Cyber Security for Utility Operations

NETL Project M63SNL34

Sponsored by the U.S. DOE Office of Energy Assurance
Managed by NETL

Final Report

Period of Performance

October, 2003 – April, 2005

Dennis Holstein and John Tengdin, OPUS Publishing

Jay Wack and Roger Butler, TecSec, Inc.

Timothy Draelos, Sandia National Laboratories[1]

Paul Blomgren, SafeNet/Mykotronx

April 18, 2005

---

[1] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Acknowledgements

The authors wish to thank Wai Tsang and Karen Burkardsmaier of TecSec, Inc. for their assistance in writing this report and to personnel at both DTE Energy and Peoples Energy for their effort and support of the utility bench tests.

Executive Summary

Under the guidance and sponsorship of DOE's Office of Energy Assurance (OEA) and managed by the National Energy Technology Laboratory (NETL), recognizing that gaps exist in the security of utility operations, Sandia National Laboratories (SNL) and its industry partners, Mykotronx, OPUS Publishing, and TecSec, embarked on a plan to bring a comprehensive cyber security solution to the operation of utilities. In the plan, the partners realized the complexity and multiyear investment necessary to bring a complete, comprehensive solution to market, yet recognized the value of making significant steps toward this solution in a short-term project.

The standard practice within current utility operations is to manage their business operations and information with common desktop solutions. Our plan was to bridge the gap between EMS/DMS/SCADA[2] operations and related business functions, and to provide a common (comprehensive) security solution that is applicable to both domains. A cyber security solution that is common across multiple, possibly competing, utilities is a future goal not specifically addressed in our project.

Each of the industry partners brought to the team cyber security expertise and/or products that are important to the development and commercialization of a comprehensive solution.

- Sandia National Laboratories brought a new, computationally efficient approach to providing cryptographic protection of data (both confidentiality and integrity). The CS-AES algorithm provides "simultaneous" encryption and authentication of data using AES[3].
- TecSec brought a mature, commercialized software product called Constructive Key Management® (CKM®), which is well suited for immediate application to the protection of utility business operations.
- OPUS Publishing brought years of practical experience in the electrical utility industry and service on standards bodies.
- Mykotronx brought years of experience in the development of cryptographic hardware.

All the partners also brought to the project their experience with the AGA-12 standard[4] as members of the body developing or reviewing this document.

Enabling the CKM software to operate in hardware within a SCADA environment, such that a single security solution can provide comprehensive information protection throughout a utility, was a major goal of the team. This led to the development and testing of proof-of-concept cryptographic modules that incorporated the CS-AES algorithm and limited CKM functionality. The project took significant steps toward securing SCADA and maintenance port links with the same protection available to business operations, evidenced by the following accomplishments, which will facilitate the design and testing of prototype modules.

1. Provided functional requirements for cyber security for utility operations.
2. Provided a high-level design for cyber security for utility operations.
3. Integrated SNL's authenticated encryption mode, CS-AES, into TecSec's CKM software.

---

[2] EMS/DMS/SCADA is Energy Management System / Distribution Management System / Supervisory Control and Data Acquisition.

[3] AES stands for Advanced Encryption Standard and CS-AES is the Cipher-State mode of operation of AES.

[4] The American Gas Association (AGA) Report No. 12 (AGA-12) is entitled "Cryptographic Protection of SCADA Communications."

4. Developed a proof-of-concept demonstration system of critical components of our cyber security system: 1) maintenance port authentication and 2) authenticated link encryption. This activity included porting elements of CKM (with CS-AES) into a hardware platform, extending the solution to SCADA field devices, which is a missing link of comprehensive utility operation security.
5. Evaluated the demonstration system at two utilities (DTE Energy and Peoples Energy), by exercising the proof-of-concept cryptographic modules for SCADA network and maintenance port security. Both gas and electric SCADA test systems were bench-tested in our utility partners' test laboratory facilities. Modbus and one proprietary communication protocol were retrofitted with cryptographic modules for these tests. In addition, the DNP3 protocol was tested in a Remote Terminal Unit (RTU) and Intelligent Electronic Device (IED) data acquisition application. Modbus and DNP3 represent almost 80 percent of the installed base for SCADA in these industries.

The outcome of this work upheld the proposed technical approach regarding a comprehensive solution to utility cyber security. The approach is designed to be a natural extension of the security policies implemented by most utility IT departments to meet the security needs of EMS/DMS real-time operations and to protect historical SCADA data used for off-line operations and related business functions.

In summary, this project provided proof-of-concept components and accelerated the development of a future cyber security solution that comprehensively addresses EMS/DMS/SCADA operations as well as related business functions. Lessons learned from this project have already been applied to other SCADA cyber security related projects with the Department of Homeland Security (DHS).

- The basic cryptographic technology needed for role-based access control in the form of CKM is ready for integration, deployment, and rigorous testing in a wide range of operational and business applications that use SCADA and operational data. CKM provides the means to control access to any named data object and how long the permission for use is valid. This project extended elements of CKM into proof-of-concept field devices for SCADA link encryption and maintenance port authentication.
- Using CKM, the management of keying materials needed by utilities' information systems is mature and ready for deployment. The extension of a limited set of these same established techniques into Secure Cryptographic Modules was assisted by this project's proof-of-concept system. Development of a Secure Cryptographic Management System (SCMS) is still needed to gracefully integrate this technology for key management into a utility-focused operational environment and was not in the scope of this project.
- Secure remote access to field device maintenance ports is ready to be implemented within a prototype cryptographic module, which can be subjected to rigorous field-testing. Cryptographic modules used for this purpose will provide protection against cyber attack and will allow the utility to continue to use their dial-up modems for remote maintenance of field devices.
- Bench tests were conducted at Peoples Energy and DTE Energy using operational communication protocols, communication equipment, SCADA masters, and RTUs/relays. Some technical problems needing additional application engineering were encountered during the tests, but they are well understood by the design engineers. Communications problems will be easily fixed, whereas some protocol issues may require more research and discussion to resolve completely. The proof-of-concept program has provided valuable knowledge for application engineers and for standards bodies to make adjustments to accommodate diverse protocols.
- Our utility partners recognized that this project made progress towards the development of technology to secure SCADA communications, but more needs to be done before it becomes commercially feasible (e.g., reduce latency).

Table of Contents

Table of Figures

Table of Tables

1 Introduction

Under the guidance and sponsorship of DOE's Office of Energy Assurance (OEA) and managed by the National Energy Technology Laboratory (NETL), recognizing that gaps exist in the security of utility operations, Sandia National Laboratories (SNL) and its industry partners, Mykotronx, OPUS Publishing, and TecSec, embarked on a plan to bring a comprehensive cyber security solution to the operation of utilities. In the plan, the partners realized the complexity and multiyear investment necessary to bring a complete, comprehensive solution to market, yet recognized the value of making significant steps toward this solution in a short-term project.

1.1 Background

The standard practice within current utility operations is to manage their business operations and information with common desktop solutions, such as Microsoft Windows. Our plan was to bridge the gap between 1) Energy Management Systems, Distribution Management Systems, and Supervisory Control and Data Acquisition (EMS/DMS/SCADA) operations and 2) related business functions, and to provide a common (comprehensive) security solution that is applicable to both domains. A cyber security solution that is common across multiple, possibly competing, utilities is a future goal not specifically addressed in our project.

1.1.1 Industry Partners

Each of the industry partners brought to the team cyber security expertise and/or products that are important to the development and commercialization of a comprehensive solution.

- Sandia National Laboratories brought a new, computationally efficient approach to providing cryptographic protection of data (both confidentiality and integrity). The CS-AES algorithm provides "simultaneous" encryption and authentication of data using AES[5].
- TecSec brought a mature, commercialized software product called Constructive Key Management® (CKM®), which is well suited for immediate application to protection of utility business operations.
- OPUS Publishing brought years of practical experience in the electrical utility industry and service on standards bodies.
- Mykotronx brought years of experience in the development of cryptographic hardware.

TecSec, OPUS Publishing, and Mykotronx continue to be major players in drafting, editing, chairing, and reviewing the AGA-12 standard[6]. Sandia has and will be conducting a security analysis of the AGA-12 document. A more in-depth discussion of the AGA-12 effort is presented in Section 1.6.

1.1.2 Utility Partners

Peoples Energy (a gas distribution utility serving metropolitan Chicago, IL) and DTE Energy (the electric utility serving the Detroit, MI area and the gas utility serving lower

[5] AES stands for Advanced Encryption Standard and CS-AES is the Cipher-State mode of operation of AES.

[6] The American Gas Association (AGA) Report No. 12 (AGA-12) is entitled "Cryptographic Protection of SCADA Communications" [R.3] .

Michigan) brought to the team the end user perspective needed to gracefully integrate our proof-of-concept cyber security solution into existing operations. Both utilities provided laboratory and field test facilities and personnel needed to demonstrate the critical components of the solution.

1.2 Objective

Our objective was to implement two critical technologies, CS-AES and CKM, into a proof-of-concept cryptographic module designed to encrypt SCADA communications and to provide access integrity to the maintenance ports of field devices over dial-up communication channels.

The basic cryptographic technology, CKM, has been tested in military and medical applications and is ready for deployment and rigorous testing in a wide range of applications that use SCADA data. CKM provides, to the granularity of any named digital data object, the means to control who has access to the data, what they can use the data for, and how long their permission for use is valid. Prior to this project, what needed to be tested was the ability of CKM to be extended to SCADA security hardware, specifically designed to support existing utility configurations.

CS-AES is a new mode of encryption, which uses information from the internal Cipher State (CS) of the AES cipher to provide the authentication very efficiently. This methodology has a number of benefits. The encryption has some of the valuable properties of Cipher-Block-Chaining (CBC) mode, yet the encipherment and authentication mechanisms can be parallelized and/or pipelined. The authentication overhead is minimal, so the computational cost of the algorithm is very nearly that of the encryption process alone. Also, the authentication process remains resistant against some initialization vector (IV) reuse. The CS-AES algorithm is valuable to SCADA security applications because it can reduce the computational overhead of providing both encryption and authentication. The CS-AES algorithm was submitted to the National Institute of Standards and Technology (NIST) as a candidate for a new standard mode of operation for AES.

1.3 Scope

Within funding limitations, the proof-of-concept cryptographic modules were designed to demonstrate that the cryptographic functions would correctly operate in a utility operational environment. Because we focused our attention on the retrofit solution for asynchronous serial communications, the cryptographic modules needed to work with two of the most common communication protocols, Modbus and DNP (Distributed Network Protocol), and with one legacy protocol.

1.4 Target Architecture

Figure 1 shows one example of how a cryptographic system can be configured. This architecture was used to demonstrate the critical components of our comprehensive solution. In this example, a cryptographic module (CM) with both authentication and encryption capability is called an SCM and a maintenance module is called an MCM.

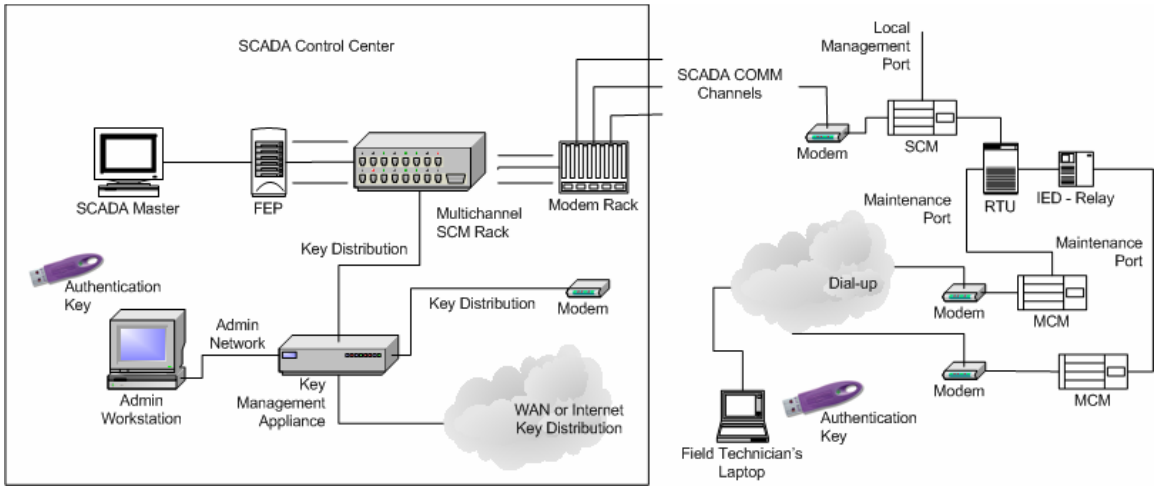

Figure 1. One Example of a Cryptographic System Configuration

In this example, the SCADA master is connected to a Front End Processor (FEP), which without cyber security would be connected to a modem rack. Rack mounted SCMs are installed between the FEP and the modem rack to provide both secure authentication and encryption on each of the SCADA communication channels. At each remote site, another SCM is installed between the modem and the Remote Terminal Unit (RTU).

Continuing with this example, Figure 1 shows that a field technician's laptop is used to access the maintenance ports over a dial-up phone line. The field technician may use an Authentication Key (hardware token) to satisfy the requirement for two-factor authentication. In this example, the technician dial-up goes to an auto-answer modem, then to the MCM, and then to the maintenance port of the RTU or to an Intelligent Electronic Device (IED), perhaps a protective relay.

In the control center, an administration workstation, shown in Figure 1, is used to manage the cryptographic keys for the system. A key management appliance is used to distribute the keys to the maintenance technicians, rack mounted SCMs, field mounted SCMs, to the MCMs, and to other cyber security devices by modem communications or Wide Area Network (WAN) or Internet/Intranet communications.

1.5 Project Chronology

This project was designed to quickly develop a proof-of-concept cryptographic module that could be field tested with our partner utilities, to gather lessons learned, to update the high-level design and commercialization plan, and provide the lessons learned to other projects. The key events are described below.

- Project kick-off meeting held at Sandia to ensure that all team members and utility partners understood the project objectives and goals.
- Functional requirements for the retrofit solution were validated by a limited survey of utilities and follow-up discussions.
- TecSec worked with Sandia to implement the ManTiCore: Encryption with Joint Cipher-State Authentication algorithm into the cryptographic modules – see [R.9] .

- Project technical interchange meeting held with all project partners, including the utility partners, to discuss the demonstration plan and to understand the configurations to be tested at both utilities.
- A demonstration at Peoples Energy resulted in quick look reports and a description of design deficiencies that needed to be corrected.
- Upgraded software/firmware in the cryptographic modules to address early lessons learned.
- A demonstration at DTE Energy resulted in quick look reports and an updated description of design adjustments that needed to be corrected.
- Comprehensive analysis of demonstration results were performed to provide lessons learned to related projects and input to the final report.
- Lessons learned from analysis and demonstration tests were used to prepare a high-level design specification for a comprehensive cyber security solution – see [R.4] .

Five Sandia technologies were introduced in the original proposal to DOE/NETL. Although the project team accomplished most of the proposed tasks of the contract, some objectives were deferred to other future projects. In summary:

- Low-Power Digital Signature Chip VHDL Design - The use of this technology was not directly applicable to this project since it involves the development of custom hardware, an expensive and time-consuming process. However, the hardware design is still viable for future use in high-speed, low-power applications requiring data authentication.
- Authenticated Encryption Algorithms - The CS-AES algorithm, one of Sandia's recently developed authenticated encryption algorithms, was integrated with TecSec's software and utilized during the project's field experiments at gas and electric utilities.
- SCADA Key Management Concepts - For this project, TecSec's Constructive Key Management (CKM) software product was readily available and satisfied many of the Sandia SCADA key management concerns.
- SCADA Security Development Laboratory (SSDL) - Sandia's SSDL was not utilized because we chose to conduct field experiments at two utilities. However, Sandia’s SCADA laboratory facilities will continue to be available for equipment evaluations and demonstration of capabilities.
- Red-team/Assessment Experience and Methods - This activity makes more sense later in the development of a cyber security solution, when a system is relatively mature (at least fully designed and implemented). Our project considered only proof-of-concept hardware components.

1.6 Relationship to Other Related Activity

Two other projects were directly related to this project - the development of a recommended practice to protect SCADA communications called AGA Report No. 12 and the development of a Secure Cryptographic Management System (SCMS) to manage the key materials required for a comprehensive solution.

1.6.1 AGA Report No. 12

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

including water and electric utilities. Several individuals from this project were part of the AGA-12 effort prior to the initiation of this project. That prior relationship has continued and has been joined by additional team members of this project. Consequently, the formulation and ultimate direction of this project has been heavily influenced by the project team's prior and ongoing relationship with the AGA-12 effort. This interaction between the two projects also led to the knowledge gained from this project being made available to the AGA-12 effort for its benefit.

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

AGA Report 12, Part 2 is a work-in-progress. Design of AGA-12 compliant cryptographic modules by Thales, which incorporates TecSec technology, and Mykotronx was completed in early 2005 and the Gas Technology Institute (GTI) project team will field-test these modules at Peoples Energy by the middle of 2005. Lessons learned from this project were provided to the AGA-12 project development group to allow members of this group who are also involved in cryptographic module development to improve their designs. When the AGA-12 cryptographic modules are field tested, performance data will be collected and used to update the AGA Report 12, Part 2 specification. The American Gas Association will then submit this specification to a comprehensive review and ballot.

1.6.2 Related Activity

Several projects and much interaction with government, industry, utility, and standards bodies are related to the project documented in this report.

Under contract to the Homeland Security Advanced Research Project Agency (HSARPA), TecSec has developed a high-level design to manage the key materials for cryptographic modules, authentication keys, and for data in any high value data repository. TecSec has been selected for a Phase II award by HSARPA as follow-on to its HSARPA Phase I effort. For Phase II, TecSec's CKM will be integrated into General Electric's EMS XA 21 product to create a Secure Cryptographic Management System (SCMS) prototype for demonstration.

TecSec and General Electric (GE) had independently been in dialog with the utility industry members regarding security. GE was commissioned by the Electric Power Research Institute (EPRI) to do an in-depth study of the information security needs within electric utilities. In the study (several hundred pages long and very detailed), several issues ran consistently throughout. One requirement from the utilities was that a comprehensive solution be provided, one that addressed the utility as a whole, not a series of unrelated solutions that were somehow glued together. GE also looked at their own offerings and realized that they needed to offer a security solution to their existing and new customers. After conducting a market study on their own behalf, GE came to the conclusion that the CKM approach from TecSec, with its modular design and

Software Development Toolkit that can serve the various information security needs within a utility, met the utilities' desire for a comprehensive solution.

Based on dialog with our utility partners and others, this project validated the belief by TecSec and GE that a comprehensive solution that addresses the utility as a whole, not a series of unrelated solutions, is needed. The need for an interim solution was defined by dialog with Industry, which then was further supported by dialog with the American Gas Association's AGA-12 efforts. AGA-12 was circulated and vetted throughout the oil, electric, and water utilities and the net result is that all utilities could participate in and benefit from this project and related projects.

In the Fall of 2004, Mykotronx was awarded a contract from GTI to develop a proof-of-concept link encryptor incorporating AGA 12's Serial SCADA Protection Protocol (SSPP). GTI required the link encryptor to function with the Modbus protocol since it is part of the class of SCADA protocols that is deemed 'most difficult'.

Further talks were held between Dennis Holstein (OPUS Publishing) and CIGRE (International Council of Large Electric Systems) in Paris, Australia, Belgium, The Netherlands, Italy, and Ireland that described the work of this project and related projects. Dennis is one of the US experts to CIGRE Study Committees B3 and B5, and he serves on three directly-related working groups: The Joint Working Group on Security, Convenor of Working Group B5.09 on Remote Online Management for Protection and Automation, and Working Group B5.11 on the Impact of IEC 61850 on Substation Automation. All three working groups address the security requirements developed by this project. The bottom line is that government efforts from DOE-OEA, TSWG, and HSARPA are all contributing different pieces toward providing a comprehensive security solution to the utility sector.

2 Findings

Enabling the CKM software to operate in hardware within the SCADA environment, such that a single security solution can provide comprehensive information protection throughout a utility, was a major goal of the team, resulting in project development and testing of proof-of-concept cryptographic modules using CKM. This project took significant steps toward achieving this goal as evidenced by the following accomplishments.

1. Provided functional requirements for SCADA cyber security for utility operations. Establishing a comprehensive set of functional requirements is important to guiding and judging designs of cyber security systems.
2. Provided a high-level design for cyber security for utility operations. Documenting a design allows it to be evaluated according to functional requirements and implemented by multiple parties.
3. Integrated Sandia's authenticated encryption algorithm, CS-AES[7], into TecSec's CKM software.
4. Developed a proof-of-concept demonstration system of critical components of our cyber security system: 1) maintenance port authentication and 2) authenticated link encryption. This activity included porting elements of CKM (with CS-AES) into a hardware platform and extending the comprehensive solution to SCADA field devices, which is a missing link of comprehensive utility operation security.
5. Evaluated the demonstration system at two utilities, by exercising the proof-of-concept cryptographic modules for SCADA network and maintenance port security. Both gas and electric SCADA test systems were bench tested in our utility partners' test laboratory facilities. Modbus and one proprietary communication protocol were retrofitted with cryptographic modules for these tests. In addition, the DNP3 protocol was tested in a Remote Terminal Unit (RTU) and Intelligent Electronic Device (IED) data acquisition application. Modbus and DNP3 represent almost 80 percent of the installed base for SCADA in these industries.

The outcome of this work validated the proposed technical approach regarding a comprehensive solution to utility cyber security. The approach is comprehensive because it is designed to be a natural extension of the security policies implemented by most utility Information Technology (IT) departments, to meet the needs of EMS and DMS real-time operations, and to protect historical SCADA data used for off-line operations and related business functions. This project provided proof-of-concept components and accelerated the development of a future cyber security solution that addresses these information operations.

2.1 Lessons Learned

In summary, lessons learned from this project have already been applied to other SCADA cyber security related projects with the Department of Homeland Security (DHS).

- The basic cryptographic technology needed for role-based access control in the form of CKM is ready for integration, deployment, and rigorous testing in a wide range of operational and business applications that use SCADA and operational data. CKM

[7] AES stands for Advanced Encryption Standard and CS-AES is the Cipher-State mode of operation of AES.

provides the means to control access to any named data object and how long the permission for use is valid. This project extended elements of CKM into proof-of-concept field devices for SCADA link encryption and maintenance port authentication.

- Using CKM, the management of keying materials needed by utilities' information systems is mature and ready for deployment. The extension of a limited set of these same established techniques into Secure Cryptographic Modules was assisted by this project's proof-of-concept system. Development of a Secure Cryptographic Management System (SCMS) is still needed to gracefully integrate this technology for key management into a utility-focused operational environment and was not in the scope of this project.
- Secure remote access to field device maintenance ports is ready to be implemented within a prototype cryptographic module, which can be subjected to rigorous field-testing. Cryptographic modules used for this purpose will provide protection against cyber attack and will allow the utility to continue to use their dial-up modems for remote maintenance of field devices.
- Bench tests were conducted at Peoples Energy and DTE Energy using operational communication protocols, communication equipment, SCADA masters, and RTUs/relays. Some technical problems needing additional application engineering were encountered during the tests, but they are well understood by the design engineers. Communications problems will be easily fixed, whereas some protocol issues may require more research and discussion to resolve completely. The proof-of-concept program has provided valuable knowledge for application engineers and for standards bodies to make adjustments to accommodate diverse protocols.
- Our utility partners recognized that this project made progress towards the development of technology to secure SCADA communications, but more needs to be done before it becomes commercially feasible (e.g., reduce latency, provide bypass mode to address crypto device failures, etc.).

2.2 Commercialization Plan

Taking cyber security technology from concept to the utility operations market requires skill, resources, and a some good fortune. Our intent was to define a commercialization plan that will decrease the risk and maximize the chances for success.

It is important to remember that the commercial market is dynamic. Shortly after the terrorist attack of September 11, 2001 the market was hot to get a quick solution to protect SCADA and related operational communications from cyber attack. However, the market has become uncertain because there is no mandate by any regulatory agency (federal or state) to require protection of those communication channels. This could change dramatically if a government mandate is forthcoming or if a cyber attack with serious consequences occurs that is well understood in the public domain. Changes might also occur if a business case can be made that convinces utility executives that the costs are recoverable, or financial liability or exposure could seriously degrade the reputation of the utility, or if threat risk assessment imposes changes in operations that add significant cost to operations. A good example of the latter would be the prohibited use of dial-up modems to remotely access the maintenance ports of field devices.

Flexibility, quickness, and information are critical to success. This Commercialization Plan can be used as a roadmap for any manufacturer to develop strategic plans and actions for the commercialization of their advanced technologies that meets the need articulated by utility operation managers responsible for SCADA and field devices.

Reference [R.3] defines commercialization as the final step in new product[8] development when the product developer makes a major marketing commitment to the product. At this stage the product developer implements a total marketing plan and works towards production capacity. Commercialization procedures involve deciding the timeliness of the product introduction, the locations where the product should be introduced, the market to be targeted, and the budget and promotional strategies for the product introduction.

There is a classic model[9] companies use to develop and launch a new product. Figure 2 shows the classic model tailored for this project. This model also illustrates where in the overall timeline we stand after this project was successfully completed - see yellow and blue shaded areas.

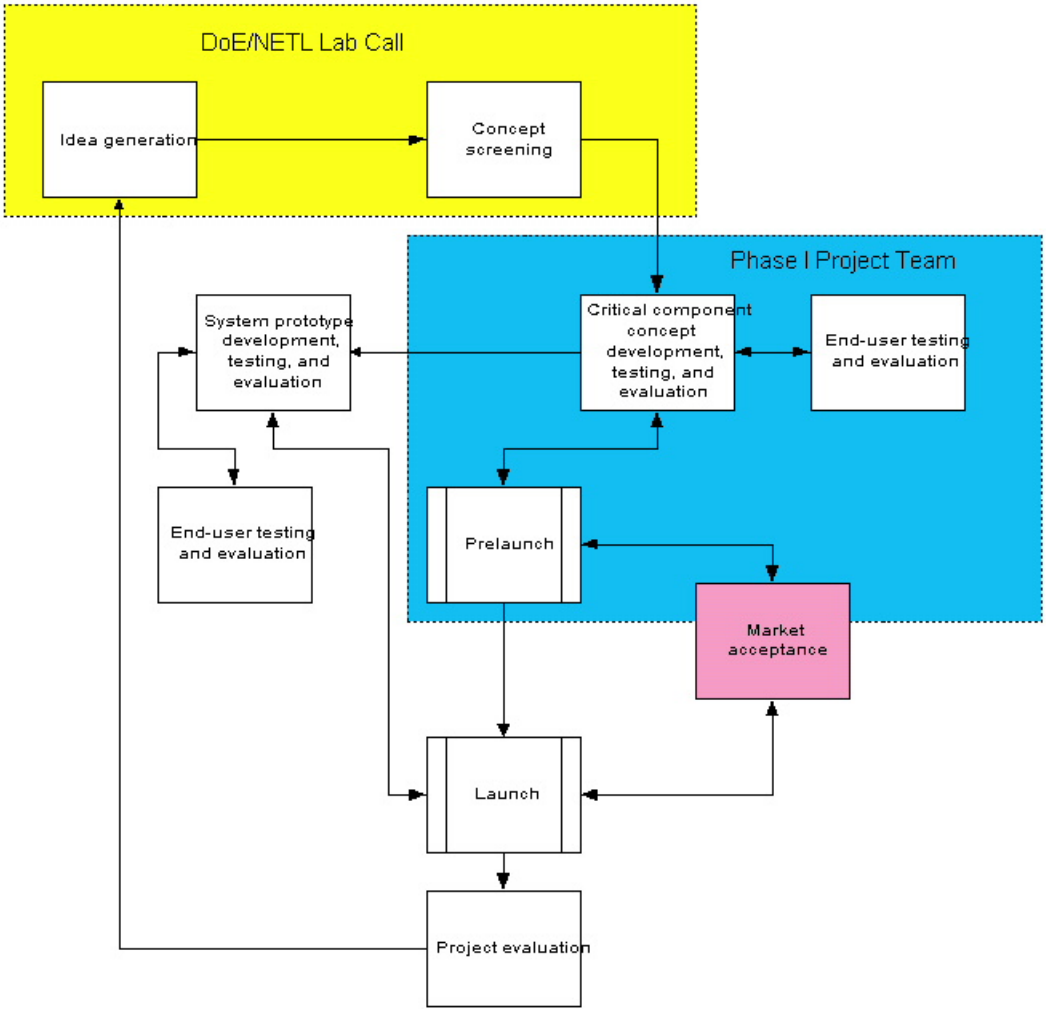

Figure 2. New Product Developments and Launch Model

[8] Product refers to both products and supporting services.

[9] Reference [R.11] provides an expanded discussion of the classic model.

Results from this project have provided valuable insight into the initial entry points to protect SCADA communication links from cyber attack and to strengthen control over access privileges to maintenance ports.

Operating the cryptographic module in the maintenance mode (MCM function) is probably the best opportunity to sell this technology in the utility market. The MCM is a very attractive retrofit solution to the utility because it provides a secure method to remotely access the maintenance ports of any field device using installed dial-up modems. If secured access is not deployed and the utility concludes the risk is unacceptable, the utility is faced with the decision to shut down the dial-up systems and send crews to the field sites when maintenance or data acquisition is required. This is very expensive!

More work is needed to improve the design of the CM to protect the SCADA communication channels from cyber attack (SCM function). After the SCM design and implementation are corrected (see Section 7 for an analysis of the SCM's performance in utility bench tests), the SCM will be a very attractive retrofit solution to get the clear text off the wire on SCADA links. However because there is no government mandate to protect the SCADA links from cyber attack, the utilities will need to make a business case to deploy this solution. Developing a convincing business case is a significant challenge!

As an objective of this project turned towards the integration of CS-AES with CKM and evaluating the effectiveness of CKM as the device-to-device and individual-to-device authentication mechanism, Mykotronx refocused their efforts on the Systems Engineering and Product Marketing aspects of the overall project. Apart from this project, Mykotronx is involved in the following activities as steps towards commercialization of cyber security products for utility operations and use on other projects.

- The key management specifications for AGA-12.
- A VHDL[10] evaluation fixture.
- A System Protection Profile for SCADA Field Communications.
- A theory of operation for AGA Report No. 12, Part 2 [R.6] .
- Proof-of-concept devices for protecting serial and IP-based SCADA, for protecting Protective Relays, and embedded processors and firmware for future field devices.
- Awarded a competitive project from GTI to build an AGA-12 compliant link encryptor.

2.3 High-Level Design Description

From the lessons learned on this project, a high-level design description "An Overarching Solution for Critical Cyber Security Components" was prepared for consideration by future projects – see [R.4] .

[10] VHDL stands for VHSIC Hardware Description Language, where VHSIC stands for Very High Scale Integrated Circuit.

3 Design Requirements

This section describes the design requirements for this project in terms of end-user requirements and technical requirements. End-user requirements are not requirements assigned to end-users (in this case, the utilities), but are those requirements captured by discussions with utility personnel.

3.1 Requirements Obtained via End-User Input

A cyber security system shall be designed to mitigate known vulnerabilities to the following attacks:

- Known-key attack where an adversary obtains some keys used previously and then uses this information to determine new keys.
- Replay attack where an adversary records a communication session and replays the entire session, or portions thereof, at some later point in time.
- An impersonation attack where an adversary assumes the identity of the legitimate entities.
- An attack against passwords. Where typically: a password is stored in a computer file as the image of an unkeyed hash function; when a user logs on and enters the password, it is hashed and the image is compared to the stored value; or when an adversary can take a list of probable passwords, hash all the entries in this list, and then compare this to the list of true encrypted passwords with the hope of finding matches.
- A forward search attack, similar in spirit to the password attack, which is used to decrypt messages.
- Interleaving attack using some form of impersonation in an authenticated protocol.

A cyber security system shall, as a minimum, provide the following:

- Authentication to establish the origin of information and to validate the identity of any entity such as an individual (person), organization, device, or process.
- Authorization which grants to any entity access privileges that convey an ability to perform a business task.
- Confidentiality to ensure that sensitive information is not disclosed to unauthorized individuals, organizations, or processes.
- Integrity to ensure that the content of a SCADA message has not been altered and any alteration of the contents of a message in transit can be detected.

EMS/DMS/SCADA system operation imposes three additional goals.

- The added time (latency) it takes for a protected packet to cross a communication link from sender to receiver shall be minimal in the sense that the degradation is within acceptable limits.
- Cyber security shall operate in a mixed mode to accommodate configurations, which include protection of some nodes, but not all nodes on a given communications channel. Mixed mode allows for incremental, staged installation on multi-drop lines.
- The authentication and authorization mechanism shall interoperate between multiple organizations, allowing the owner of a resource to dictate and manage who may access their resources, what role they are authorized to perform, and how long they may perform this role.

3.2 Technical Requirements

Functional requirements for energy system operations are specified for protection of the SCADA links (including multi-drop lines), protection of maintenance ports, protection of data residing in the SCADA master, and protection, management, and distribution of cryptographic keys.

3.2.1 Protection of the SCADA Links (including multi-drop lines)

1. Provide cryptographic modules suitable for installation on existing communication lines and in substation environments.
2. Use cryptographic keys to provide secure login identification (ID) of the cryptographic modules. Once established, communications between the computer and the SCM shall be encrypted.
3. Use login IDs at each terminal to establish a cryptographic session for communicating SCADA messages.
    - Cryptographic algorithm shall be as transparent as possible to SCADA protocols, but the cryptographic modules installed at the master stations shall be able to determine destination addresses for mixed mode operation.
    - Algorithm shall not impose more than a 20% decrease in SCADA polling frequency.
    - Final selected algorithm shall meet the requirements of AGA Report 12.
4. Provide a means for mixed mode operation from the master station (with some RTUs equipped with SCMs on their communication ports and some with no SCM) on multi-drop lines.
5. The SCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if its power supply is lost.
6. Retrofit of SCADA links shall require no software changes in either the master station or in the RTUs.

3.2.2 Protection of Maintenance Ports

1. Remote access shall be usable over dial-up connections from a computer (notebook or desktop) to an IED's maintenance port.
2. Access shall use two factor authentication; e.g., cryptographic authentication key (or Smart Card) in a Universal Serial Bus (USB) port and Personal Identification Number (PIN) to establish secure ID before allowing remote access from the computer to the maintenance port via an MCM.
3. Once communication is established between the computer and the MCM, messages shall be encrypted.
4. Once access is permitted, MCM shall allow use of existing passwords in the IED and require minimal changes in the computer's existing remote access software.
5. MCM shall terminate the access if the USB authentication key (or Smart Card) is removed.
6. MCM shall terminate the access if no activity is detected for a configurable period of time.
7. The MCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if the power supply is lost.

3.2.3 Protection of Data Residing in the EMS/SCADA Master

1. External access to the SCADA database (access other than by the SCADA operator) shall be allowed only to authenticated users with access rights.

2. Authentication shall be two factor; e.g., cryptographic authentication key in a USB port (or SmartCard) and PIN.
3. Access rights shall include read only, write only, and read/write and shall include an expiration date/time.

3.2.4 Protection, Management, and Distribution of Cryptographic Keys

One common key management system shall be used for instantiating the keys for requirements described in Sections 3.2.1, 3.2.2, and 3.2.3.

The key management system shall comply with the recommendations in AGA-12 Addendum 1. AGA-12 Addendum 1 recommendations are implemented in the design described in [R.7] and [R.8] .

4 Units under Test

All units under test used for this project are proof-of-concept units. The units had not reached the stage of a prototype. Robust testing and analysis was not part of these tests.

4.1 As-built Cryptographic Module Description

Figure 3 shows the proof-of-concept cryptographic module hosted on a Texas Instrument (TI) Innovator™ development kit. A full description of the TI Innovator is available on the TI web site - www.ti.com, keyword "innovator."

Figure 3. Proof-of-Concept Cryptographic Module

4.1.1 Cryptographic Module Hardware Description

The OMAP5910 is a highly integrated hardware and software platform, designed to meet the application processing needs of next-generation embedded devices. The OMAP platform enables OEMs to quickly bring to market devices featuring rich user interfaces, high processing performance, and long battery life through the maximum flexibility of a fully integrated mixed processor solution. The dual-core architecture provides benefits of both DSP and RISC technologies, incorporating a TMS320C55x DSP core and a high-performance TI925T ARM core.

The DSP core of the OMAP5910 device is based on the TMS320C55x DSP generation CPU processor core. The C55x DSP architecture achieves high performance and low power through increased parallelism and total focus on reduction in power dissipation. The CPU supports an internal bus structure composed of one program bus, three data read buses, two data write buses, and additional buses dedicated to peripheral and DMA activity. These buses provide the ability to perform up to three data reads and two data writes in a single cycle. In parallel, the DMA controller can perform up to two data transfers per cycle independent of the CPU activity.

The C55x CPU provides two multiply-accumulate (MAC) units, each capable of 17-bit x 17-bit multiplication in a single cycle. A central 40-bit arithmetic/logic unit (ALU) is supported by an additional 16-bit ALU. Use of the ALUs is under instruction set control, providing the ability to optimize parallel activity and power consumption. These resources are managed in the address unit (AU) and data unit (DU) of the C55x CPU.

The C55x DSP generation supports a variable byte width instruction set for improved code density. The instruction unit (IU) performs 32-bit program fetches from internal or external memory and queues instructions for the program unit (PU). The program unit decodes the instructions, directs tasks to AU and DU resources, and manages the fully protected pipeline. Predictive branching capability avoids pipeline flushes on execution of conditional instructions. The OMAP5910 DSP core also includes a 24K-byte instruction cache to minimize external memory accesses, improving data throughput and conserving system power.

The OMAP5910 multimedia processor contains three universal asynchronous receiver/transmitter (UART) peripherals. UART1 and UART2 are UART modems with autobaud capability. UART3 is a modem with IrDA. Either the MPU (default) or the DSP controls the three UARTs via three TIPB switches (one for each UART). Figure 4 shows UART view of the OMAP 5910 device with the UART peripherals highlighted.

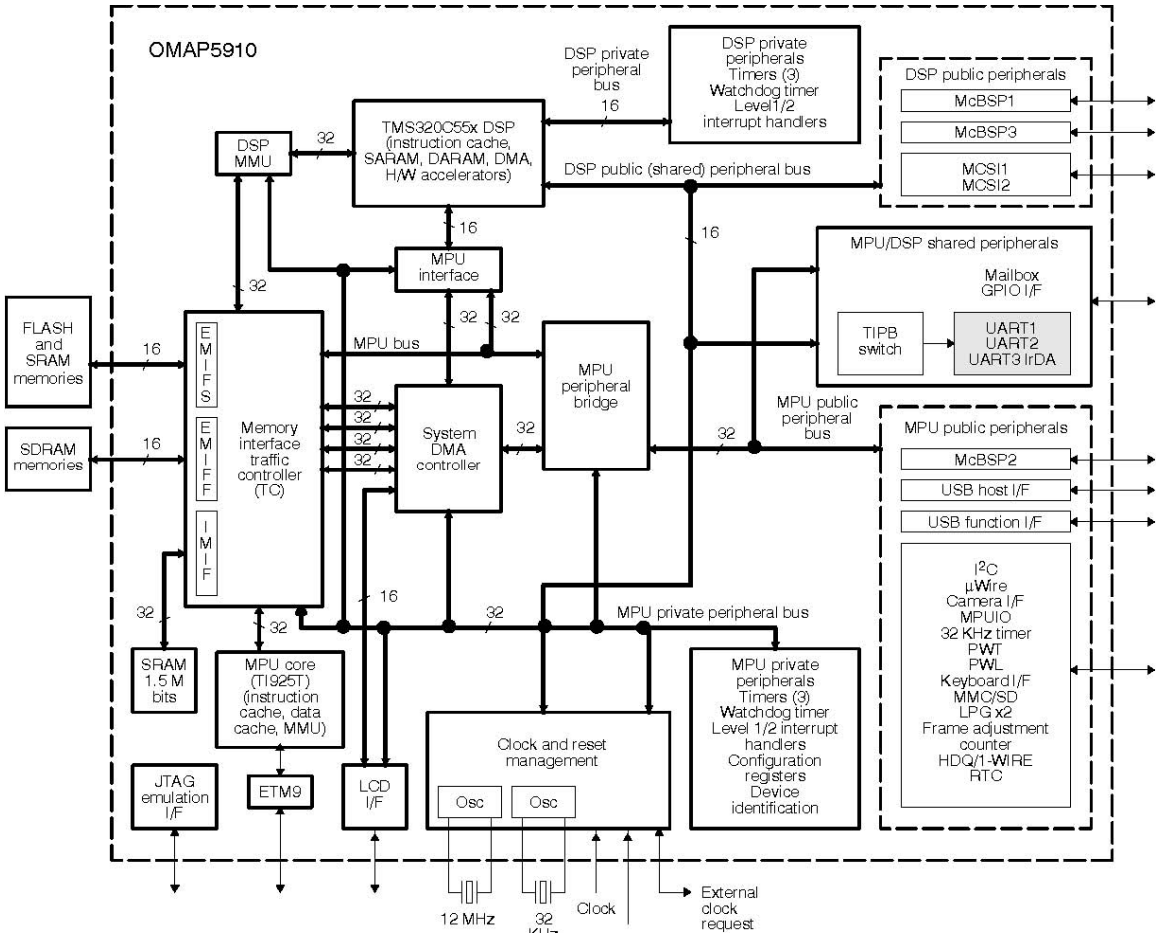

Figure 4. UART View of the TI Innovator OMAP 5910

4.1.1.1 Main UART Features

The main features are as follows:

- Selectable UART/autobaud modes (UART1 and 2 only).
- Dual 64-entry FIFOs for received and transmitted data payloads.
- Programmable and selectable transmit and receive FIFO trigger levels for DMA and interrupt generation.
- Programmable sleep mode.
- Complete status-reporting capabilities in both normal and sleep mode.
- Frequency prescaler values from 0 to 65535 to generate the appropriate baud rates.
- An interrupt request to the system if there are multiple DMA requests.

4.1.1.2 UAR/Modem Functions (UART 1/2)

- Baud rates from 300 bits/s to 1.5M bits/s.
- Autobaud between 1200 bits/s and 115.2K bits/s.
- Software/hardware flow.
- Programmable serial interface characteristics.

- False start bit detection.
- Line break generation and detection.
- Fully prioritized interrupt system controls.
- Internal test and loopback capabilities.
- Modem control functions (CTS, RTS, DSR, and DTR).

4.1.1.3 Why the TI Innovator OMAP 5910 Was Selected

TecSec selected the TI Innovator OMAP 5910 because of a commercial migration strategy to the ARM 9 core processor. TecSec chose to write the cryptographic functions onto the ARM Processor identified as the TI925T, Main Processing Unit (MPU), shown in Figure 4 for migration to other platforms. Since many hardware platforms are available in the market and the specifics of the hardware change often, the primary software elements were developed to be portable to other platforms.

4.1.1.4 Functional Limitations of the TI Innovator

Several limitations of the TI Innovator caused problems in successfully demonstrating the proof-of-concept cryptographic modules.

- The TI Innovator does not support carrier detect.
- The TI Innovator tends to overheat, causing hardware failures.
- Even with a DSP core, the TI Innovator does not have the performance needed for IP based protocols because it does not have hardware support for the cryptographic engines at this time.
- As the TI Innovator is not a cryptographic device; therefore it provides no protection of its internal data.

4.1.2 Cryptographic Module Software Functional Description

The SCM and MCM contain firmware that initializes the hardware module. This initialization involves both configuring and adjusting the hardware for SCM use, as well as the testing of the firmware integrity and Federal Information Processing Standard (FIPS) testing of the cryptographic routines. The firmware is split into three distinct components:

- Boot module
- Flash writing module
- Operating system

The Boot Module performs the hardware initialization, firmware integrity checks, secure loading of firmware, and basic cryptography routines. This module also contains and installs the flash writing routines. Effectively the boot module is the kernel (or core) of the whole firmware. All communication to/from the user is performed on the local serial port on the Proof-of-Concept SCMs and MCMs.

The flash writing routine is packaged separately so that both the boot module and operating system may be reloaded. This routine is relocated into RAM, because as the flash memory is being reprogrammed, you cannot access the current values (you cannot run code from the flash as you program the flash).

The operating system is a two-level state machine that controls the current state of the SCM/MCM and limits the operations that can be performed in each state. This component effectively makes the TI chipset into an SCM or MCM.

All timing and communications between the states and the local and remote communications ports are controlled in this component. All protocol recognition and support is also located at this level.

The SCM and MCM modules were designed to use the same firmware to help reduce cost and development effort. A set of options control the operation of the operating system component and basically configure the device as an SCM or MCM.

4.2 Cryptographic Module Configuration Set-up

Figure 5 shows an engineer configuring the cryptographic module for each demonstration. The module could be configured to operate in either the SCM or MCM mode.

For the purpose of this demonstration, TecSec used a set of testing Credentials and a test Domain to demonstrate the proof of concept (see References [R.13] and [R.14] for a full description of terms used in Constructive Key Management). Downloads from the notebook computer were used to update the firmware at each test site. Since problems were expected during the bench tests, fixes to the firmware could be made and retested on site. The keys used for encryption were created dynamically from the TecSec Domain and Credentials – each time the link was created, a totally new key was created. This test fully demonstrated the use of CS-AES authenticated encryption with session keys.

The firmware for the SCM and the MCM presents ASCII menus to the user and accepts ASCII commands. These commands and menus are used to step the user through the configuration of the device. This setup procedure was adequate for a proof-of-concept demonstration; it is probably not the procedure that will be used for production units.

For the production units a client side utility to configure the SCM and MCM is preferred by the end user because the RTUs and IEDs are configured in a similar manner.

Figure 5. Cryptographic Module Setup

4.3 As-built Maintenance Notebook Computer for MCM

The as-built maintenance notebook computer used to demonstrate the functions of the MCM are described in terms of the notebook computer software, the USB authentication key, the interaction between the USB authentication key and the notebook computer software, the interaction between the USB key and the communication session, and the interaction between the MCM, notebook computer software, and authentication key.

4.3.1 Notebook Computer Software Description

The software on the notebook computer contains a version of the MCM operating system running on a customized boot module that is written for the notebook operating system. This software also utilized a software package from Constellation Data Systems Inc (www.virtualperipherals.com) which creates virtual serial ports.

The MCM notebook software uses a virtual serial port for the local port and the actual physical serial port and/or modem for the remote port. Once the software is installed, the only changes that are required to the normal software used to communicate to the maintenance ports is that the control software (not the MCM software) be configured to use the virtual serial port instead of the real serial port.

The notebook MCM software uses the TecSec CKM Desktop Software Development Kit (SDK) to provide access to a hardware device that contains a maintenance person's authorization set.

4.3.2 USB Authentication Key Description

The USB authentication key is a “holder” for the TecSec soft token implemented on an Aladdin eToken.

4.3.3 Interaction between USB Authentication Key and Notebook Computer Software

When the eToken is removed from the notebook computer the related keys stored in the notebook are erased. These keys are required for notebook computer software to correctly interact with the MCM software – see 4.3.5.

4.3.4 Interaction between USB Authentication Key and Communication Session

There is no direct interaction between the USB authentication key and the communication software in either the notebook computer or the MCM.

4.3.5 Interaction between MCM, Notebook Computer Software, and Authentication Key

Without the hardware device, the notebook MCM software cannot create (nor can it maintain) a connection to the MCM that is protecting the maintenance port. Upon detection of the removal of the hardware device, any open connection through the notebook MCM software is closed and the computed CKM session key is securely destroyed.

5 Test Configurations for Proof-of-Concept Demonstration

Test configurations of the environments and units under test are described for each test site provided by the participating utilities.

5.1 Peoples Energy Configurations

The test configurations used for the project proof-of-concept demonstration at People Energy included Modbus point-to-point, multi-drop, and radio communications.

5.1.1 Modbus Point-to-Point SCM Configurations

Figure 6 shows the Modbus point-to-point SCM configuration installed at Peoples Energy for this demonstration. Each SCM has a DTE (Data Terminal Equipment) male 9 pin connector and a DCE (DATA Communication Equipment) female 9 pin connector. The DCE is connected to the terminal server and to RTU 20. The DTE is connected to the modem, which forms the communication link between the communication hub and the field site. Channel speeds can vary from 9600 bps to 19.2 Kbps.

Modbus/RTU functions 03 and 16 (10 hex) were used for the demonstration. The maximum message packet length was 4 Kbytes. A protocol analyzer was used to check that transmissions were encrypted.

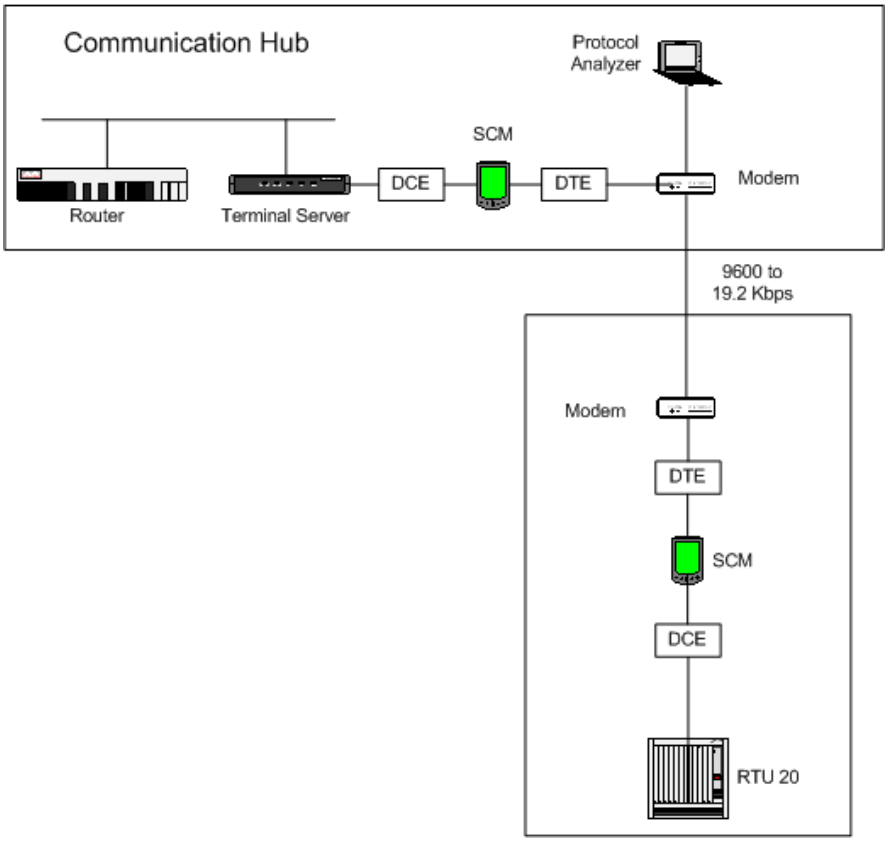

Figure 6. Point-to-Point SCM Configuration

Figure 7 shows the two RTUs, labelled TL85 and TL86, used for demonstration at Peoples Energy. The SCM was connected to these RTUs in either a point-to-point configuration as shown in Figure 6, or in a multidrop configuration using a port share as shown in Figure 9 and Figure 11, or in a multidrop mixed mode configuration as shown in Figure 10.

Figure 8 shows the DCE used for the tests.

Figure 7. RTUs Used For Demonstration at Peoples Energy

Figure 8. DCE Used For Demonstration at Peoples Energy

Figure 9 shows the same basic configuration as Figure 6 except a port share device is included to support two RTUs. For this configuration the field SCM protects both RTUs. The channel speed between SCMs was set at 9600 bps for this configuration; and the channel speed between the SCM and port share device (to the RTUs) was varied from 9600 bps to 19.2 Kbps.

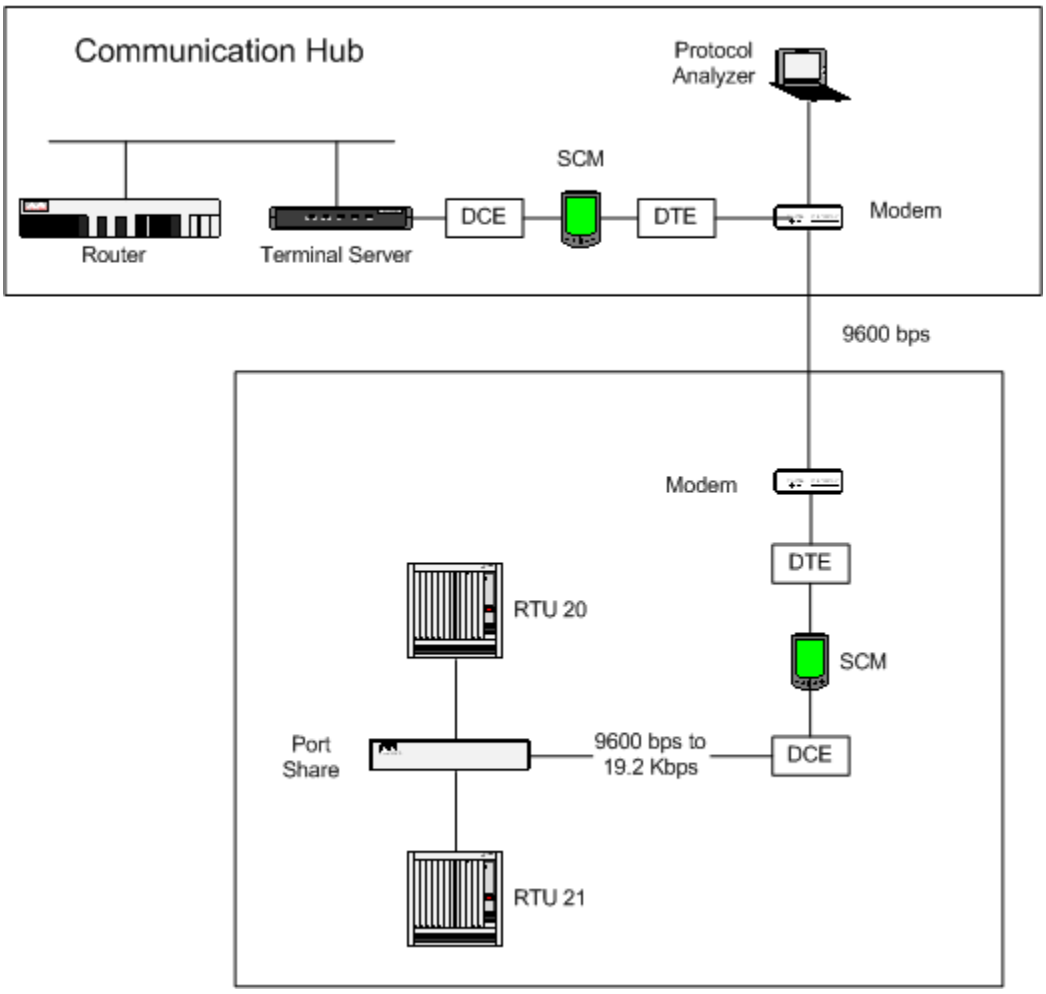

Figure 9. Point-to-Point with Point Share SCM Configuration

5.1.2 Modbus Multi-Drop SCM Configurations

Figure 10 shows the multi-drop, mixed mode SCM configuration implemented with a port share device. The channel speed for this configuration was 9600 bps.

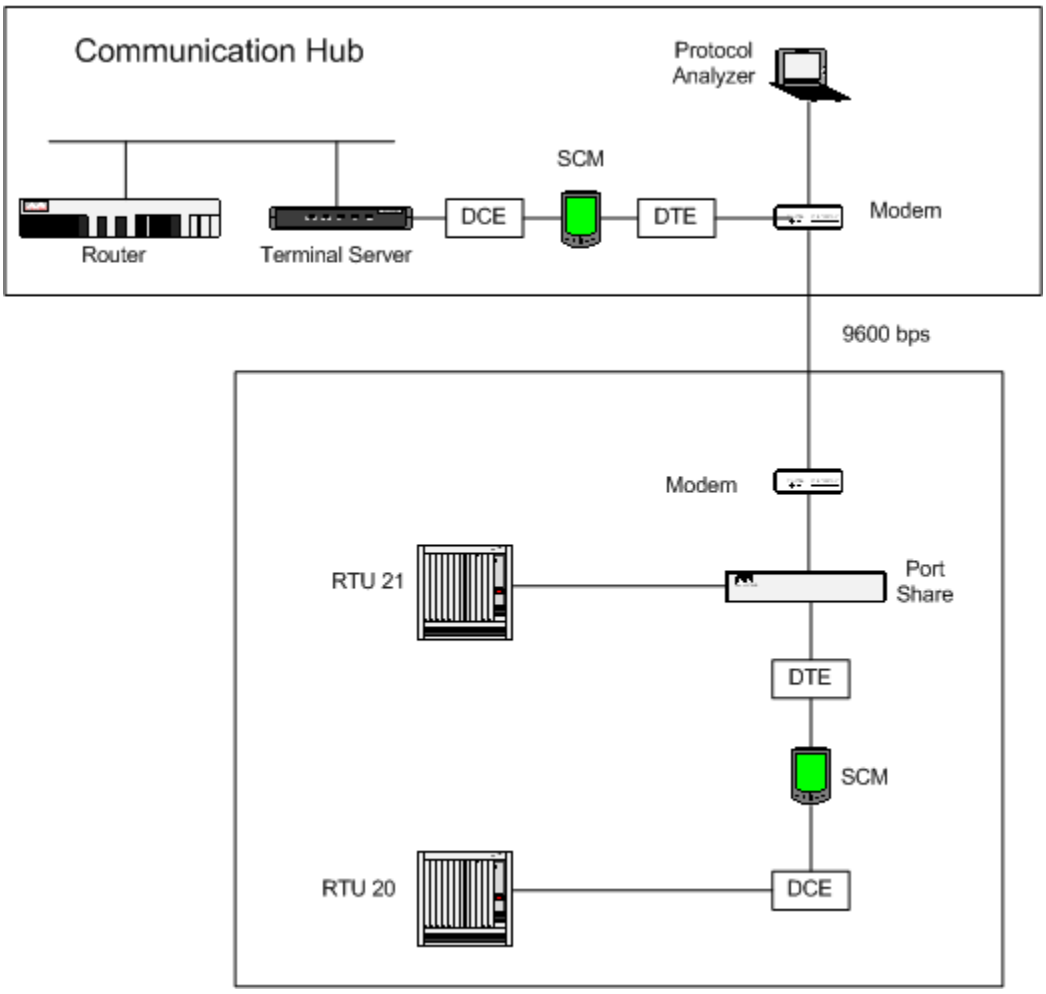

Figure 10. Multi-drop Mixed Mode with Port Share SCM Configuration

Figure 11 shows the multi-drop with a port share device and one SCM to protect RTU 20 and one SCM to protect RTU 21. The channel speed from the port share to SCMs was 9600 bps and the channel speed to the RTUs was 19.2 Kbps. The SCM was designed to handle different baud rates between the input side and the output side to reduce the latency introduced by the SCM's need to buffer encrypted data into the SCM and decrypted data out of the SCM.

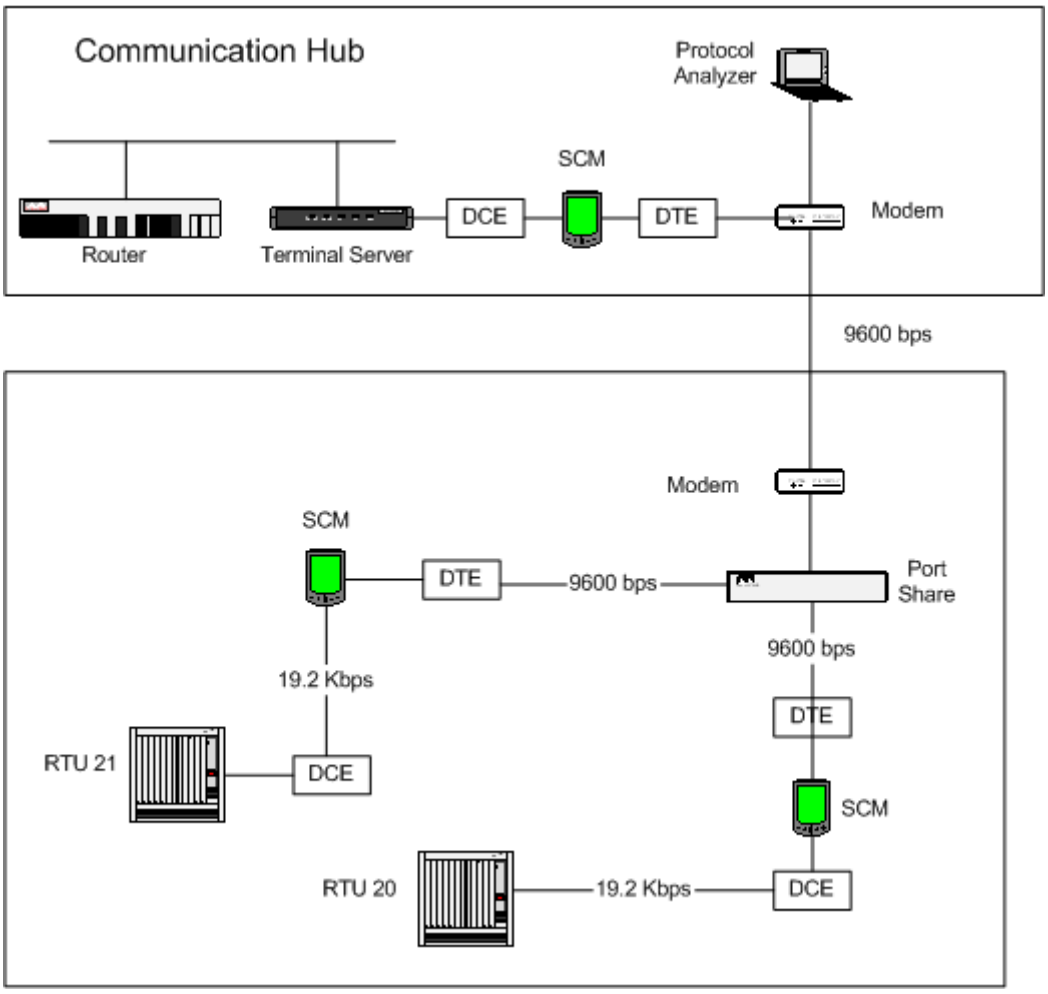

Figure 11. Multi-drop with Port Share SCM Configuration

5.1.3 Modbus Radio Communication Configuration

Figure 12 shows the point-to-point radio SCM configuration. This configuration is the same as Figure 6, except radios operating at 1200 bps are used instead of modems.

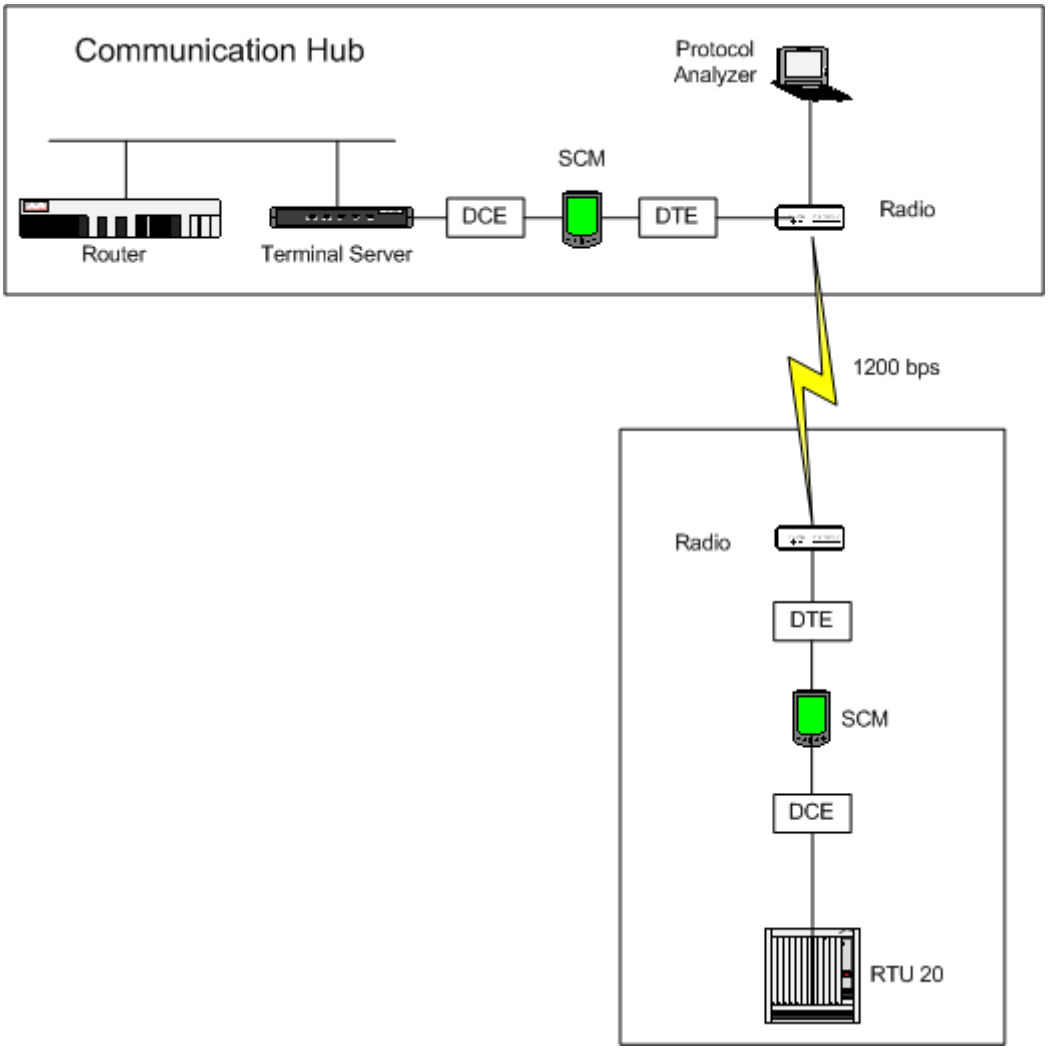

Figure 12. Point-to-Point Radio SCM Configuration

Figure 13 shows the radio and antenna used for the demonstration at Peoples Energy.

Figure 13. Radio and Antenna Used For Demonstration at Peoples Energy

5.2 DTE Energy Test Configurations

The DTE Energy test configurations used for this demonstration included dial-up MCM, DNP3, and a legacy communication protocol.

5.2.1 Dial-Up MCM Configurations

Figure 14 shows the remote dial-up MCM configuration used to demonstrate improved authentication and confidentiality of access to the maintenance port of a field device. An engineer or technician inserts an authentication key into the USB port of the notebook computer and enters a Personal Identification Number (PIN). This procedure implements two factor authentication – something you have and something you know. TecSec loaded the needed components of the CKM software on the notebook computer before the demonstration was started.

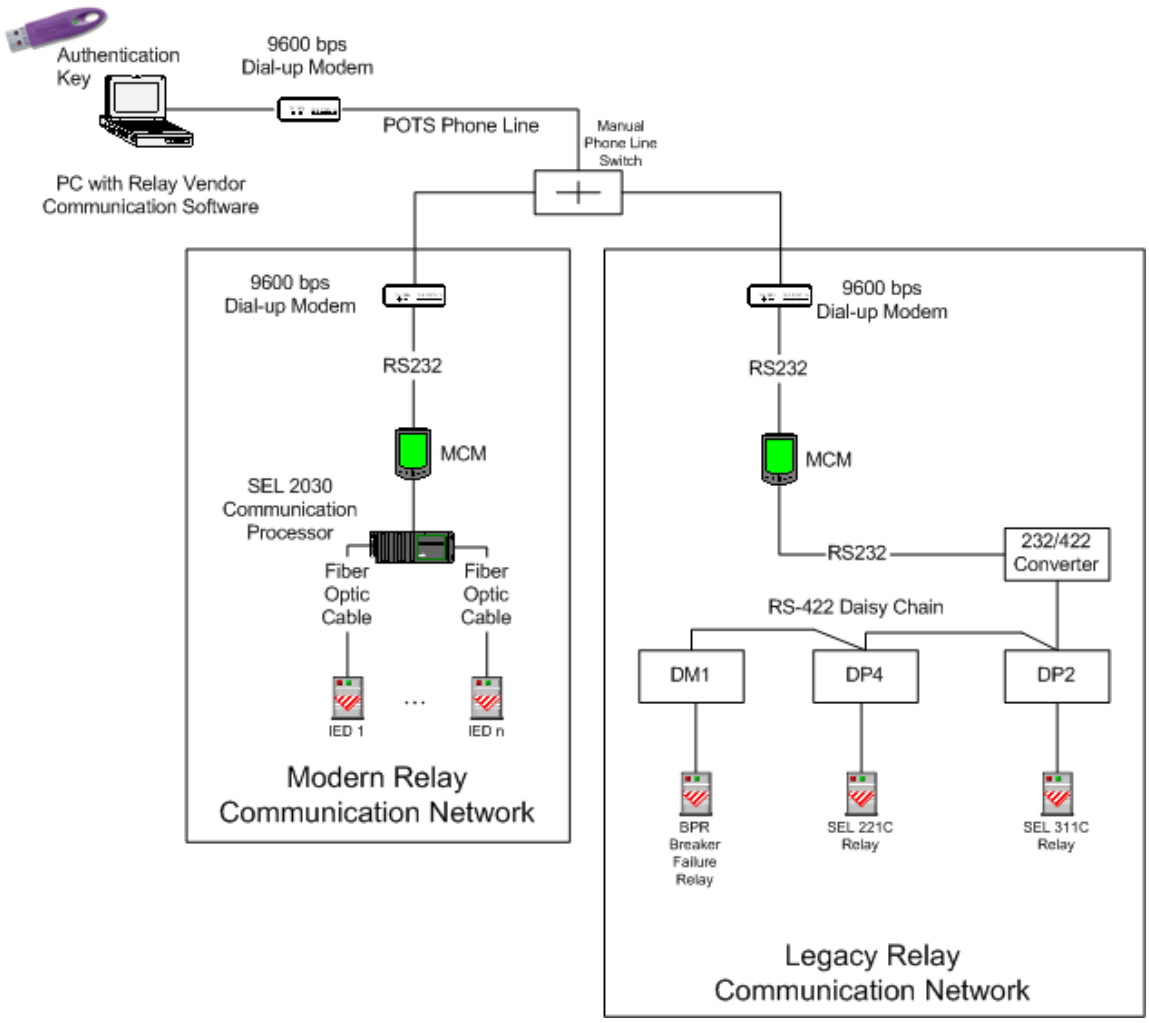

Figure 14. Maintenance Port Demonstration Configurations

The engineer then dials up the answering modem to gain access to the maintenance port of the protected field device (an IED or relay shown in Figure 14). The MCM intercepts the request from the software on the notebook computer and generates a challenge to that software. If the MCM receives a positive response from the notebook computer software, it allows a message to be decrypted and sent to the maintenance port on the field device. Thereafter, the interaction between the engineer and the relay is

carried out in the same manner as when there is not an MCM in the communication path.

The 9600 bps dial-up modem shown in Figure 14 was pre-connected because the TI Innovator does not support the carrier detect signal. Also, TecSec only implemented an RS232 serial interface on the TI Innovator and when a non-RS232 interface was required, a converter was installed as shown in Figure 14.

A manual phone line switch was used to select each configuration network to be demonstrated. Two communication networks were successfully demonstrated.

5.2.1.1 Modern Relay Communication Network

A modern relay communication network connected the MCM to an SEL 2030 communication processor, which in turn was connected by fiber optic cable to several IEDs. In this configuration the MCM protected access to the SEL 2030, not access to the individual IEDs.

5.2.1.2 Legacy Relay Communication Network

A legacy communication network connected the MCM through an RS 232/422 converter, which was connected through a daisy chain configuration to several relays.

5.2.1.3 Recommended Change to MCM Functional Requirements

Although not originally stated as an MCM functional requirement, TecSec implemented encryption of the message between the notebook computer and the MCM. This should be a requirement for the following reasons.

- The MCM functional requirement specifies the need to enforce proof of authorization.
- With dial-up communications, it is fairly easy for an organized attacker to connect to the lines at either end and maintain the connection after the legitimate technician (or engineer) has completed the task and attempts to hang up.
- The protection of the data that is sent over the dial-up line gives the ability for both ends to only accept data from a proven source. Except for an insider who already has the rights, the attacker would not have the ability to create the encryption key and therefore would not be able to maintain the integrity of the transmitted data.
- Without encryption, the only fallback for ending the session is to disconnect the line. Any organized attacker that was trying to gather information would be able to monitor the communications and keep the communication channel open long after the authorized party was finished.

The MCM functional requirements in 3.2.2 have been updated to include this encryption requirement.

5.2.2 DNP3 SCADA Communication Test Configurations

Figure 15 shows the DNP3 SCADA communication configurations provided by DTE Energy for this project. Communications between the emulated operations center and the laboratory was over a 1200 bps communication channel using a legacy protocol.

The entry point in the laboratory was an ACS 7560 RTU. The DNP3 SCADA protocol was used over a 19.2 Kbps communication channel to demonstrate the SCM mixed mode operating functions. To accommodate the SCM, RS232 I/O interface converters

were installed to interface to RS485 devices. Real SATEC meters that use DNP3 were the installed IED field devices.

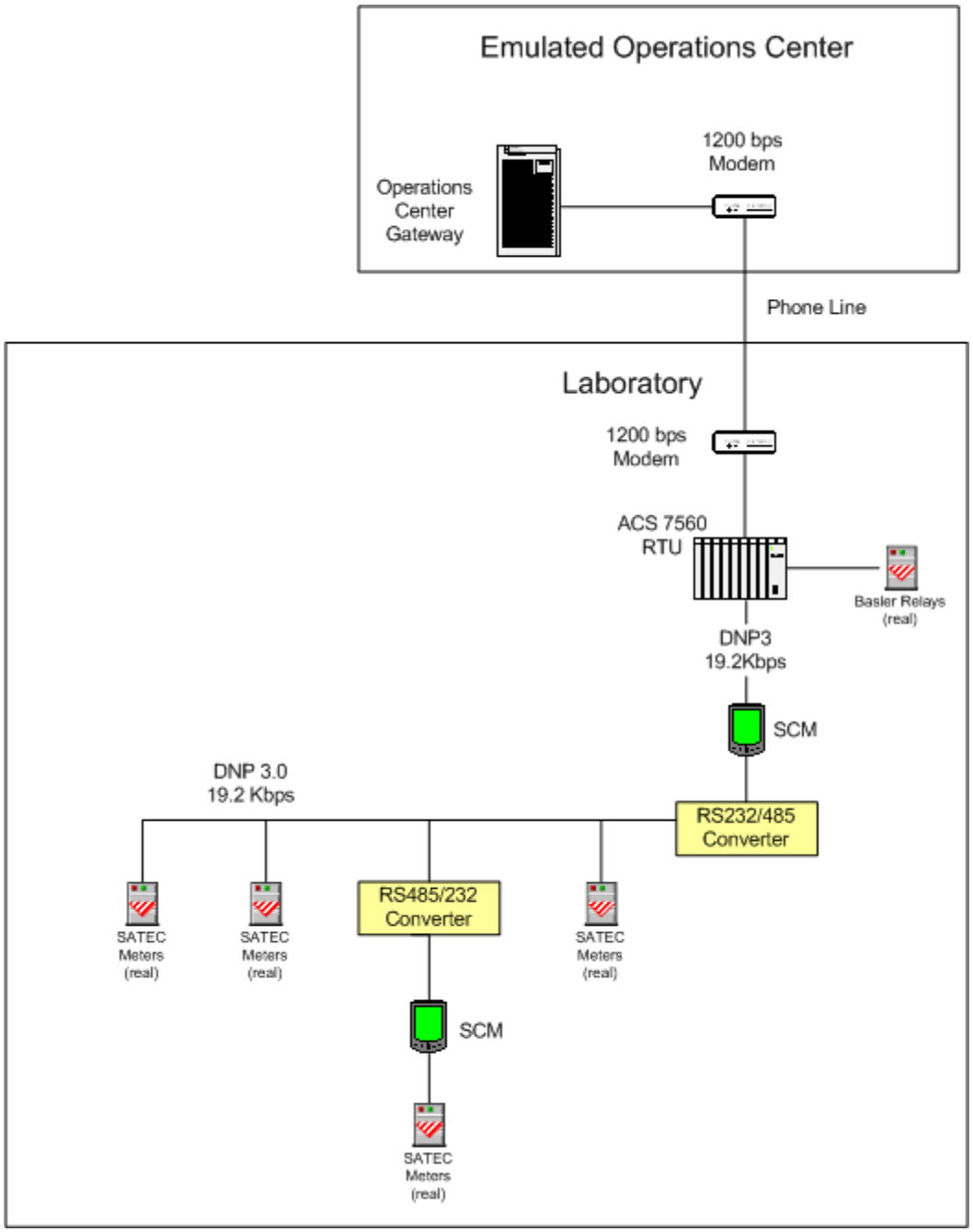

Figure 15. DNP3 SCADA Communication Configurations

Figure 16 shows the SCMs used to protect DNP3 communication to the SATEC meters.

Figure 16. SCMs and Meters Used for DNP Demonstration at DTE Energy

5.2.3 Electric SCADA Communication Protocol Configuration

Figure 17 shows the SCADA communication configuration used to demonstrate SCM operation in a mixed mode environment. DTE Energy provided an emulated operations center in their laboratory with an SCM between the operations center gateway and a 1200 bps modem.

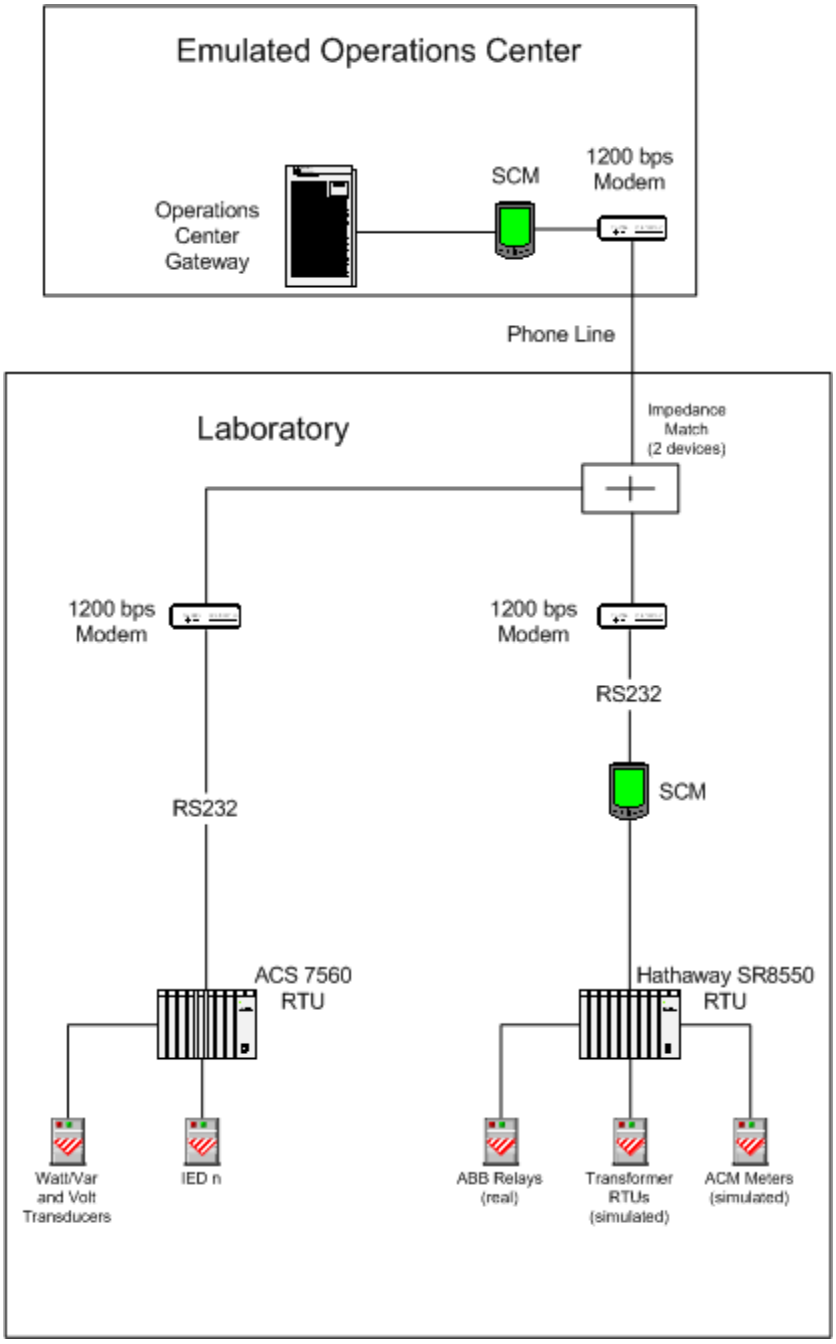

Figure 17. Legacy SCADA Communication Configuration

6 Design Requirements Audit of Technical Requirements

Within cost and schedule constraints, design requirements specified in Section 3 were implemented to the level of detail needed to demonstrate the functionality of the critical components of our cyber security solution. Table 1 describes the degree of implementation designed into the proof-of-concept units under test.

Table 1. Design Requirements Audit

Final report cross reference	Technical requirement	Degree of implementation	Comment
3.2.1	Provide cryptographic modules suitable for installation on existing communication lines and in substation environments.	Specifically addressed the retrofit requirements without requiring changes in either master station or RTU software.	
	Use cryptographic keys to provide secure login identification (ID) of the cryptographic modules.	Implemented the CKM key generation system.	Point-to-point demonstration showed this worked correctly.
	Use login IDs at each terminal to establish a cryptographic session for communicating SCADA messages.	Implemented in the CKM specification of Role-based Access Control (RBAC).	Point-to-point demonstration showed this worked correctly.
	Provide a means for mixed mode operation from the master station (with some RTUs equipped with SCMs on their communication ports and some with no SCM) on multi-drop lines.	Designed to support mixed mode.	Demonstration did not successfully show that this works satisfactorily – See Section 7.2.3.
	The SCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if its power supply is lost.	Not implemented	This is beyond the capability of the TI Innovator, but could be implemented in a final product.

Final report cross reference	Technical requirement	Degree of implementation	Comment
	Retrofit of SCADA links shall require no software changes in either the master station or in the RTUs.	Specifically addressed the retrofit requirements without requiring changes in either master station or RTU software.	Point-to-point demonstration showed this worked correctly. Note: the baud rate between the SCM and the RTU was increased to 19.2 Kbps (see Figure 11 and related text in Section 5.1.2).
3.2.2	Remote access shall be usable over dial-up connections from a computer (notebook or desktop) to an IED's maintenance port.	Implemented with a preset modem baud rate.	Point-to-point demonstration showed this worked correctly.
	Access shall use two factor authentication; e.g., cryptographic authentication key (or Smart Card) in a Universal Serial Bus (USB) port and Personal Identification Number (PIN) to establish secure ID before allowing remote access from the computer to the maintenance port via an MCM.	Implemented with a token on a USB authentication key.	Point-to-point demonstration showed this worked correctly.
	Once access is permitted, MCM shall allow use of existing passwords in the IED and require minimal changes in the computer's existing remote access software.	Implemented.	Point-to-point demonstration showed this worked correctly.
	MCM shall terminate the access if the USB authentication key (or Smart Card) is removed.	Implemented by using the CKM encryption mode. If the token was not available from the authentication key, the notebook computer did not have the needed key material to perform encryption.	Point-to-point demonstration showed this worked correctly.

Final report cross reference	Technical requirement	Degree of implementation	Comment
	MCM shall terminate the access if no activity is detected for a configurable period of time.	Implemented	Timeout worked for several cases. It did not work in all cases due to one or more implementation flaws that were only marginally related to the timeout issue. See Section 7.4.4.
	The MCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if the power supply is lost.	Not implemented.	This is beyond the capability of the TI Innovator, but could be implemented in a final product.
3.2.3	External access to the SCADA database (access other than by the SCADA operator) shall be allowed only to authenticated users with access rights.	Not implemented.	This is beyond the capability of the TI Innovator, but could be implemented in a final product.
	Authentication shall be two factor; e.g., cryptographic authentication key in a USB port (or SmartCard) and PIN.	Not implemented for SCADA operations.	
	Access rights shall include read only, write only, and read/write and shall include an expiration date/time.	Not implemented.	
3.2.4	Protection, Management, and Distribution of Cryptographic Keys	Not implemented.	

7 Analysis of Demonstration Results

Our analysis of the demonstration results is first divided into two groups: cryptographic functions and communication functions. This is followed by analysis of the SCM operating mode and the MCM operating mode. Figure 18 shows the network analyzer used and notebook computer used to measure performance for the demonstration performed at Peoples Energy.

Figure 18. Network Analyzer and Notebook Computer Used To Measure Performance

7.1 Cryptographic Functions

The protocol analyzer shown in the configuration diagrams in Section 5.1 was used to monitor the traffic between SCMs. Review of these data showed the cryptographic functions to be operating as designed.

7.2 Communication Functions

Cryptographic functions were analyzed using point-to-point communication statistics that were collected during the field tests. The primary objective of these tests was to determine if the functions of the cryptographic modules operated correctly. Performance numbers were collected to determine if the functions were corrupted by noise on the line or other events. Performance measures related to latency introduced by the cryptographic modules was deferred to AGA-12 testing.

Implementation issues related to Modbus throughput, detection of headers, mixed-mode communication, and radio communication were also analyzed. The following discussion is provided as an introduction to the technical issues discussed in this section.

- Throughput has to do with the rate at which data can be effectively communicated.
- Detection of headers is an issue when dealing with various protocols that specify headers differently and some that don't specify a header at all. A header is defined as a set of leading characters of a message that describe the format, content, or some characteristic of the remainder of the message. Typical elements of a header might include the destination address for the message, the source address of the message, and the length and/or format of the data within the message.
- Mixed-mode operation, as described by the AGA 12 Task Group, is a situation where, due to costs, deployment schedules, maintenance or some other factor, a subset of the SCADA devices on a shared communication channel may be protected (via encryption) by SCMs and the remaining SCADA devices are not protected. The result of mixed-mode operation is that both plaintext (unencrypted) and ciphertext (encrypted) SCADA messages use a shared channel. The AGA 12 Task Group's primary concern with mixed-mode operations is that it is statistically possible that a ciphertext message may have the same set of leading characters (i.e. the header) as a plaintext message. Therefore, a legacy SCADA device may interpret and process a ciphertext message as a valid plaintext message, leading to unpredictable results within the SCADA device. The opposite situation can occur as well (i.e., a plaintext message can be interpreted as a valid ciphertext message).
- Encryption offers the ability to scramble data, which results in ciphertext. This provides confidentiality or privacy of the data. Authorized users can decrypt or unscramble the data, which results in the original plaintext. Most encryption algorithms employ a block cipher, which encrypts data in blocks of, say, 16 bytes. If communication of data of less than 16 bytes is desired, then some kind of padding is performed, resulting in 16 bytes of plaintext to encrypt. This requires the recipient of encrypted data to collect the entire block of ciphertext before decryption can take place. Larger data messages can require multiple blocks of plaintext and ciphertext.
- Data authentication offers the ability of a recipient of communication to validate the integrity of the communicated data message. Data authentication does not change the contents of the message, but computes an authentication tag that must be communicated with the message. The recipient of the message can compute an authentication tag based on the received message and compare it to the tag received with the message to test whether any part of the message has been modified.

The challenging question is, "How does one develop a single SCM to address all of these issues?" The experiments conducted at our utility partners' facilities provided valuable insight into these challenges.

7.2.1 Point-To-Point Communication Statistics Collected

A point-to-point 9600 baud Modbus configuration without cryptographic modules was used to collect statistics over a 16 hour period at Peoples Energy. Polls per hour varied from 4206 to 4218 without experiencing a dropped poll, resulting in a reliability ratio of 100%.

Using the same configuration with cryptographic modules, an unacceptable level of dropped polls was introduced. Table 2 shows the raw data collected. All failures recorded were due to no reply; no failures were caused by a checksum failure, a long message, or any other observable cause.

Table 2. Point-To-Point Configuration Summary with Cryptographic Modules

Time	Success	Failure	Reliability Ratio	No reply
2100	2739	55	98.03	55
2200	2618	88	96.75	88
2300	2776	43	98.47	43
0000	2668	72	97.37	72
0100	2849	26	99.10	26
0200	2625	84	96.90	84
0300	2667	74	97.30	74
0400	2642	79	97.10	79
0500	2745	51	98.18	51
0600	2713	59	97.87	59
0700	2406	55	97.77	55

Analysis by TecSec determined that the principle cause of the dropped polls was the timing mechanism implemented in the Innovator 5910. Other causes included the performance limitations of the Innovator 5910 with respect to cryptographic computations and communications and the overhead (memory and processor) of the operating system running on this hardware. All of these causes provide valuable information for designing and building future cryptographic devices for SCADA security. The following subsections provide an in-depth discussion of the issues and tradeoffs associated with operating cryptographic equipment in actual SCADA communications environments.

7.2.2 Modbus Throughput Issue

Modbus throughput was directly affected by the SCM link encryption implementation, which held an entire message, regardless of size, until it was encrypted or decrypted before forwarding it to the target device. This ‘Holdback’ can introduce an excessive amount of latency into the SCADA system at both SCMs.

In an attempt to reduce latency, the AGA 12 Serial SCADA Protection Protocol (SSPP) was designed to function with different suites or modes of operation. One mode of operation, ‘No-Holdback’, is based upon the block length of the underlying encryption algorithm (AGA 12 supports only one symmetric encryption algorithm – AES, which has

a block size of 16 bytes). When an SCM receives a message, the SSPP protocol buffers the proper number of bytes before performing a cryptographic (i.e., encryption or decryption) operation. After the cryptographic operation, No-Holdback allows the SCM to immediately forward the block of data to the target device. There are two concerns with No-Holdback: 1) the SCM is passing part of a message to the target device before it knows the entire message is valid (i.e., authentic), and 2) there will be jitter (i.e. delays or timing gaps) between the blocks of data. Both of these conditions could be detrimental to the native SCADA system – not validating or authenticating the message before forwarding it could allow an attacker to embed malicious code within an apparently longer valid message; and jitter can disrupt Modbus communications due to the fact that Modbus messages are delineated by timing gaps on the communication channel. Jitter could be interpreted by a SCADA device as a break between messages, resulting in the fragmented message being considered line noise.

In an attempt to improve security and eliminate jitter, the AGA 12 Task Group designed a second mode of operation called 'Full-Holdback'. Full-Holdback allows the sending SCM to forward blocks of data to the receiving SCM as they are ready (exactly the same as No-Holdback). However, at the receiving SCM, the SSPP protocol waits until the entire message has been received, decrypted, and validated before forwarding it to the target SCADA device. Full-Holdback by its very nature adds latency to the SCADA system, but it eliminates the concerns that malicious code may reach the SCADA device and that a SCADA message may contain too much jitter resulting in the SCADA device treating it as line noise.

In the AGA 12 Task Group's attempt to research the trade-offs between quickly delivering data and latency introduced by improving security, two other operating mode options were studied and quickly discarded, the use of a streaming cipher and the possibility of a Partial or n-byte Holdback.

The AGA 12 Task Group's recommendation is to use SSPP in Full-Holdback mode if you are using a SCADA protocol such as Modbus that delineates messages with timing. Alternatively, SSPP in No-Holdback mode may be used if you are using a SCADA protocol such as DNP3, which delineates messages based upon a 'length' field within the message's header.

7.2.3 Modbus Header Issues in a Multi-drop Mixed-Mode Topology

During one phase of our testing, we configured a SCADA communications channel with a SCADA Master and two RTUs. The SCADA Master and one RTU were protected by an SCM and one RTU was left unprotected. The AGA 12 Task Group refers to this configuration as a Multi-drop Mixed-Mode topology (i.e. Multi-drop – more than one RTU is on the channel; Mixed-Mode – both protected and unprotected traffic occurs on the same channel). During normal operation, the SCM serving the SCADA Master will interrogate the SCADA message from the Master to determine the message's destination address. If the message is addressed to the un-protected RTU, the Master's SCM would simply allow the message to pass through as-is. If, on the other hand, the message is addressed for the protected RTU, the Master's SCM would forward a header and the encrypted message to the remote SCM.

During this phase of testing, we experienced sporadic problems where the remote, Slave SCM would stop processing messages. It was later determined that the problem was due to collisions (matching header fields) between Modbus message headers and our

protected message headers. In this scenario, the SCADA master is the originator of all messages which will be received by all field devices on that channel. The master is configured to send messages meant for unprotected field devices in plaintext and messages meant for protected field devices as ciphertext. The messages are of varying length and content. The master is performing a poll of the RTUs in the remote locations. As soon as the response is received from one poll, the next poll was sent. The first symptom observed was that the unprotected RTU would work all the time, but after some period of time (sometimes a really short period of time), the protected RTU failed to receive messages. After significant diagnosing of the problem, it was observed that the plaintext data would periodically have a byte pattern that matched the encrypted block header. This forced the Slave SCM to start processing the data as encrypted. In the process, the sequence numbers and other information became corrupted as far as the Slave SCM saw them. The root problem was that the data was really plaintext, not an encrypted header.

TecSec suggested that the detection of the message header in the SCM should look for a period of silence (configurable) before a header byte would be recognized. This should not add any latency, since most devices will receive a significant amount of data before they begin transmitting results.

The AGA-12, Part 2 team leader, John Kinast from GTI, provided insight into the detection of headers issue. In mixed-mode, the fact that SCADA messages sometimes (randomly) appeared to be headers for encrypted messages confused the SCM, requiring a reset of the session to continue to operate. This caused a number of message packets to fail. TecSec suggested two ways of overcoming these problems.

- The first way is to have a more complex header that is much harder to hit with random data. This however can significantly impact the latency of the system.
- The second way is to look for a short period of inactivity before recognizing a header. This significantly reduces the chances of having the plaintext message fragment be interpreted as a ciphertext header. In many cases, this time interval may already exist and therefore no additional latency would be introduced. The underlying industry protocols that are supported will have to be examined to determine if the inactivity checking could work and what the appropriate value would be.

The AGA 12 Task Group, in researching how to place protected traffic on the same channel as unprotected traffic, identified a specific problem with some SCADA protocols. This problem manifests itself when the first byte of the SCADA header is data instead of a flag character. Modbus is one of these protocols in which the first byte of its header is the message's destination address. In very large Modbus systems, it is possible that nearly every conceivable single-byte value may be a valid device address. To compensate for this situation, SSPP implements a flagging and escaping scheme. This scheme defines a set of configurable two-byte flags to delineate the start of a message, the start of the payload, and the start of the trailer. In addition, SSPP's "escaping" scheme removes any ambiguity in the event that two adjacent bytes in its ciphertext payload should match one of the configurable two-byte flags.

7.2.4 Radio Communications

Any MCM or SCM that is used with radios, or other devices that require settling times, will require that the cryptographic module have configurable delay settings that force it to wait a set time after the serial handshake lines transition to a valid state before any data is sent.

7.3 SCM Operating Mode

For each configuration, the following sequence was used to demonstrate correct operation of the SCM operating mode.

1. A normal polling sequence was executed without SCMs. Command and response data was collected and retained for comparison.
2. An SCM was installed at the master station end of the communication channel only.
3. The attempt to open an SCM session failed because an SCM was not installed at the field device end of the communication channel. The SCM was removed from the master station end of the communication channel.
4. An SCM was installed at the field device end of the communication channel only.
5. The attempt to open an SCM session failed because an SCM was not installed at the master station end of the communication channel. The SCM was removed from the field device end of the communication channel.
6. SCMs were installed at both ends of the communication channel.
7. An SCM session was opened and the same polling sequence used for Step 1 above was executed. Command and response data was collected and retained for comparison.
8. Command and response data collected was compared and no differences were identified. The cryptographic function performed as designed.

7.4 MCM Operating Mode

The following scenarios were successfully demonstrated.

7.4.1 Nominal Operational Sequence

1. Engineer inserts the USB authentication key into the notebook computer.
2. CKM software requests a 4 digit PIN to be entered.
3. When the correct PIN is entered the token stored on the USB authentication key is used by the CKM software on the notebook computer to encrypt the message traffic over the dial-up communication to the MCM.
4. MCM issues a challenge to the CKM software on the notebook computer to verify authentication.
5. After authentication is verified, the engineer interacts with the protected IED and verifies that the correct information is exchanged.
6. Engineer closes the dial-up connection.
7. Engineer redials for access to the IED maintenance port and, again, the sequence beginning with the entry of the 4 digit PIN is repeated to show that the communication session must be reinitialized and that no residual is left from the previous dial-up.

7.4.2 Incorrect PIN Demonstration

This demonstration showed that a user has N chances to enter the correct PIN. When N was exceeded, the session was terminated by the CKM software on the notebook computer and a new PIN was then required because the old PIN was no longer valid.

TecSec preset N to 10 for this demonstration. Distribution of a new PIN was not demonstrated.

7.4.3 Authentication Key Demonstration

After Step 5 of Section 7.4.1, the authentication key was removed from the notebook computer USB port before Step 6. Without the authentication key, the CKM software on the notebook computer did not have the token to encrypt the message and in effect the communication session was terminated because the MCM could no longer decrypt a message from the notebook computer.

The authentication key was reinserted into the USB port on the notebook computer and the CKM software in the notebook computer required starting the sequence with Step 1 in Section 7.4.1. The sequence could not continue from Step 5.

7.4.4 Timeout Issue

In Table 1, it was noted that timeout was shown to work in several cases, but not all. The timeout value is one of the parameters that should be configurable by the end user.

The complicating factor in the timeout was that the Innovator does not support modem detection of carrier detect. Implementation of a full prototype cryptographic module needs to ensure that modem detection of carrier detect is supported.

TecSec tried to use additional timers for the demonstration, but those timers introduced other problems. Given the difficulty of using the additional timers and the time available to perform the demonstration, the test team made the decision to proceed with other tests and revisit this issue at another time.

7.5 Peoples Energy Assessment

The communication difficulties experienced during the Peoples Energy tests are not unusual – they reflect a normal operating environment. In fact, the “bench” tests attempted were performed in an ideal situation with a minimal amount of noise.

With regard to Section 3.2.3, Protection of Data Residing in the EMS/SCADA Master, it is our opinion that protection of data at rest can be obtained by “hardening” the SCADA system and/or using off-the-shelf products. We feel that protecting data at rest is important; however it should be up to the end user how the system should be secured. After discussing this option with our SCADA vendor, implementing this system would void any warranty that exists and also likely break the system and cause undesirable behavior. Simply put, retrofitting a system with the recommended protection will not only be intrusive to SCADA systems, but will also be very expensive to implement.

With regard to Section 4.2, Cryptographic Module Configuration Set-up, we believe that it is important to note that because of the nature of SCADA communications, often noisy, often non-persistent, the need to create a totally new key each time the link is created should be reviewed. In the laboratory environment, this proved to be the cause of a large number of dropped messages and a large decrease in the performance in comparison to our benchmark.[11]

In conclusion, we would like to thank the project team for giving us an opportunity to provide input as a utility towards the development of security tools for SCADA systems.

---

[11] After further investigation, TecSec determined that the problem was not a re-keying issue. Rather, it was related to misidentifying packets in the header, which forced re-keying and re-synchronization (see the Section 7.2.3 discussion).

7.6 DTE Energy Assessment

We see a great need for technology that will enable us to encrypt our SCADA communications. The Cyber Security for Utility Operations Project made progress in this area. However, more needs to be done before it becomes commercially feasible (e.g., reduce latency, provide bypass mode to address crypto device failures, etc).

8 Summary and Conclusions

This section includes:

- A summary that addresses what the project accomplished, what is left to do, and the meaning of the outcome of the project.
- A conclusion that addresses how this project will advance the protection of SCADA communications, the near term ongoing activities by the team members, and the next recommended action for DOE.

8.1 Summary

Our objective was to implement two critical technologies, CS-AES and CKM, into a proof-of-concept cryptographic module designed to encrypt SCADA communications and to provide access integrity to the maintenance ports of field devices over dial-up communication channels. CS-AES was integrated into CKM, and a limited set of CKM functionality was implemented in the cryptographic modules.

- Proof-of-concept cryptographic modules were used to demonstrate that cryptographic functions would correctly operate in a utility operational environment. Because we focused our attention on the retrofit solution for asynchronous serial communications, the cryptographic modules needed to work with two of the most common communication protocols, Modbus and DNP3.
- Lessons learned from the project (see Section 2.1) were reviewed with the AGA-12 development team and provided valuable guidance for team members who are also developers of prototype cryptographic modules. Recent tests of these new prototypes at Peoples Energy showed that most of the communication problems experienced with our proof-of-concept module (the TI Innovator) were corrected and performance was well within the allocated target of 20% reduction in polling frequency.

Two high priority tasks need attention.

- A key management system needs to be developed and demonstrated to fulfill the requirement of protecting data at rest and to manage the keying material for all components of the target architecture (see Section 1.4). HSARPA has selected TecSec for award to demonstrate this capability.
- A full system prototype of the target architecture (using commercially available implementations of the cryptographic solution set described for the target architecture) needs to be developed in a comprehensive SCADA testbed facility, then tested in selected utility environments. Sandia and Idaho National Laboratories have the comprehensive SCADA testbed facilities and the partner utilities participating in this project have offered to continue the work in their facilities.

Our utility partners reflected on the meaning of this project by stating, in effect, “We see a great need for technology that will enable us to encrypt our SCADA communications. The Cyber Security for Utility Operations Project made progress in this area.” Clearly, this project was a good first step.

8.2 Conclusions and Recommendations

This project, coupled with the work on AGA Report No. 12, is recognized by many in the community who are familiar with these works to be the best and most comprehensive approach to protect SCADA communications and access to the maintenance ports of field devices.

- Informal review of our results by manufacturers, system integrators, and utility engineers is underway as part of our recommended commercialization plan (see Section 2.2). Early feedback indicates that several companies are now building retrofit link encryptors for SCADA operations that meet the design requirements offered by this project.
- System integrators and SCADA manufacturers are beginning to work with these companies to add them to their SCADA systems as value-added components.

The SNL team members continue to work on AGA Report No. 12 and the development of prototypes to ensure that the cryptographic protocol is well defined and compliant hardware devices are tested in both laboratory and utility environments.

A role for DOE-OEA in a follow-on effort would be in funding the development and comprehensive testing of a full prototype of the target architecture shown in Figure 1.

9 Definitions and Acronyms

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

9.1 Definition of Terms

Approved security function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either specified in an approved standard, or adopted in an approved standard and specified either in an annex of the approved standard or in a document referenced by the approved standard, or specified in the list of approved security functions.
Authentication	A process that establishes the origin of information, or validates an entity’s identity.
Authorization	Access privileges granted to an entity; conveys an “official” sanction to perform a security function or activity.
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
Credentials	The means to associate access and use permission with a cryptographic value.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.
Cryptographic key component (key component)	One of two or more secret numbers that are combined to produce a key using split knowledge procedures.
Cryptographic Module (CM)	The set of hardware, software, and/or firmware contained within a cryptographic boundary that implements approved security functions (including cryptographic algorithms and key generation).
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
Cyber attack	Exploitation of the software vulnerabilities of information technology-based control components.
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
Domain	A grouping of roles, categories, credentials and policies with common security needs. See [R.14] for a full explanation of how domains are used.
Encryption	The process of changing plaintext into ciphertext using a cryptographic algorithm and key.
Firmware	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Hash function	A function that maps a bit string of arbitrary length to a fixed length bit string. With cryptographic hash functions, it is computationally infeasible to find any input that map to a pre-specified output, and It is computationally infeasible to find any two distinct inputs that map to the same output.
Intelligent Electronic Device (IED)	Any device incorporating one or more processors capable of receiving or sending data/control from/to an external source (e.g., electronic multifunction meters, digital relays, controllers).
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Maintenance port	The physical access mechanism (interface) on an IED or RTU through which a maintenance engineer can access data, and access or change settings and programs with the IED or RTU. The port is typically RS-232 (a standard for asynchronous serial data communications). The access may be controlled by several levels of passwords, For remote access via dial-up phone lines; an external or internal automatic answering modem is required.
Mixed mode	Pertaining to a communication arrangement where some devices on a shared communication channel are protected by cryptographic modules and some are not.
Multidrop	Pertaining to a communication arrangement where several devices share a communication channel. See [R.12]
Non-repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.
Operator (SCADA)	An individual in the utility control center that is responsible for on-line SCADA system control.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Plaintext	Unencrypted data with format additions or changes, such as framing or padding.
Port	A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).
Slave	A device that gathers data or performs control operations in response to requests from a master and sends response messages in return. It may also generate unsolicited responses.
Substation or station	The term, including its qualifier, is used to generically address all remote sites housing devices that control transmission and distribution of gas, electricity, water, wastewater, etc. Examples are electric power substations, pumping stations, compressor stations, and gate stations.
Supervisory control data acquisition system (SCADA and automatic control)	A system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station). The supervisory system may be combined with a data acquisition system, by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions.

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

9.2 Definition of Acronyms

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

HSARPA	Homeland Security Advanced Research Project Agency
ID	Identification
IED	Intelligent Electronic Device
IT	Information Technology
IU	Instruction Unit
Kbps	Kilo bits per second
MCM	Maintenance Cryptographic Module
MPU	Main Processing Unit
PIN	Personal Identification Number
PU	Processing Unit
NETL	National Energy Technology Laboratory
NIST	National Institute of Science and Technology
RBAC	Role-based Access Control
RTS	Ready To Send
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCM	SCADA Cryptographic Module
SCMS	Secure Cryptographic Management System
SDK	Software Development Kit
SNL	Sandia National Laboratories
SSDL	SCADA Security Development Laboratory
SSPP	Serial SCADA Protection Protocol
TI	Texas Instrument
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
WAN	Wide Area Network

10 References

[R.1] Cyber Security for Utility Operations – Functional Requirements, October 19, 2004

[R.2] Demonstration plan for critical cyber security components, May 4, 2004.

[R.3] Commercialization plan for critical cyber security components, August 25, 2004

[R.4] An Overarching Solution for Critical Cyber Security Components - Design Specification, NETL Project M63SNL34, October 14, 2004.

[R.5] AGA Report No. 12: Cryptographic Protection of SCADA Communications, Part 1, Background, Policies, and Test Plan.

[R.6] AGA Report No. 12: Cryptographic Protection of SCADA Communications, Part 2, The Retrofit Solution.

[R.7] HSARPA Sponsored CKM-based Management System for SCADA/DCS Operations, HSARPA Project NBCHC040081.

[R.8] Secure Cryptographic Management System (SCMS) Design Document.

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

[R.10] Dictionary of Marketing Terms, 3rd Edition, 2000, Barron's Business Guide

[R.11] Corchels, Linda, The Product Manager's Handbook, 2nd Edition, 2000, NTC Business Books.

[R.12] IEEE 100 Authoritative Dictionary of IEEE Standard Terms, Seventh Edition.

[R.13] CKM Glossary of Terms, dated April 4, 2004.

[R.14] System Planning Guide for Constructive Key Management, dated June 22, 2004.