

Secure SCADA Communication Protocol Performance Test Results

M.D. Hadley
K.A. Huston

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



This document was printed on recycled paper.

Secure SCADA Communication Protocol Performance Test Results

M.D. Hadley
K.A. Huston

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 cryptographic implementation and performance impact of the Secure SCADA Communication Protocol (SSCP) upon supervisory control and data acquisition (SCADA) communications. This report presents performance test data derived from proof of concept implementations of the SSCP.

The cryptographic review utilized the Federal Information Processing Standards (FIPS) guidance for hashed message authentication code implementations and the SSCP source code. The performance testing task built upon the test plan developed for the previous American Gas Association (AGA) performance testing project. The test equipment, data analysis techniques, and communication equipment and methods of this test plan were directly duplicated. However, the telemetry methods were altered in response to lessons learned from discussions with asset owners. Each proof of concept implementation of the SSCP was evaluated for performance impact, the source of additional latency identified, and the reduced latency associated with varying the length of the authenticator identified.

While gas, water and electric industries all utilize SCADA systems, the manner in which they are used differs significantly. Common telemetry schemes in the gas industry request information from remote sites on the order of every 60 to 90 seconds. Water system telemetry requirements may involve requests every 10 to 15 minutes whereas SCADA 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 was to evaluate the SSCP when operated in SCADA environments patterned after the electric industry. By examining the impact within more demanding environments, the impact for less demanding environments can be inferred.

To summarize findings, the performance tests identified that the SSCP will introduce more latency i.e., delays communications in low bandwidth environments and when implemented as two “bump in the wire” microcontroller devices. Embedding the technology into end devices will dramatically reduce the amount of latency introduced by the SSCP. The cryptographic review provided reinforcement that the SSCP developers followed good engineering practices when designing and implementing the authentication algorithms. Impacts on latency of commercial implementation may be different from the tested devices. This report does not attempt to quantify whether the SSCP performance impact will be acceptable in the SCADA applications of individual asset owners.

Acronyms and Definitions

Acronym	Definition
AGA	American Gas Association
DNP	Distributed network protocol
FEP	Front end processor
FIPS	Federal Information Processing Standards
HMAC	Keyed-hashed message authentication code
IC	Industrial computer
I/O	Input/output
MC	Microcontroller
NIST	National Institute of Standards and Technology
PC	Personal computer
PNNL	Pacific Northwest National Laboratory
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SSCP	Secure SCADA communication protocol

Contents

Summary.....	iii
Acronyms and Definitions.....	iv
Figures.....	vi
1.0 Introduction.....	1
2.0 Test Environment.....	2
2.1 Telemetry Scenario.....	2
3.0 Cryptographic Review.....	3
4.0 Performance Test Results.....	5
4.1 Baseline Communication.....	5
4.2 SSCP Protected Communication.....	7
4.2.1 <i>Embedded SCADA Mater to Industrial PC (IC)</i>	9
4.2.2 <i>Embedded SCADA Master to Microcontroller (MC)</i>	10
4.2.3 <i>Industrial PC to Industrial PC</i>	12
4.2.4 <i>Microcontroller to Microcontroller</i>	13
4.3 Summary Comparison.....	14
4.4 Latency Details.....	15
4.5 Control Tests.....	17
5.0 Conclusion.....	18

Figures

Figure 1. Relative timing of telemetry request typically of electric power industry practices in seconds.....	2
Figure 2. Baseline latency by baud rate.....	7
Figure 3. Various SSCP implementation methods	8
Figure 4. Round-trip request and response circuit between embedded SCADA and RTU via an industrial PC.....	9
Figure 5. Latency of round-trip communication versus baud rate for configuration of Figure 4	10
Figure 6. Round-trip request and response circuit between embedded SCADA and RTU via a microcontroller.....	10
Figure 7. Latency of round-trip communication versus baud rate for configuration of Figure 6	11
Figure 8. Round-trip request and response circuit between master substation server and RTU via two industrial PCs.....	12
Figure 9. Latency of round-trip communication versus baud rate for configuration of Figure 8	13
Figure 10. Round-trip request and response circuit between master substation server and RTU via two two microcontroller concept boards.....	13
Figure 11. Latency of round-trip communication versus baud rate for configuration of Figure 10.....	14
Figure 12. Latency comparison for all topologies	15
Figure 13. Latency component values versus baud rate	16
Figure 14. Latency versus HMAC length.....	16
Figure 15. Latency impacts for imbedded solutions.....	17
Figure 16. Control command latency at 2400 baud for each evaluated implementation combination.....	17

Tables

Table 1. Baseline communication results	6
Table 2. Response times versus baud rate for configuration shown in Figure 4	9
Table 3. Response times versus baud rate for configuration shown in Figure 6	11
Table 4. Response times versus baud rate for configuration shown in Figure 8	12
Table 5. Response times versus baud rate for configuration shown in Figure 10	14

1.0 Introduction

The U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, requested the services of Pacific Northwest National Laboratory (PNNL) to investigate the latency impact of the secure SCADA communications protocol (SSCP) on serial communication. This effort builds upon previous work performed at PNNL to measure the latency introduced by vendor products built to the American Gas Association 12, Part 2 standard. In both investigations, serial communication environments patterned after those used by electric power companies were modeled in a laboratory setting. SCADA communications are time sensitive, and the introduction of latency can result in a loss of information. The objective of this effort is to measure the additional time the SSCP introduces into the serial communication environment.

The results of performance and security testing of an innovative control system communications authenticator technology developed by the Pacific Northwest National Laboratory (PNNL) are reported in this document. The SSCP is currently available in three proof of concept implementations: embedded on a SCADA input/output (I/O) or front end processor (FEP) server, as a bump in the wire industrial personal computer (PC) solution, and also on a microcontroller concept board. Each implementation utilizes different processor speeds, contains varying amounts of available memory, and represents equipment utilized in the electric industry. Combinations of these implementation options were also examined.

The SSCP implementations utilize a 12-byte authenticator by default. Testing with authenticators ranging from 4 bytes to the maximum number of bytes supported by the message authentication algorithms were used (either 20 04 32 depending on the algorithm) and the differences in latency measured. The performance tests utilized the distributed network protocol (DNP) and typical telemetry schemes for the electric industry. The impact upon control commands was also captured. Prior to measuring the latency of SSCP authenticated communication, unauthenticated communication was captured to establish a baseline. The cryptographic review compared the SSCP source code with Federal Information Processing Standards (FIPS) guidance, as well as address questions received from SCADA vendors.

The various test environments are discussed in Section 2. Section 3 contains a cryptographic review (to explore if SSCP developers followed approved methods and protocols to implement authentication), while Section 4 details the results for each of the configuration tested. Overall conclusions are contained in Section 5.

2.0 Test Environment

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

- Null modem cables
- Dell PowerEdge 1850
- Sage2300 remote terminal unit (RTU)
- ST62K shuttle computers
- Rabbit semiconductor microcontroller concept boards
- Triangle MicroWorks SCADA Data Gateway

This equipment was operated at communication rates of 1200, 2400, 4800, 9600, and 19200 baud and polling frequencies of 1, 2, 3, and 5 seconds.

2.1 Telemetry Scenario

Figure 1 shows a typical telemetry scenario for the electric power industry. This telemetry approach differs from the AGA testing previously performed and was modified to more accurately reflect electric system telemetry configurations. Multiple types of data are requested at different intervals. The status message interval was varied during performance testing activities, while analog and accumulator requests were submitted once per minute. When more than one request is made during a time period, a 100-millisecond (mS) delay is used to ensure the communication channel is ready for the next request.

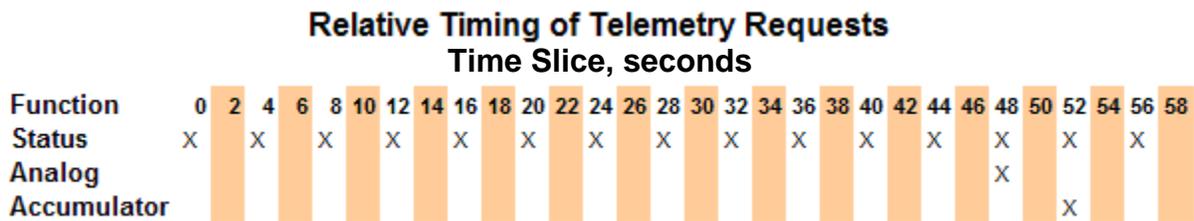


Figure 1. Relative timing of telemetry request typically of electric power industry practices in seconds

3.0 Cryptographic Review

The SSCP utilizes a hashed message authentication code (HMAC) as the authentication mechanism. A mathematical function, National Institute of Standards and Technology (NIST) approved SHA-1 or SHA-256 algorithm, is used by the message sender to produce the HMAC value that is formed by condensing a unique identifier + message input + the symmetric key. The HMAC is sent to the message receiver along with the message and unique identifier. The receiver computes the HMAC based on the received message + unique identifier + the symmetric key. The receiver compares the result computed with the received HMAC. If the two values match, the message has been correctly received, and the receiver is assured that the message is authentic.

The introduction of a unique identifier for each message is needed, given predictable and repeatable SCADA data. Without a unique identifier, the HMAC value would repeat as well, and would provide insufficient message integrity. Two separate fields comprise the unique identifier: a 4-byte time field and a 2-byte sequence number. Time is maintained to the degree of accuracy of a second, and the sequence number is used for multiple communications within a 1-second time window. Using this scheme ensures that the HMAC provides a unique value for repeatable messages.

While the SSCP employs an HMAC to provide message authentication, the HMAC may be truncated to support low bandwidth environments. SSCP developers followed this guidance from NIST (2002¹) when truncating the HMAC:

“A well-known practice with message authentication codes is to truncate their output (i.e., the length of the HMAC used is less than the length of the output of the hashing function L). Applications of this standard may truncate the output of HMAC. When a truncated HMAC is used, the t leftmost bytes of the HMAC computation shall be used as the message authentication code. The output length, t , shall be no less than four bytes (i.e., $4 \leq t \leq L$). However, t shall be at least $L / 2$ bytes (i.e., $L/2 \leq t \leq L$) unless an application or protocol makes numerous trials impractical. For example, a low bandwidth channel might prevent numerous trials on a 4 byte message authentication code, or a protocol might allow only a small number of invalid message authentication code attempts.”

By truncating the HMAC, the impacts upon latency can be tailored to the communication environment. It is recommended that key updates occur more frequently, when shorter HMAC lengths are used.

The final area reviewed for proper cryptographic implementation covers both session negotiation and key updates. The SSCP supports two methods for each, Diffie-Hellman and pre-shared session keys. In the first method, the SSCP incorporates a pre-shared seed

¹ NIST. 2002. “The Keyed-Hash Message Authentication Code (HMAC).“
<http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>

key to encrypt the Diffie-Hellman session negotiation event. To mitigate the frequent use of a seed key, key history is maintained by both master and remote devices. Instead of reverting to the seed key, the last known good key is used first to re-establish communication after an interruption of communication or power loss. Diffie-Hellman allows either device to request key updates. Given the distributed nature of control systems, the SSCP implementation requires that key updates are always initiated by the master. Finally, Diffie-Hellman can be implemented in one or two round trip methods. The SSCP utilizes the two round trip method because it is more secure.

Key update algorithms require more processor resources than authentication algorithms. In response, the SSCP supports pre-shared keys for remote devices with limited processing capabilities. This approach builds upon the cryptographic one-time pad algorithm, where a message is encrypted with a random key that is known by both the sender and receiver and used only once. The primary difference is that the pre-shared keys implemented in the SSCP are unique for a session, not each individual message. The strength of this approach lies with the randomness of the keys and that each key is used only once. Flash memory in a device can store enough keys in 3 MB to update keys once per hour for 10 years. Session negotiation and key updates become a simple offset into the list of random pre-shared keys.

When the authentication solution is embedded on an I/O server, all key update activities are logged. Logging provides support for regulatory compliance and the identification of potential intrusion attempts.

Future SSCP implementations in commercial products need to follow these guidelines to ensure a strong, robust authentication solution. Cryptographic implementations that are not well done provide a false sense of security.

4.0 Performance Test Results

The following tables and charts were generated using the data from the tests defined above. The AGA performance testing activity utilized a protocol analyzer to capture data. The embedded nature of one SSCP implementation required a different approach be used to maintain consistency. As a result, the data was captured using log files generated by the Triangle MicroWorks SCADA Data Gateway product. A representative sample of performance impact results are presented below to illustrate the main findings. Additional reports or views of the test data can be provided upon request.

Before measuring the impact the SSCP protocol has upon SCADA communication, a series of baseline tests were conducted. The DNP protocol was used with communication rates of 1200, 2400, 4800, 9600, and 19200 baud. Telemetry requests per the scheme identified in Section 2 were made with 1-, 2-, 3-, and 5-second time periods. Baseline control requests were also captured. Addition of the SSCP will add latency to each telemetry or control request and response. The amount of latency is dependent upon many factors, including which SSCP implementation is used, the baud rate, and the length of the authenticator. The baseline tests will allow the impact to be accurately measured.

4.1 Baseline Communication

Before the latency impact that the SSCP imposes on telemetry and control requests can be measured, the normal communication times of the SCADA requests had to be determined. 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 the consistency of the PNNL test environment, a small

sample size was used for the analysis. Table 1 summarizes baseline communication characteristics for each baud rate. The columns in Table 1 represent the following:

Baud	The communication rate used for the performance test
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 in the sample.
Rel Stdev	The relative standard deviation is a percentage calculated by dividing the standard deviation by the average. The higher the relative standard deviation, the more variability that exists for the communication.

The values in the table depict the time required for the request to be sent to the remote device and the response to be received by the SCADA Data Gateway.

Table 1. Baseline communication results

Baseline Results					
Null Modem Connection					
Baud	Min (ms)	Max (ms)	Average (ms)	Stdev (ms)	Rel Stdev (ms)
1200	328	641	502	132	26.3%
2400	172	391	296	67	22.8%
4800	109	250	183	41	22.1%
9600	63	188	134	34	25.5%
19200	47	156	104	33	31.8%

Baseline measurements determined that analog and accumulator requests provided identical response times with the PNNL test environment. Analog requests are used to represent both types of requests in the following charts. Figure 2 depicts expected behavior, i. e., communication times decrease linearly as the baud rate increases for both status and analog requests.

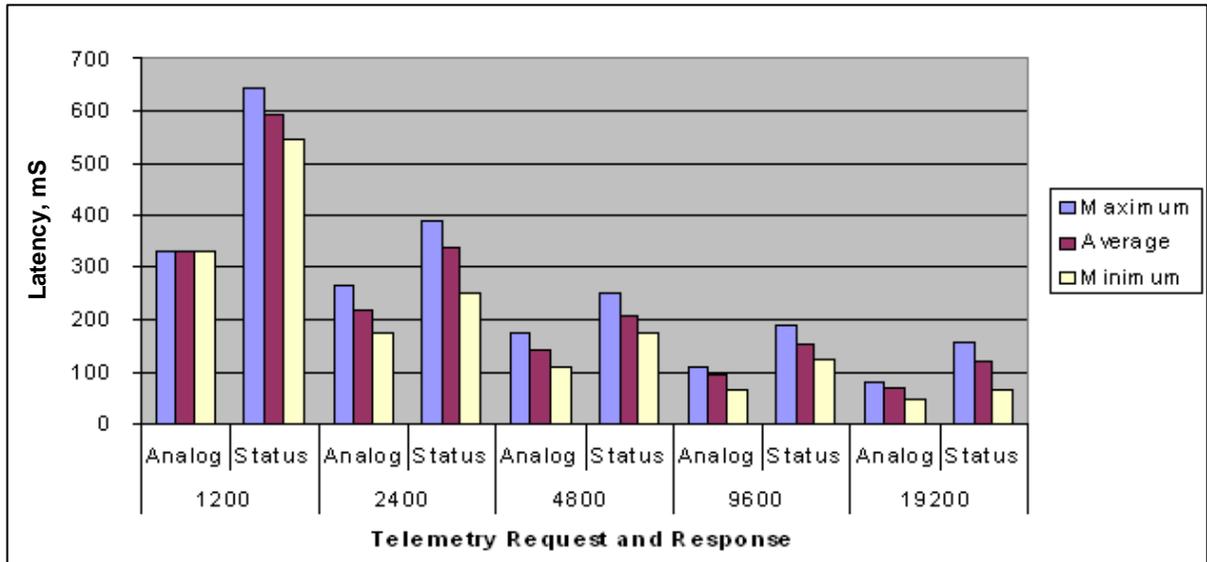


Figure 2. Baseline latency by baud rate

4.2 SSCP Protected Communication

Introduction of the SSCP into a serial communication channel will add latency to communication. The latency impact upon communication is dependent upon many factors including baud rate, communication media, telemetry scheme, field device selection, and the length of the authenticator. The purpose of this section is to show the impact on communication in various SCADA configurations.

During laboratory testing, four different SSCP implementation combinations were used. The SSCP software was embedded on a SCADA master server, a microcontroller, and an industrial computer. The four combinations were:

- Embedded SCADA master server to microcontroller (MC)
- Embedded SCADA master server to industrial PC (IC)
- Microcontroller to microcontroller
- Industrial PC to industrial PC.

Figure 3 illustrates the various implementation approaches.

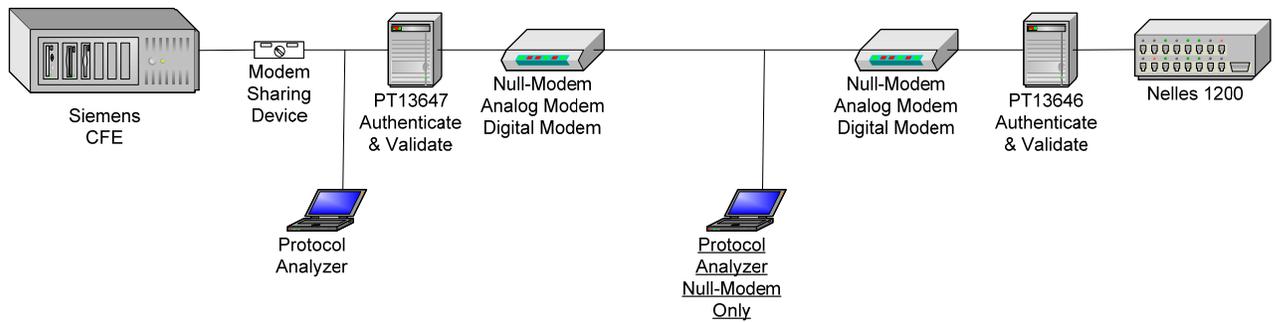


Figure 3. Various SSCP implementation methods

The currently embedded software and the bump in the wire industrial PC or microcontroller implementations utilize the following process to authenticate and validate communication:

- The SCADA master generates the telemetry or control request for the RTU.
- The embedded SSCP software intercepts the request to the communication port.
- The embedded SSCP software generates a unique identifier.
- The embedded SSCP software calculates the authenticator based upon the SCADA message, the unique identifier, and the destination's unique key.
- The embedded SSCP software sends the authenticated message with the SSCP additions to the original communications port.
- The SSCP software on the microcontroller or industrial PC receives the requests and waits for the entire message to arrive.
- The SSCP software performs message integrity checks to ensure the message has not been replayed or injected.
- The SSCP software validates the authenticator to ensure the message has not been altered.
- The SSCP software extracts the original message.
- The original message is sent to the RTU.
- The field device processes the request from the SCADA master.
- The steps are reversed for the response from the RTU to the SCADA master.

4.2.1 Embedded SCADA Master to Industrial PC (IC)

The concept implementations of the SSCP require that a round-trip request and response be buffered and transmitted four times between the SCADA master and the RTU as indicated in Figure 4.

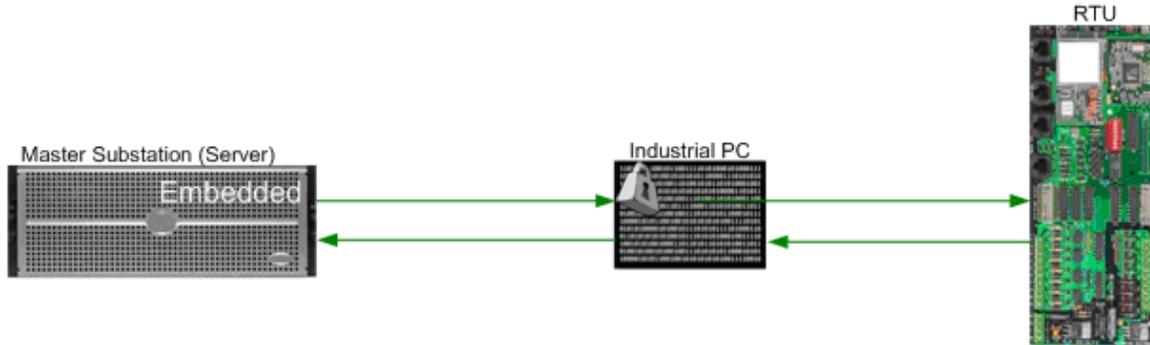


Figure 4. Round-trip request and response circuit between embedded SCADA and RTU via an industrial PC

Table 2 summarizes response times for each baud rate for all telemetry messages in the captured data sample. Column titles are as defined for Table 1. The SSCP was implemented as a software solution on the SCADA master and on an industrial PC for the RTU. As baud rates double, it would be anticipated that the response time decreases proportionately. The captured data validated expected communication behavior.

Table 2. Response times versus baud rate for configuration shown in Figure 4

Server To Industrial PC					
Null Modem Connection					
Baud	Min (ms)	Max (ms)	Average (ms)	Stdev (ms)	Rel Stdev (ms)
1200	1187	1735	1513	272	18.0%
2400	640	953	808	131	16.2%
4800	328	547	455	70	15.3%
9600	188	344	277	44	15.9%
19200	109	250	180	36	20.1%

Figure 5 depicts the latency imposed on a telemetry request and response utilizing a 12-byte authenticator. Shorter authenticator sizes will significantly reduce the latency impact. The latency impact is significantly reduced as the baud rate rises, becoming a smaller percentage increase when compared to the baseline.

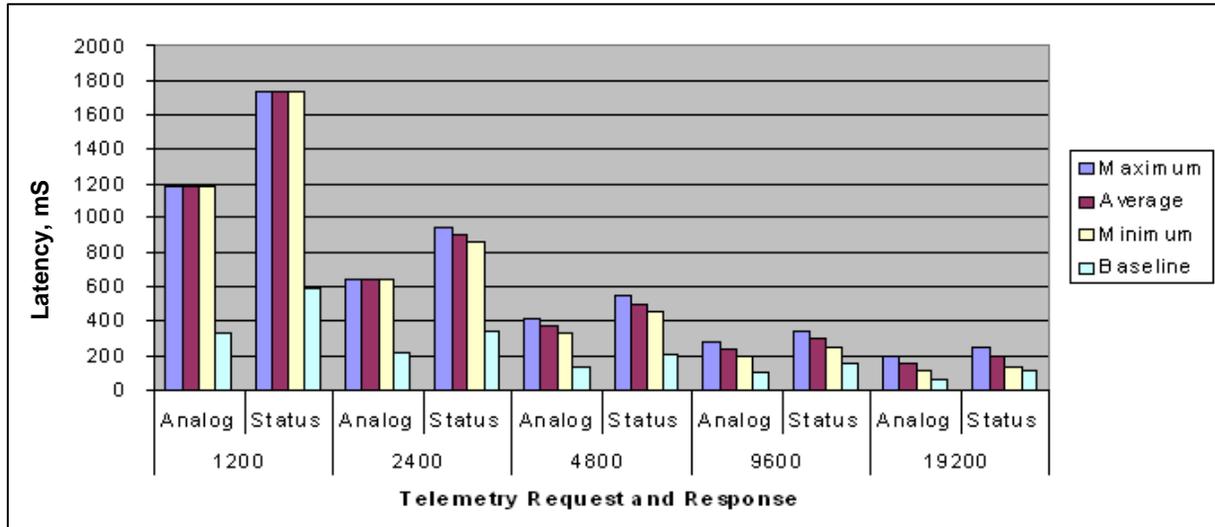


Figure 5. Latency of round-trip communication versus baud rate for configuration of Figure 4

4.2.2 Embedded SCADA Master to Microcontroller (MC)

The SSCP was implemented as a software solution on the SCADA master and on a microcontroller concept board for the RTU as illustrated in Figure 6. For this configuration, Table 3 summarizes response times versus baud rates for all telemetry messages in the captured data sample. Column titles in Table 3 are as defined in Table 1.

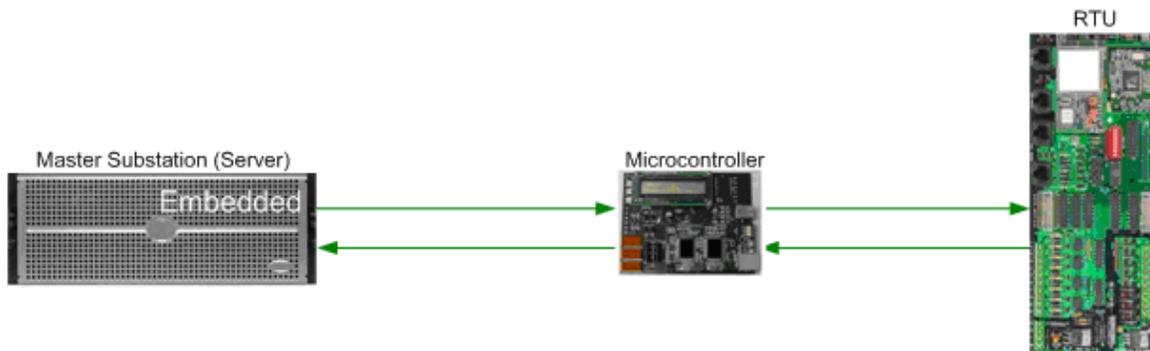


Figure 6. Round-trip request and response circuit between embedded SCADA and RTU via a microcontroller

Table 3. Response times versus baud rate for configuration shown in Figure 6

Server To Microcontroller Null Modem Connection					
Baud	Min (ms)	Max (ms)	Average (ms)	Stdev (ms)	Rel Stdev (ms)
1200	1297	1735	1543	220	14.3%
2400	703	1047	911	116	12.8%
4800	438	656	576	74	12.9%
9600	297	469	395	45	11.3%
19200	250	359	305	26	8.6%

As previously noted, when the baud rates double, the response time decreases proportionately. The captured data validate expected communication behavior. These results also demonstrate that while the performance impact upon communication is partially based upon processor speed (the industrial PC contains a Pentium 4 operating at 2.8 GHz and the microcontroller contains a 44.2-MHz processor), the vast majority of the latency is associated with the length of the authenticator and capturing, buffering, and retransmitting the SCADA message.

Figure 7 depicts the latency added to a telemetry request and response utilizing a 12-byte authenticator. The latency impact is significantly reduced as the baud rate rises, becoming a smaller percentage increase when compared to the baseline.

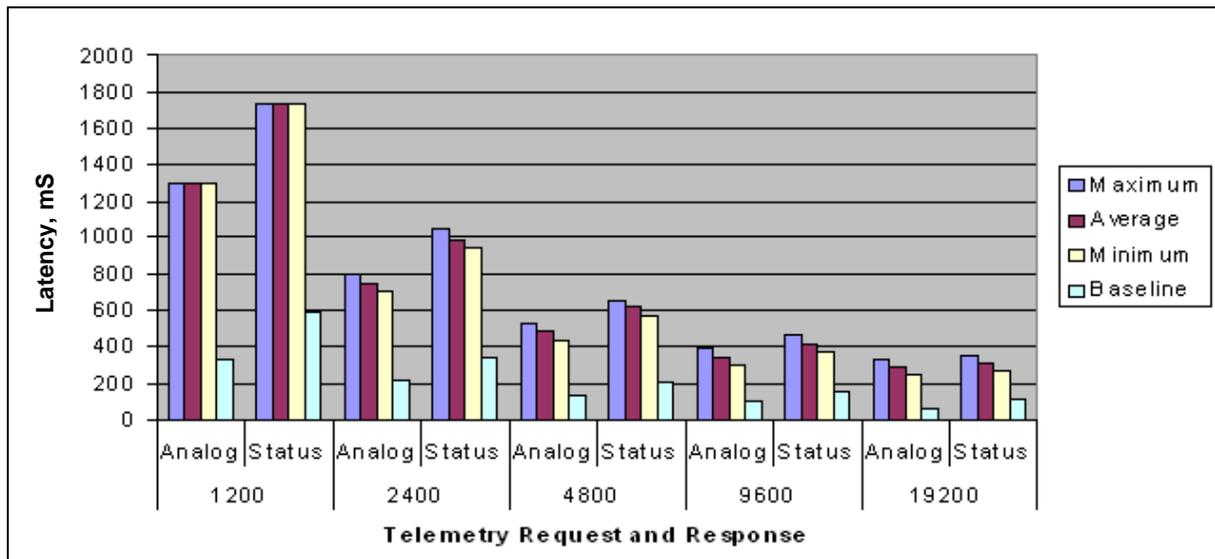


Figure 7. Latency of round-trip communication versus baud rate for configuration of Figure 6

4.2.3 Industrial PC to Industrial PC

The SSCP was next implemented using two industrial PCs, one for each side of the communication channel as illustrated in Figure 8. Table 4 summarizes response times for this configuration versus baud rates for all telemetry messages in the captured data sample. Column titles in Table 4 are as defined in Table 1.

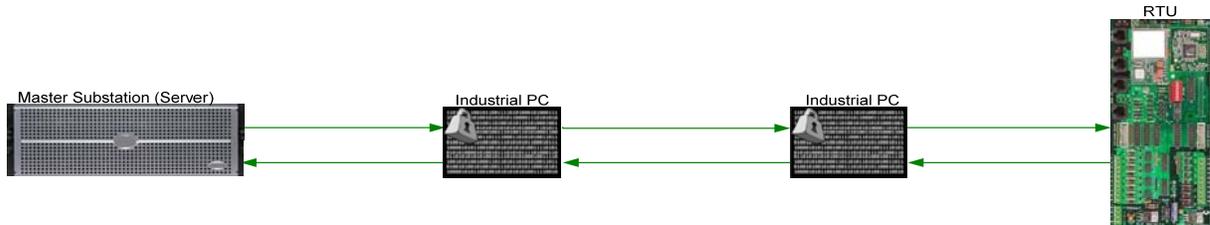


Figure 8. Round-trip request and response circuit between master substation server and RTU via two industrial PCs

As baud rates double, response time is expected to decrease proportionately. It is also reasonable to expect that this configuration would add more latency than that of the embedded SSCP implementations. The captured data validate both aspects of expected communication behavior.

Table 4. Response times versus baud rate for configuration shown in Figure 8

Industrial PC To Industrial PC					
Null Modem Connection					
Baud	Min (ms)	Max (ms)	Average (ms)	Stdev (ms)	Rel Stdev (ms)
1200	1640	2407	1996	389	19.5%
2400	844	1266	1090	167	15.3%
4800	422	704	586	94	16.0%
9600	219	407	326	55	17.0%
19200	141	266	210	034	16.0%

Figure 9 depicts the latency upon a telemetry request and response utilizing a 12-byte authenticator. The latency impact is significantly reduced as the baud rate rises, becoming a smaller percentage increase when compared to the baseline.

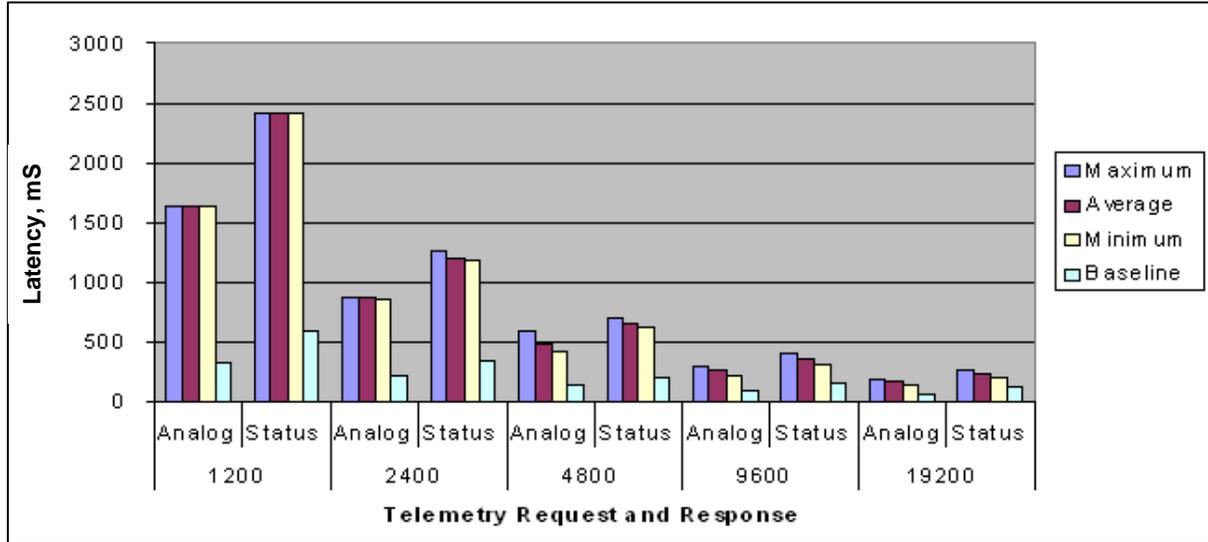


Figure 9. Latency of round-trip communication versus baud rate for configuration of Figure 8

4.2.4 Microcontroller to Microcontroller

Finally, the SSCP was implemented using two microcontroller concept boards, one for each side of the communication channel as indicated in Figure 10. Table 5 summarizes response times for this configuration versus baud rates for all telemetry messages in the captured data sample. Column titles in Table 5 are as defined in Table 1.

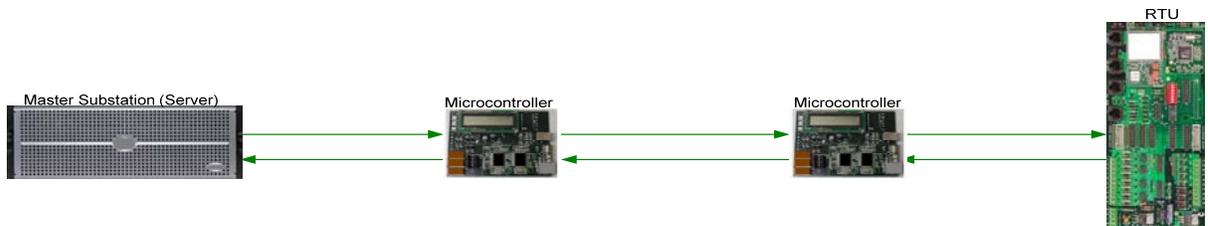


Figure 10. Round-trip request and response circuit between master substation server and RTU via two microcontroller concept boards

Again it is seen that as baud rates double, response time decreases proportionately. The expectation that this implementation would add more latency than the embedded SSCP implementations is validated by the captured data.

Table 5. Response times versus baud rate for configuration shown in Figure 10

Microcontroller to Microcontroller Null Modem Connection					
Baud	Min (ms)	Max (ms)	Average (ms)	Stdev (ms)	Rel Stdev (ms)
1200	1640	2407	1996	389	19.5%
2400	984	1422	1251	204	16.3%
4800	610	907	793	101	12.8%
9600	438	641	551	64	11.6%
19200	344	516	437	46	10.6%

Figure 11 depicts the latency imposed on a telemetry request and response using the configuration of Figure 10 utilizing a 12-byte authenticator. The latency impact is significantly reduced as the baud rate rises, becoming a smaller percentage increase when compared to the baseline.

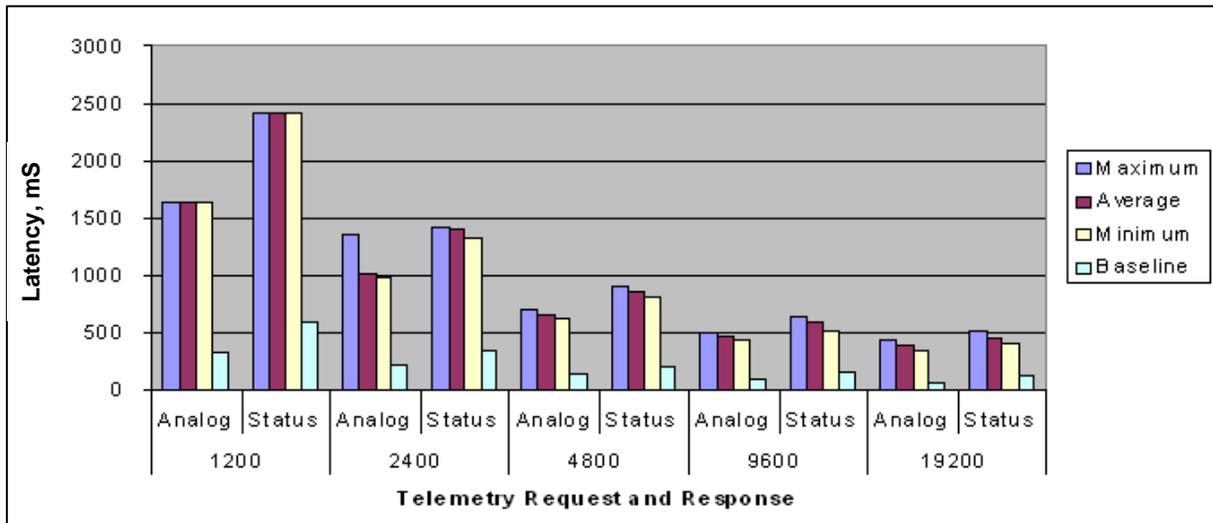


Figure 11. Latency of round-trip communication versus baud rate for configuration of Figure 10

4.3 Summary Comparison

Figure 12 compares all topologies against the baseline. It is apparent that the embedded solutions with either the IC or MC are faster than implementing two intermediate devices between the master and RTU.

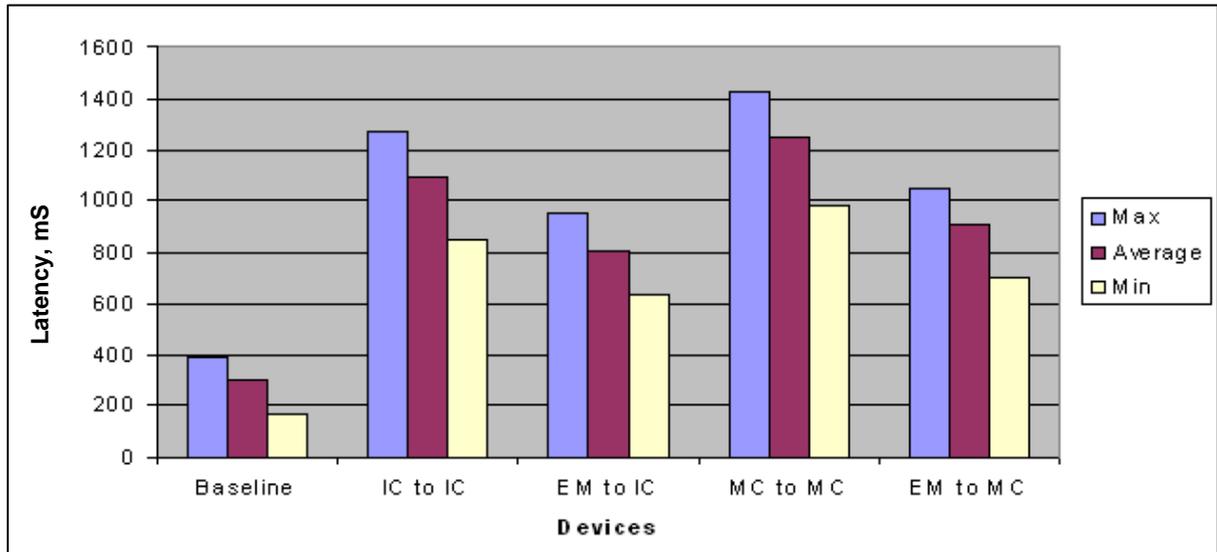


Figure 12. Latency comparison for all topologies

4.4 Latency Details

Figure 13 depicts the sources of latency for the round-trip authentication and validation process when the SSCP is implemented as a software solution on the SCADA master and on an industrial PC for the remote RTU. Portions of the SSCP implementation introduce static latency. For example, the length of the information that uniquely identifies the SCADA message and the amount of time to calculate and validate the authenticator does not vary. The largest single factor adding latency is labeled retransmit. Retransmit includes the latency associated with capturing, buffering, and retransmitting the message by the industrial PC. In this graph, the authenticator is 12 bytes. Request and response headers contain 13 bytes for the unique identifier, as well as the processing time to calculate the authenticator. As baud rate increases, the retransmit impact upon latency remains the largest single factor.

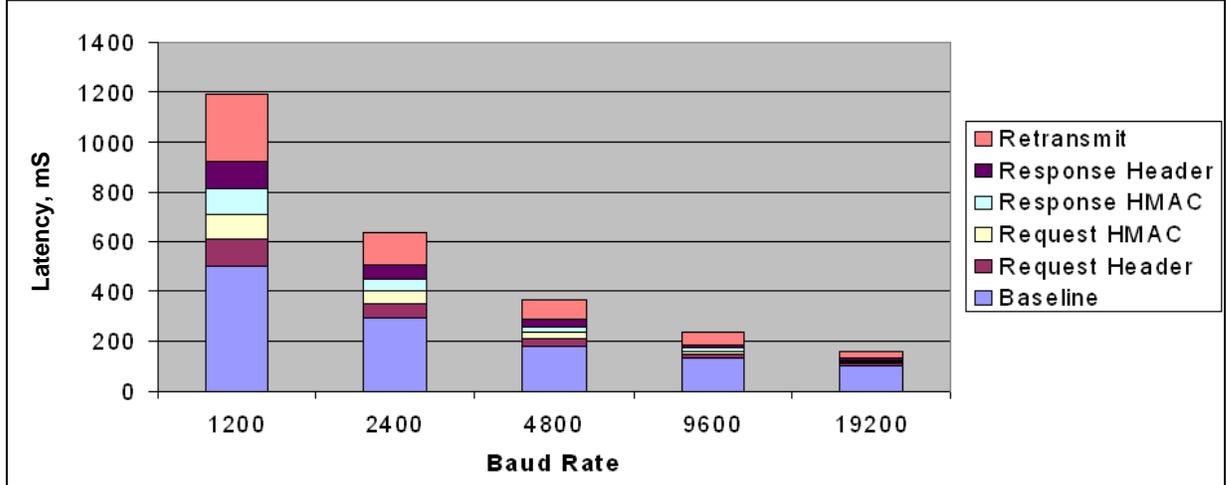


Figure 13. Latency component values versus baud rate

Figure 14 illustrates the impact that the length of the authenticator has upon latency. A SHA-1 hashing algorithm will produce a 20-byte message authentication code, and a SHA-256 algorithm will produce a 32-byte authenticator. The graph depicts the impact upon a request or response, but not round-trip communication. Reducing the length of the authenticator from 20 to 4 bytes reduces the latency from 166 to 33 mS for a telemetry request. These values need to be doubled to obtain the total latency of round-trip communication.

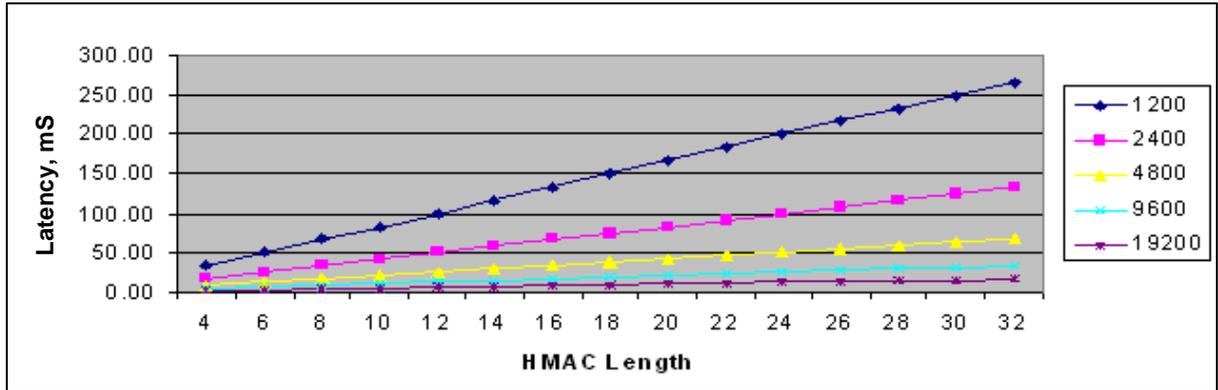


Figure 14. Latency versus HMAC length

When the SSCP is embedded natively into the SCADA master and RTU, latency will be significantly reduced. Figure 15 depicts the anticipated embedded latency impact with a 4-byte authenticator. Embedding the SSCP removes the retransmit latency and the end result is minimal additional latency.

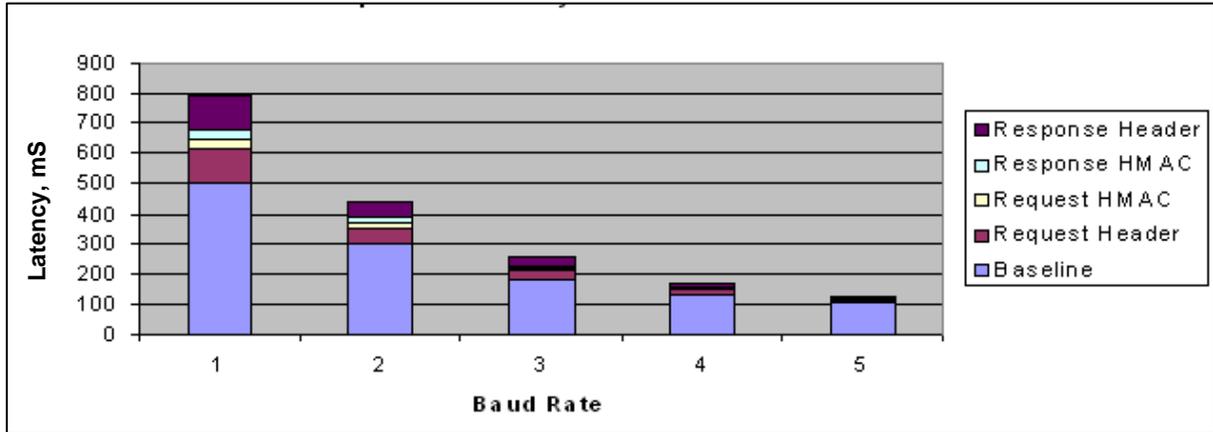


Figure 15. Latency impacts for imbedded solutions

4.5 Control Tests

The control tests illustrated in Figure 16 summarize the findings for each implementation combination. Control commands were issued using the “select-before-operate” DNP method. This method requires two requests and responses before the control function is enacted by the RTU. The impact on control follows the telemetry impact detailed earlier in this report.

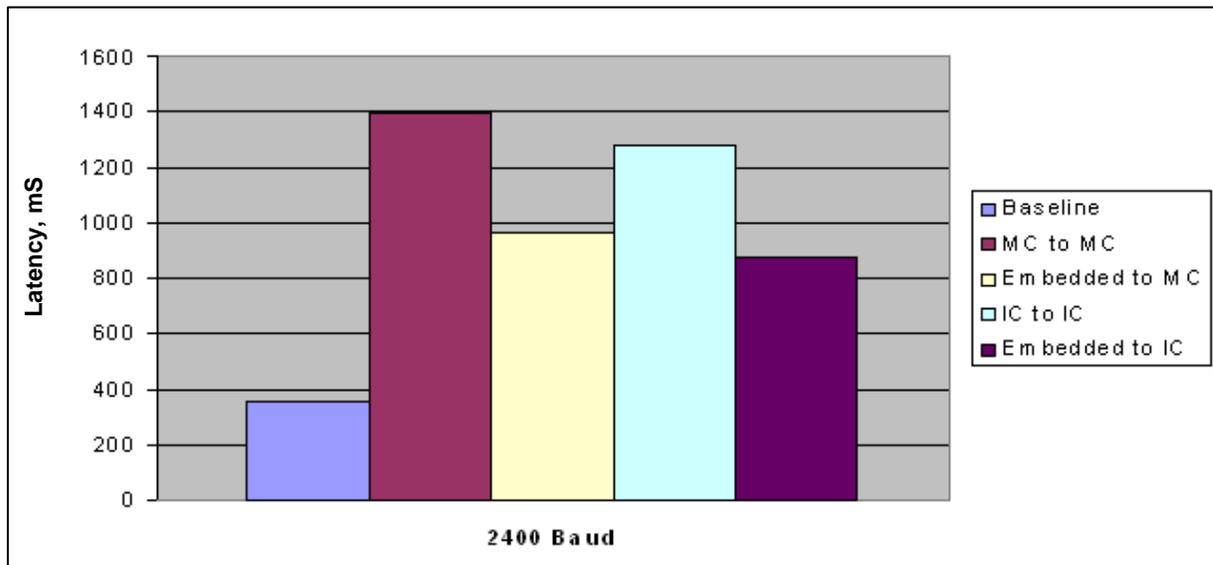


Figure 16. Control command latency at 2400 baud for each evaluated implementation combination

5.0 Conclusion

Optimal performance of the SSCP will be achieved once the technology is natively embedded into SCADA master servers and field devices. Current proof-of-concept implementations more than double baseline communication time. The anticipated latency impact for embedded solutions with the 4-byte authenticators only adds about 60% of the baseline contribution. Because maintaining support for legacy devices is critical, however, the SSCP must be available for implementation as an inexpensive solution that can be added to legacy SCADA infrastructure. The above performance tests demonstrated that processing power does not influence latency to the same extent as retransmission of the message or the length of the authenticator. This implies that SSCP devices that support legacy systems will not require robust processors or vast amounts of memory.