have on round-robin telemetry schemes. The y-axis shows polling cycles per hour. The amount of telemetry requests that can be completed within 1 hour is decreased by both supported cipher suites; the cumulative effect of added latency for each telemetry request and response is indicated by the difference in height for the baseline and SCM-protected communication. Note that CTR mode and PE mode performance do not substantially differ.

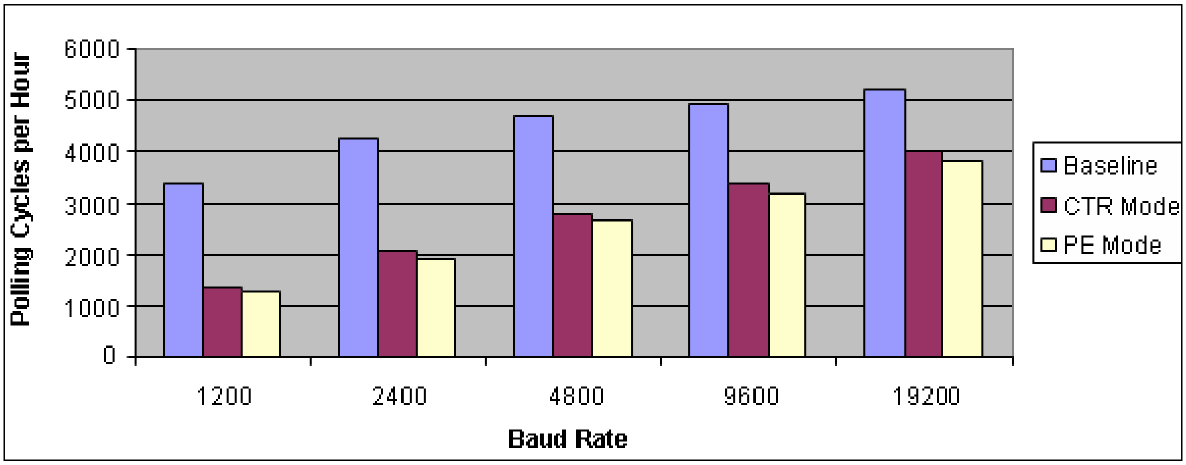


Figure 23. Round-robin SCM-2 (FD-1)

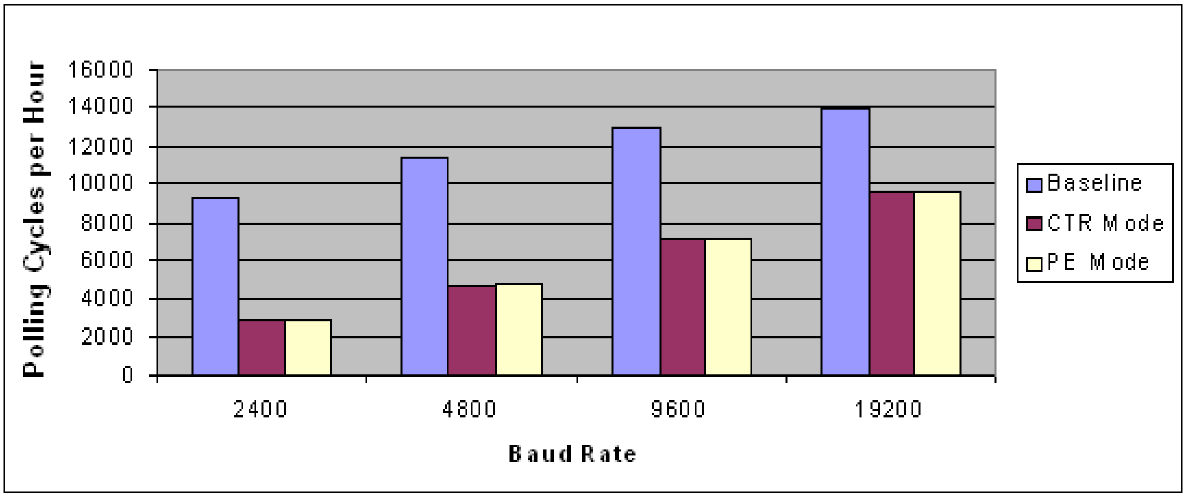


Figure 24. Round-robin SCM-1 (FD-2)

Table 8 summarizes the impact on polling cycles per hour for both the FD-1 (SCM-2) and FD-2 (SCM-1) for DNP requests. SCM-1 communication was consistent for both PE and CTR mode and is included in a single column. It is not appropriate to directly compare SCM-1 and SCM-2 performance numbers because of compliance to different AGA-12 versions, and the amount of data returned by the FD-1 far exceeds that of the FD-2 for Class 0 data. In all cases below, as baud rate or the interval between telemetry requests increases, SCM-protected communication approaches our baseline measurements.

Table 8. Impact on polling cycles per hour for both FD-1 and FD-2

	FD-1			FD-2		
Baud	**Baseline**	**SCM-2 PE**	**CTR**	**Baseline**	**SCM-1 PE**	**CTR**
1200	3383	2260	2333	3600		
	1730	1738	1718	1800		
	1168	1145	1152	1200		
	697	710	708	720		
2400	3506	3487	3493	3600	3463	3456
	1767	1753	1754	1800	1795	1794
	1176	1200	1176	1200	1200	1200
	709	710	708	720	720	720
4800	3546	3323	3541	3600	3600	3600
	1782	1763	1776	1800	1800	1800
	1189	1112	1188	1200	1200	1200
	709	678	708	720	713	713
9600	3560	3560	3560	3600	3600	3600
	1789	1758	1788	1800	1800	1800
	1189	1178	1188	1200	1200	1200
	720	710	720	720	720	720
19200	3569	3560	3553	3600	3600	3600
	1789	1776	1788	1800	1800	1800
	1200	1178	1200	1200	1200	1200
	720	720	720	720	720	720

Figure 25 shows the impact on polling cycles per hour as a percent of the baseline. The normal baseline measurement is shown as unity, and any number below 1 represents reduced performance. For an explanation of how to interpret this chart, examine the yellow line. At rates below 9600 baud, a reduction in polling cycles per hour is present. At 1200 baud, polling cycles per hour is only 30% of normal, and at 2400 baud, it is 50% of normal. The impact for Modbus appears to be greater for all baud rates and polling frequency combinations than for DNP.

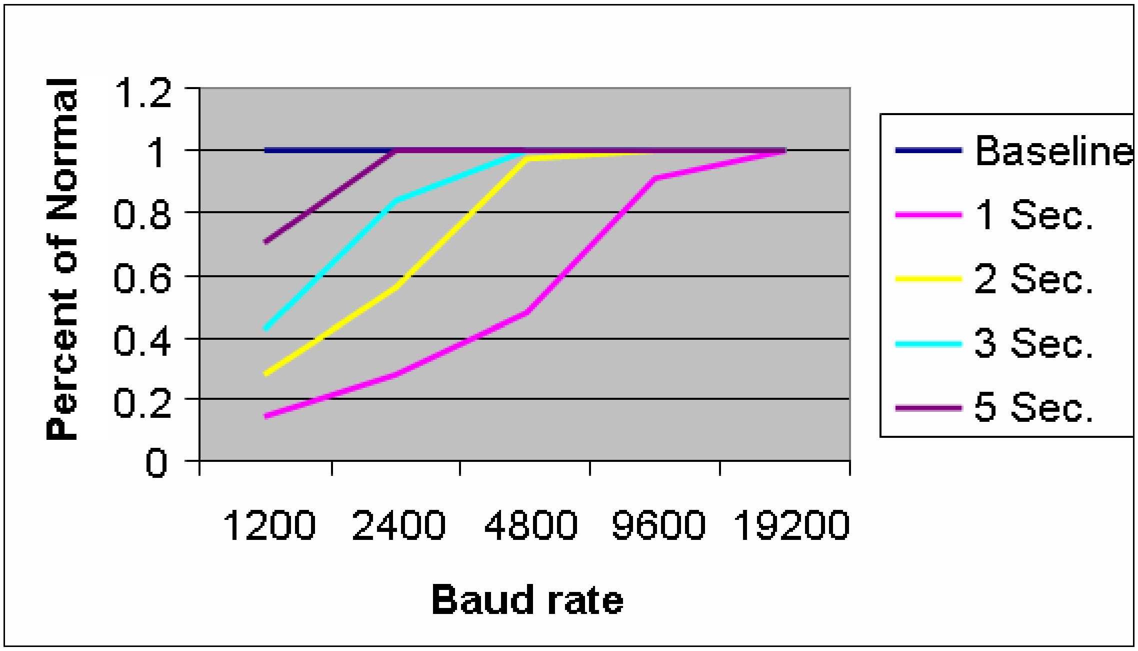


Figure 25. SCM-2 Modbus PE mode

4.6 Control Tests

The control tests shown in Figure 26 below summarize the findings for the SCM-1 modules and similar results are available for other vendor SCMs. Both supported AGA-12 cipher suites are included, and the DNP control request was made using the industry standard method of “select-before-operate”. This method requires two messages from the I/O server to enact the control, compared to a direct operate method that only utilizes a single message. Each message is approximately the same length as a telemetry request. From Modbus, the impact would be equivalent to a telemetry request. Similar to telemetry requests, the latency impact on control decreases as baud rate increases. Note that the SCM-1 devices did not function at 1200 baud. A good estimate for the level of impact on control with CM in place is to double the latency associated with a telemetry request.

Control with the Modbus protocol is not impacted as heavily as DNP because of fundamental differences governing how the protocols function. Modbus works in a “direct operate” mode, where a single control request is given to the remote device. The receiving device simply enacts the request and returns a response. While DNP can function in this manner, typical implementations use a select before operate method. This approach utilizes two requests from the master to enact the control, and each request contains a response. For the Modbus protocol, the impact on control is the same as the impact for a single telemetry request.

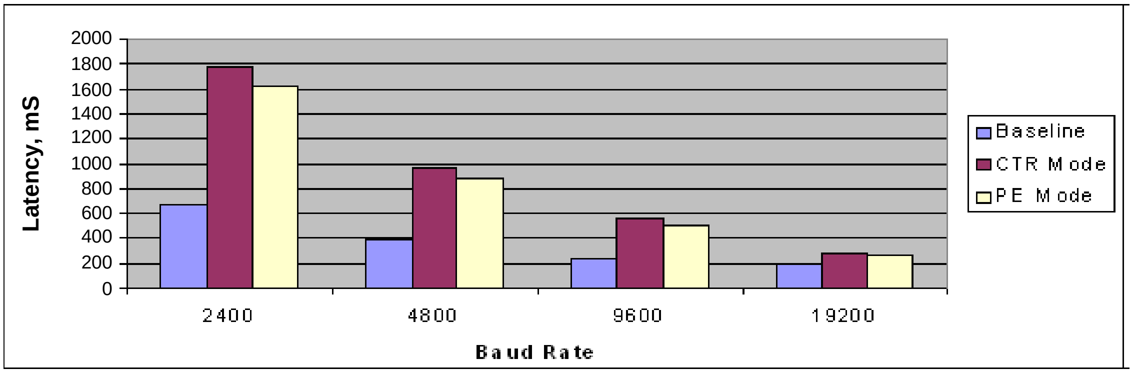


Figure 26. CNP control impact

4.7 Stress Tests

Stress tests were performed according to the test plan. Table 9 indicates the minimum telemetry window in milliseconds, before communication errors occur. The request in this example is for DNP Class 1 data only using the SCM-1 and cipher suite 2. At polling frequencies smaller than indicated in the table, responses are not received before the next request is submitted, resulting in a loss of data.

Table 9. Minimum telemetry window versus baud rate

Baud Rate	1200	2400	4800	9600	19200
Telemetry Window, mS	750	700	350	200	100

4.8 Failover Tests

All SCM-protected and baseline communication environments successfully passed all failover tests and resumed communication as expected (see Table 10).

Table 10. Failover Test Results

Vendor	Cipher Suite	Communication Failure	Power Failure
SCM-1	1 and 2	Passed	Passed
SCM-2	1 and 2	Passed	Passed
FD-1	Baseline	Passed	Passed
FD-2	Baseline	Passed	Passed
FD-3	Baseline	Passed	Passed

4.9 Interoperability

Interoperability tests were performed between the vendor SCMs and the Arcom Viper Gold Standard. In the case of both vendors, their SCMs fully interoperated with the Gold Standard computers running the same version of SCADASafe software to which the SCM was developed (see Table 11).

Table 11. Interoperability Matrix

Vendor	Cipher Suite	Gold Standard Interoperation
SCM-1	1 and 2	Passed
SCM-2	1 and 2	Passed

5.0 Observations, Concerns and Conclusions

The purpose of the performance tests undertaken in this task was to measure vendor products developed to the AGA-12 standard, when operated in SCADA environments patterned after those of the electric industry. This report presents performance test data to assist organizations evaluating AGA-12 technology, but does not attempt to quantify whether the performance will be acceptable for their particular application. This section of the report provides final thoughts on observations, concerns, and conclusions derived as a result of performance testing activities.

5.1 Observations

The AGA-12 Part 2 standard defines modes of operation not implemented in vendor solutions. As a result, the analysis contained in this report cannot definitively determine the comprehensive impact on communication for the complete standard. Nevertheless, the report does provide a detailed assessment of the impact of the partial vendor implementations for a variety of control system telemetry and control environments.

The performance differences between PE and CTR mode were surprising; PE mode did not outperform CTR mode as expected. The operational model prepared by GTI demonstrates the theoretical differences between CTR and PE mode. The model indicates that PE mode would introduce less latency than CTR mode. In practice, however, both vendor solutions did not support the operational model's prediction. In his book *Secrets and Lies*, Bruce Schneir (2000) discusses this very issue. The difference between a good encryption algorithm and implementation of that algorithm can cause unexpected consequences. From a performance perspective, the source code itself needs to be examined to determine why measured performance and anticipated performance differ for the cipher suites.

Significant variability was determined to exist in the typical communication behavior of some field devices (see Table 2). This table summarized the variability of one field device. The relative standard deviation (RSD) column represents a measure of precision. A RSD value greater than 5% demonstrates a lack of precision in the device. The RSD values in Table 2 are calculated using data from 1 hour's worth of traffic at each baud rate and frequency. One would anticipate the RSD to decrease with larger frequency values. This table shows an unpredictable variability in communication characteristics. Referring back to the histogram for the baseline communication characteristics for FD-1 (Figure 14) shows spikes at several places (see the blue line). This observation introduces two significant issues worthy of further consideration. First, interviews with SCADA engineers identified an expected loss of communication between 1 to 3 percent. This raises the issue of whether field device response time variability can account for the lost communication. The second issue concerns the possibility that the variability in communication may represent a "fingerprint" of the field device. More research is needed in these areas to determine if devices can be identified by simply monitoring response times.

5.2 Concerns

A principal concern observed during performance testing activities is the impact of repeated decommissioning of SCM-1 devices upon SCADA communication. To avoid the problem, the device had to be taken out of service with all data communication cables removed prior to making a configuration change. This repeated decommissioning was unpredictable and may be a barrier to implementation. During laboratory performance testing, the reliability of vendor equipment was observed. While not directly related to performance, reliable operations of vendor equipment will directly impact the willingness of asset owners to adopt any technology. The security objectives for control systems are personnel safety, reliable operations, data integrity, and lastly confidentiality. The AGA-12 devices provide data confidentiality and integrity, but SCM-1 devices adversely impacted reliability. An installed security appliance that is inoperable provides no added value to the field device. No SCADA data, no control functions, and no remote engineering access are supported. A decommissioned device is equivalent to a failed modem. Security solutions cannot adversely impact reliable operations or personnel safety.

5.3 Conclusions

The AGA-12 vendor CMs will add latency to serial SCADA communication. As anticipated, the impact is greatest in low-bandwidth environments, where small message sizes are the norm. In addition, the impact is greater on timing-based protocols, such as Modbus, than for length-based protocols, such as DNP3. Round-robin telemetry environments will be impacted to a greater extent than time-slice environments given the cumulative effect the additional latency has for each request and associated response. The potential impact on telemetry environments increases when multiple telemetry requests are made during a time-slice window. Finally, the additional latency on control commands for select before operate implementations should be noted.

The results provide industry (asset owners, AGA vendors, standards groups, etc.) with unbiased information regarding the expected impact AGA-12 cryptographic modules introduce into SCADA communications. While telemetry schemes vary from one organization to the next, the representative measurements in the report provide a good basis for determining the impact upon telemetry and control for any utility. The value to industry comes from testing in an unbiased manner with common protocols and field device equipment. Industry can use the results as benchmarks to accompany purchasing decisions. The results do not convey a guarantee the vendor cryptographic modules will function with the specific protocols, telemetry schemes, and communication media in production utility environments. The test environment was modeled after the telemetry schemes typically found in electric utilities. Modbus and DNP were selected because of the high level of use in multiple critical infrastructure sectors.

The results are sufficient to provide a general impact assessment. The use of protocols, field device equipment and telemetry schemes is unique to the asset owner. An asset owner should not assume that these laboratory tests will match their operating environment directly. Testing using the individual asset owner's equipment, protocols, telemetry schemes, and communication media should still be performed in a non-production environment prior to making purchasing decisions.

6.0 References

Gas Technology Institute. 2004. “Protecting SCADA Communications.” http://www.gastechnology.org/webroot/app/xn/xd.aspx?it=enweb&xd=4reportspubs%5C4_8focus%5Cprotectingscadacommunications.xml

Hadley, M.D., and K.A. Huston. 2006. “AGA-12, Part 2 Performance Test Plan.” PNNL-SA-53037. National SCADA Test Bed, Pacific Northwest National Laboratory, Richland, WA. http://www.oe.energy.gov/DocumentsandMedia/AGA_12_Part_2_Performance_Test_Plan.pdf\

http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf

NIST. 2002. “The Keyed-Hash Message Authentication code (HMAC).” FIPS Pub 198, http://csrc.nist.gov/publications/fips/fips198/fips-0198a.pdf

Schneir, B. 2000. Secrets and Lies. John Wiley & Sons. Hoboken, NJ