



AGA Report No. 12

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

March 14, 2006

Disclaimers and copyright

The American Gas Association's (AGA) Operating Section provides a forum for industry experts to bring collective knowledge together to improve the state of the art in the areas of operating, engineering and technological aspects of producing, gathering, transporting, storing, distributing, measuring and utilizing natural gas.

Through its publications, of which this is one, the AGA provides for the exchange of information within the gas industry and scientific, trade and governmental organizations. Each publication is prepared or sponsored by an AGA Operating Section technical committee. While AGA may administer the process, neither the AGA nor the technical committee independently tests, evaluates, or verifies the accuracy of any information or the soundness of any judgments contained therein.

The AGA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on AGA publications. The AGA makes no guaranty or warranty as to the accuracy and completeness of any information published therein. The information contained therein is provided on an "as is" basis and the AGA makes no representations or warranties including any express or implied warranty of merchantability or fitness for a particular purpose,

In issuing and making this document available, the AGA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the AGA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

The AGA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does the AGA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance is solely the responsibility of the certifier or maker of the statement.

The AGA does not take any position with respect to the validity of any patent rights asserted in connection with any items which are mentioned in or are the subject of AGA publications, and the AGA disclaims liability for the infringement of any patent resulting from the use of or reliance on its publications. Users of these publications are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Users of this publication should consult applicable federal, state, and local laws and regulations. The AGA does not, through its publications intend to urge action that is not in compliance with applicable laws, and its publications may not be construed as doing so.

*Any changes in this document that are believed to be appropriate should be communicated to AGA by completing the last page of this report titled **"Form for Suggestion to Change AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan"** and sending it to: **Operations & Engineering Services Group, American Gas Association, 400 North Capitol Street, NW, 4th Floor, Washington, DC 20001, U.S.A.***

© American Gas Association 2006 All rights reserved.

PREFACE

Following the September 11, 2001 terrorist attack on U.S. soil, the AGA Gas Control Committee (GCC) and the Automation & Telecommunication (A&T) Committee agreed to support development of an AGA report that would demonstrate how encryption may be applied to protect gas Supervisory Control And Data Acquisition (SCADA) communication systems from cyber attack. The A&T Committee adopted the SCADA Communication Encryption Suite, which was proposed by the Gas Technology Institute (GTI) in 1999, as a basis for developing a gas SCADA communication protection system.

Over the past few years, AGA has and continues to serve two functions in the development of this SCADA communication protection system: 1) support the gas industry's effort to obtain Federal funding for the project and 2) provide in-kind services through AGA staff and committee volunteers to make information on applications, systems, operations, etc. available and to offer critical review of the draft report.

AGA and GTI have worked closely with the relevant government agencies; manufacturers, suppliers, vendors of SCADA system; and the gas industry SCADA experts across the nation to develop this SCADA protection system. This group, titled the AGA 12 Task Group, has been open to all individuals with knowledge of or interest in SCADA encryption. The active members of the group included SCADA manufacturers (Telvent, Bristol Babcock and Emerson/Fisher, and General Electric), cryptographic module and router manufacturers (CISCO Systems, Mykotronx, Thales, and Weston Technology), research groups (EPRI, GTI, and many consultants), and government groups (NIST and Sandia National Laboratories). The group also included four utilities (KeySpan Energy, Peoples Energy, PSE&G, and Wisconsin Electric-Wisconsin Gas). While few utility members participated in the detailed discussions regarding highly technical level decisions, their input was crucial to determining the operational environment of SCADA systems and the consequent constraints on SCADA encryption.

The AGA 12 Task Group was mandated to offer initially a short-term retrofit solution for existing systems and later a long-term solution applicable to new systems and Internet-based SCADA communications. In accord with the numbering format for AGA's other reports, the group was directed to number the reports as AGA 12-1, 12-2, 12-3, etc. Also in keeping with AGA's other reports, the implementation of this report and any subsequent AGA 12 series of reports would be voluntary and at the sole discretion of the individual companies based on their own risk assessment.

Shortly after the AGA 12 Task Group began its work on developing a report to protect gas SCADA systems, the group expanded its scope to include water and electric SCADA systems. The reasons for this scope expansion were as follows:

- The marginal effort of including water and electric was believed to be small because SCADA systems are technically and operationally similar
- Coordination on the front-end would reduce the odds of conflicting SCADA security systems
- Avoidance of duplication of similar efforts
- SCADA system operators would benefit from economies of scale if the non-recurring engineering and certification costs were spread over more units

- Combined utilities (gas & electric) would only need to incur training, maintenance, and inventory costs for one SCADA encryption technology rather than two
- Inclusion of more industries would attract more manufacturers and volunteers to work on the project because of broader applicability and larger potential markets, and
- Issues introduced in response to electric industry concerns were found to be beneficial to the gas and water industry, particularly, protection of maintenance ports and a heightened need for minimizing latency.

Following the expansion of the project scope from gas SCADA communications encryption to a multi-industry (electric and water) practice, an invitation was extended to the water and electric utilities to participate on the AGA 12 Task Group. The Awwa Research Foundation provided financial support. NERC monitored the report's progress.

In the process of developing the report, the AGA 12 Task Group decided that a comprehensive SCADA encryption methodology required a two-pronged approach starting with the development of a solid foundation of corporate policy for addressing cyber security; followed by the reinforcement of specific procedures necessary for retrofitting cryptographic modules to existing SCADA systems. The group recognized that a comprehensive program required installation of hardware and software that is supported by operating procedures and appropriate corporate policies. Experience shows that if a cryptographic system is compromised, it is more often due to poor policies and operating procedures than to an assault on the cryptographic system itself.

To effectuate this methodology and keeping in sequence with AGA's other reports, the AGA 12 Task Group decided to split the AGA 12 report and number them as follows:

- AGA 12, Part 1: Cryptographic Protection of SCADA Communications: Background, Policies & Test Plan
- AGA 12, Part 2: Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications
- AGA 12, Part 3: Cryptographic Protection of SCADA Communications: Protection of Networked Systems
- AGA 12, Part 4: Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components

How to Read AGA 12, Part 1

AGA 12, Part 1 is intended to serve as a guideline for voluntary implementation of a comprehensive cyber security posture. It focuses on providing background information for improved assessment of a company's cyber security posture, suggesting policies for a comprehensive cyber security plan and offering a sample test plan for operator implementation.

The premise for AGA 12, Part 1 is rooted in the operator's performance of risk assessment analysis on his/her cyber system. A consistent risk assessment analysis equips the operator with the information necessary to understand consequences and formulate an objective business case. Following the performance of a cyber risk assessment analysis, the operator may elect to deploy the encryption methodology that follows in the AGA 12 series of technical reports (i.e., Part 2 and so on). The reader

should note that AGA 12, Part 1 is independent of the rest of the AGA 12 series. Compliance with AGA 12, Part 1 does not require compliance with the rest of the AGA 12 series.

In reading AGA 12, Part 1, it is essential the reader understands the specific and restricted definitions of the terms “may,” “must,” “recommended,” “shall,” and “should” as defined in section 1.4.1. Furthermore, chapters, sections and appendices in this report are labeled as either “Informative” or “Normative.” Material labeled as “Informative” is provided for reader education and background. If SCADA operators wish to claim compliance with AGA 12, they either must comply with the recommendations labeled as “Normative” or specifically document that a particular recommendation is not being followed with a statement of the reason not to follow this recommendation.

Executive summary

Since the terrorist attacks of September 11, 2001, the United States' outlook on security has changed. Always a core element of American life, security is no longer taken for granted. Today, the safety of our country and the resources we rely upon should be worked at daily. Our nation's security is only as strong as its weakest link. Once thought of as operating over secure networks, SCADA systems and DCS are in fact vulnerable. As providers of life-critical products and services, the natural gas, electricity, water, wastewater and pipeline industries need to develop new security systems and procedures. There is a need for high-quality protection because the amateur hackers of the past are being joined by more sophisticated attackers who increasingly are focused upon criminal and terrorist intent.

The purpose of the AGA 12 series — of which this is the first part — is to save SCADA operators time and effort by proposing a comprehensive system designed specifically to protect SCADA communications. AGA 12, Part 1 focuses on the background needed to understand the threats to SCADA communications, an approach to developing comprehensive security policies that include protection of SCADA communications, system-level requirements, and a general plan for testing equipment. Forthcoming, the AGA 12 reports are intended to address practices including retrofitting existing SCADA systems, networked systems, and cryptographic protection embedded in SCADA system components. Key management, protection of data at rest, and security policies are expected to be addressed in future addenda to AGA 12. Though this work originated in the gas industry, the AGA 12 Task Group sought to develop a set of practices that protect gas, electricity, water, wastewater, and pipeline real-time control systems.

AGA 12, Part 1 has been reviewed by experts in cryptography and communications, so that these practices might result in a secure cryptographic system. Cryptography is a difficult and subtle technology; therefore, the AGA 12 Task Group believes that utilities may find it easier and more secure to follow these practices, rather than implementing a proprietary solution whose security is difficult to evaluate.

End users may use the AGA 12 series to establish the general requirements for procuring a SCADA cyber security solution by including this specification in their procurement requirements. System integrators may use the AGA 12 series to ensure that SCADA cyber security is specified properly, and that the system test plan meets all the requirements needed to commission its security solution. Finally, manufacturers of SCADA hardware, software, and firmware may use the AGA 12 series to ensure that their product offerings address the needs of the end user for SCADA cyber security.

Acknowledgements

Paul Blomgren, SafeNet-Mykotronx
Bill Burr, National Institute of Standards and Technology
Jim Coats, Triangle MicroWorks
Bernie Cowens, SafeNet
Byron Coy, U.S. Department of Transportation Research and Special Programs Administration,
Office of Pipeline Safety
Kimberly Denbow, American Gas Association
Jim Evans, St. Claire Group, LLC
Matthew Franz, Cisco Systems, Inc.
Ray Gannon, Bristol Babcock
Grant Gilchrist, GE Energy Services
Art Griesser, National Institute of Standards and Technology
Matthew W. Harris, Peoples Energy Corporation
Dennis Holstein, OPUS Publishing
John A. Kinast, Gas Technology Institute
Joe McCarty, Gas Technology Institute
Michael McEvilley, Decisive Analytics
Kevin McGrath, KeySpan Energy Delivery
Brian McKeon, AirLink Communications, Inc.
John Meyo, Weston Technology
Steve Pettit, We Energies
Fred Proctor, National Institute of Standards and Technology
Ali Quraishi, American Gas Association
Bill Rush, Gas Technology Institute
Irv Schwartzenburg, Emerson Process Management
Aakash Shah, Gas Technology Institute
George A. Shaw, Peoples Energy Corp.
Lee Smith, HLS Consultant Services
John Tengdin, OPUS Publishing
Jay Wack, TecSec, Inc.
Al Wavering, National Institute of Standards and Technology
Joe Weiss, KEMA, Inc.
James Westervelt, Public Service Electric and Gas Co.
Clay Weston, Weston Technology
Andrew Wright, Cisco Systems, Inc.
Members of the AGA Gas Control Committee

AGA Report No. 12

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

March 14, 2006

Table of contents

How to Read AGA 12, Part 1	ii
1 Overview (informative).....	1
1.1 Scope of AGA 12.....	2
1.2 Purpose of AGA 12, Part 1	2
1.3 Document organization.....	2
1.4 How to read this report	3
1.4.1 Terminology	4
1.4.2 Road map for readability	4
2 Introduction (informative).....	6
2.1 SCADA communication systems are at risk.....	6
2.1.1 Vulnerabilities can be exploited	6
2.1.2 Attackers have a range of capabilities and motives	7
2.1.3 A successful attack can have serious consequences	8
2.2 Cyber security, cost, and operating issues.....	8
2.2.1 A published cryptography system is secure and flexible.....	9
2.2.2 Cost impacts of AGA 12	9
2.2.3 Operational impacts of AGA 12, Part 1	10
2.2.4 Certifying and evaluating AGA 12 products	10
2.3 Practice for addressing the limitations of cryptographic protection	10
2.4 Other considerations	10
3 Steps to define cyber security goals (normative)	12
3.1 Define the cyber security goals and practices.....	12
3.2 Understand the vulnerabilities, threats, and risks.....	13
3.3 AGA 12, Part 1 recommends two activities to determine the best course of action	13
3.4 Perform post-implementation audits.....	13
4 Cryptographic system requirements (normative)	14
4.1 System compliance requirements	15
4.1.1 AGA 12 compliance	15
4.1.2 NIST FIPS PUB 140-1 and 140-2 compliance	15
4.1.2.1 Cryptography compliance.....	17
4.1.2.2 Cryptographic hardware compliance.....	17
4.1.2.3 Cryptographic software compliance	18
4.1.2.4 Cryptographic algorithm compliance	18
4.1.3 Compliance certification	18
4.2 Cryptographic system component requirements.....	19

4.2.1	Management components	19
4.2.2	Cryptographic module components	19
4.2.2.1	General	20
4.2.2.2	SCADA Communication channel encryption components	20
4.2.2.3	Maintenance communication channel protection components	21
4.2.3	Environmental and power supply requirements	21
4.2.4	Quality requirements	21
4.2.4.1	SCADA Interoperability.....	21
4.2.4.2	Scalability.....	22
4.2.4.3	Reliability	22
4.2.4.4	Availability.....	22
4.2.4.5	Maintainability	22
4.2.4.6	Flexibility and expandability.....	22
4.3	Cryptographic system performance requirements	22
4.3.1	SCADA system response time	22
4.3.2	Cryptographic interoperability.....	22
4.4	Cryptographic system design goals	23
4.4.1	Key management	23
4.4.2	External communication interfaces to the SCADA system	23
4.4.2.1	Control center communication interface.....	23
4.4.2.2	Local SCADA master communication interface	24
4.4.2.3	RTU communication interface	24
4.4.3	Intrusion detection and forensics.....	24
5	Technical references (normative).....	26
Appendix A	Bibliography (informative).....	A-1
A.1	Books	A-1
A.2	Related standards	A-1
A.3	Web sites	A-2
Appendix B	Definition of terms, acronyms and abbreviations (normative).....	B-1
B.1	Definition of terms.....	B-1
B.2	Definition of acronyms and abbreviations	B-13
Appendix C	SCADA fundamentals (informative)	C-1
C.1	Characteristics of SCADA	C-1
C.1.1	Data acquisition	C-1
C.1.2	Status indications	C-2
C.1.3	Measured values	C-2
C.1.4	Monitoring and event reporting.....	C-2

C.1.5	Status monitoring.....	C-3
C.1.5.1	Limit-value monitoring	C-3
C.1.5.2	Trend monitoring	C-3
C.1.5.3	Data-quality analysis	C-4
C.1.5.4	Alarm processing	C-4
C.1.6	Control functions.....	C-4
C.1.6.1	Individual device control	C-4
C.1.6.2	Messages to regulating equipment	C-4
C.1.6.3	Sequential control schemes	C-4
C.1.6.4	Automatic control schemes	C-5
C.2	SCADA communication systems.....	C-5
C.2.1	Dedicated communication channel configurations.....	C-5
C.2.2	Native communication protocols.....	C-8
C.2.3	Communication links	C-8
Appendix D	Cryptography fundamentals (informative)	D-1
D.1	First considerations	D-1
D.2	Digitization of plaintext.....	D-2
D.3	Conversion of plaintext to ciphertext — the keytext generator.....	D-2
D.3.1	The secret keying variable.....	D-3
D.3.2	Matched plaintext and ciphertext will not compromise the keying variable.....	D-3
D.4	Block cipher function — modern keystone	D-3
D.4.1	Electronic codebook mode	D-4
D.4.2	Counter mode.....	D-4
D.4.3	Output feedback mode	D-4
D.4.4	Cipher block chaining	D-4
D.5	Hashing to achieve integrity	D-5
D.6	Methods to achieve authentication.....	D-5
D.7	Cryptographic keys and systems.....	D-5
D.7.1	Use of cryptographic keys for encryption	D-6
D.7.1.1	Long-lived keys.....	D-6
D.7.1.2	Short-lived keys	D-6
D.7.2	Use of cryptographic keys for digital signing	D-7
D.7.3	Use of digital certificates.....	D-7
D.8	Cryptographic algorithms.....	D-7
D.9	Cryptographic hardware	D-7
D.9.1	User token — the emerging technology	D-8
D.9.2	Desirable features in cryptographic hardware.....	D-8

Appendix E	Challenges in applying cryptography to SCADA communications (informative)	E-1
E.1	Encryption of repetitive messages	E-1
E.2	Minimizing delays due to cryptographic protection.....	E-1
E.3	Assuring integrity with minimal latency.....	E-1
E.3.1	Intra-message integrity	E-2
E.3.2	Inter-message integrity	E-3
E.4	Accommodating various SCADA poll and retry strategies	E-3
E.5	Avoiding communication channel collisions	E-4
E.6	Supporting mixed-mode deployments.....	E-4
E.7	Supporting broadcast messages.....	E-4
E.8	Incorporating key management.....	E-5
Appendix F	Cyber security practice fundamentals (normative).....	F-1
F.1	Recommendations for staffing an InfoSec team	F-1
F.2	Awareness of cyber security assurance.....	F-2
F.3	Recommendations for writing cyber security policies	F-4
F.4	Recommendations for performing assessment and analysis.....	F-6
F.4.1	Three-layer analysis	F-7
F.4.1.1	First steps	F-7
F.4.1.2	Post-TLA evaluation	F-7
F.4.2	Cyber security architecture analysis.....	F-7
F.4.3	Successive compromise analysis.....	F-8
F.4.4	Risk analysis.....	F-8
F.4.4.1	Quantitative analysis	F-8
F.4.4.2	Qualitative analysis.....	F-9
F.4.4.3	The final step of risk analysis	F-9
F.5	Auditing.....	F-9
F.5.1	Preliminary action auditing	F-9
F.5.2	Post-implementation auditing	F-9
F.5.3	Recursive auditing	F-10
Appendix G	Classes of attacks against SCADA systems (informative).....	G-1
G.1	Technical references	G-1
G.2	Classes of attacks and security models addressed in the AGA 12 series	G-1
G.2.1	Communication participants and channels.....	G-1
G.2.2	Attacks on encryption schemes.....	G-2
G.2.3	Types of attack on signature schemes.....	G-3
G.2.3.1	Key-only attacks	G-3
G.2.3.2	Message attacks.....	G-3

G.2.4	Protocols and mechanisms	G-4
G.2.5	Attacks on protocol	G-4
G.2.6	Models for evaluating security	G-5
G.2.6.1	Unconditional security	G-5
G.2.6.2	Complexity-theoretic security	G-6
G.2.6.3	Provable security	G-6
G.2.6.4	Computational security	G-6
G.2.6.5	Ad hoc security	G-6
G.2.7	Attacks against SCADA databases and related repositories	G-7
G.2.7.1	Threats	G-7
G.2.7.2	Security model	G-7
G.3	Classes of attacks not addressed in the AGA 12 series	G-7
G.3.1	Physical attacks on SCADA	G-8
G.3.2	Layers of security not addressed	G-8
G.3.3	Interdependencies on other networks	G-8
G.3.4	Denial of service caused by cyber attack	G-8
G.3.4.1	Leased-line or dial-up communication service	G-9
G.3.4.2	IP-based communication service	G-9
G.3.4.3	Countermeasures for IP-based communication service attacks	G-9
G.3.5	Risk of terminal emulation attached directly to SCADA components	G-10
Appendix H	Cryptographic system test plan (normative)	H-1
H.1	Introduction	H-1
H.1.1	Purpose	H-1
H.1.2	Scope	H-1
H.1.3	Test and evaluation objectives	H-1
H.1.4	Intended use for CSTP	H-1
H.1.4.1	Primary use	H-1
H.1.4.2	Other uses	H-1
H.1.5	Maintenance of this document	H-2
H.2	Technical references	H-2
H.3	Test requirements and evaluation criteria	H-3
H.3.1	Functional and performance requirements	H-3
H.3.1.1	Evaluation of compliance with CM design requirements	H-3
H.3.1.2	Application feature/functional testing	H-3
H.3.1.2.1	Test measurements	H-3
H.3.1.2.2	Test configurations	H-4
H.3.1.2.3	Load model	H-4

H.3.1.3 Synchronization testing	H-4
H.3.1.3.1 Clock synchronization test	H-4
H.3.1.3.2 CM jitter test	H-4
H.3.1.3.3 CM protocol synchronization test	H-5
H.3.1.3.4 Requirements to measure performance characteristics	H-5
H.3.1.3.4.1 Timing measurements	H-5
H.3.1.3.4.2 Block length probing	H-5
H.3.1.3.4.3 Effect of message content on latency	H-6
H.3.1.3.4.4 Throughput testing	H-6
H.3.1.3.4.5 Throughput measurements	H-6
H.3.1.3.4.6 Performance test configurations	H-7
H.3.1.3.4.7 Load model	H-7
H.3.1.3.5 Evaluation of the effect of noise on CM performance	H-7
H.3.1.3.6 Susceptibility to adverse conditions	H-8
H.3.2 Operability tests	H-8
H.3.2.1 Regression testing	H-8
H.3.2.2 Reliability testing	H-8
H.3.2.2.1 Test measurements	H-9
H.3.2.2.2 Test configurations	H-9
H.3.2.2.3 Load model	H-10
H.3.2.2.3.1 Throughput load model	H-10
H.3.2.2.3.2 Load modeling bursty traffic	H-10
H.3.2.2.3.3 Baseline load model	H-10
H.3.2.3 Bottleneck identification and problem isolation	H-11
H.4 Interoperability testing	H-11
H.5 Special test setup requirements	H-11
H.5.1.1 General considerations	H-11
H.5.1.2 Key channel characteristics	H-11
H.5.2 Modbus time-out parameter assignment	H-12
H.6 Test reports	H-13
H.6.1 Ownership of test results	H-13
H.6.2 Standard report format	H-13
H.7 Test architecture and environment	H-13

Table of figures

Figure 4-1 One example of a cryptographic system configuration.....	14
Figure C-1 SCADA system can be configured point-to-point.....	C-6
Figure C-2 SCADA system can include RTUs connected in series	C-6
Figure C-3 SCADA systems can include RTUs connected in a series-star configuration	C-7
Figure C-4 SCADA system with RTUs in a multi-drop architecture	C-7
Figure C-5 Example of communication links	C-9
Figure D-1 Conversion of plaintext to ciphertext	D-3

Table of tables

Table 1- 1 AGA 12, Part 1 Organization.....	2
Table 1- 2 Document roadmap for readability	5
Table 2- 1 Reality of the vulnerabilities	6
Table 2- 2 Capabilities and motivation to initiate an attack	7
Table 4- 1 FIPS PUB 140-2 requirements.....	16
Table B- 1 Definition of Terms.....	B-1
Table B- 2 Definitions of Acronyms and Abbreviations	B-13
Table F- 1 Cyber security categories and classes	F-2

1 Overview (informative)

The AGA 12 series of documents proposes practices designed to protect SCADA communications against cyber attacks. The practices focus on ensuring the confidentiality of SCADA communications; i.e., known to be unaltered by potential attackers and that can be authenticated as having originated from valid authorized users.

This report, AGA Report No. 12, “Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan” (AGA 12, Part 1), is the basic document that applies generally to all areas of cryptographic protection of SCADA systems.

Subsequent documents will address more specific subjects, such as:

AGA 12, Part 2: Retrofit link encryption for asynchronous serial communications

AGA 12, Part 3: Protection of networked systems

AGA 12, Part 4: Protection embedded in SCADA components

Additional topics planned for future addenda in this series include key management, protection of data at rest, and security policies.

Because gas, water, wastewater, electricity, and pipeline SCADA systems have many commonalities, the recommendations of the AGA 12 series can be applied to these other systems.

In addition, portions of this report apply to some DCS used in process or manufacturing control systems.

The purpose of the AGA 12 series is to save SCADA system owners’ time and effort by proposing a comprehensive system designed specifically to protect SCADA communications. While the use of cryptographic protection is not required, the purpose of the AGA 12 series is to develop practices that are intended to provide secure and easy-to-implement cryptography.

The AGA 12 series is being developed under the guidance of experts in cryptography and communications. AGA 12, Part 1 uses cryptographic algorithms approved by NIST and requires FIPS PUB 140-2 compliance.¹ Because cryptography is a sufficiently difficult and subtle area, the AGA 12 Task Group has developed the following path to aid in securing SCADA communications and significantly improving secure access to the maintenance ports of field devices.

It is essential for SCADA system operators to recognize that cryptography serves as only one tool to aid in SCADA security. Cryptography is effective only if it is deployed as part of a comprehensive set of cyber security policies and when it is combined with adequate attention to security of physical infrastructure access. Operating a secure cryptographic system requires more than a technological fix. Systems are compromised most often by attacks against lax operating procedures and poor implementations. Consequently, AGA 12, Part 1 provides a series of model policies that may be used or modified to meet specific company requirements.

¹The AGA 12 series, with the appropriate tailoring for SCADA operations, uses approved standards to ensure that the cryptographic recommendations made in the series of reports are well-vetted and represent the best technology for this application.

1.1 Scope of AGA 12

The scope of AGA 12, Part 1 is to describe the need for SCADA system protection and suggest that an affordable solution may be available. AGA 12, Part 1 proposes steps to define cyber security goals and cyber security practice fundamentals. More significant, AGA 12, Part 1 also defines the cryptographic system requirements and constraints, and cryptographic system test plan applicable to the AGA 12 series.

1.2 Purpose of AGA 12, Part 1

Different audiences will find different uses for the AGA 12 series. In this context, AGA 12, Part 1 serves three purposes:

End users: As an initial step to establishing a cyber security program that defines what is to be protected and all the goals and requirements to protect it. These general requirements should be used to implement, procure, and maintain a SCADA cyber security solution. These requirements necessary for application of the AGA 12 series may be included in the users' procurement specifications.

System integrators: As an initial step to ensuring that SCADA cyber security is specified properly and that the system test plan meets requirements needed to commission the deployed SCADA communication system security solution.

SCADA manufacturers of hardware, software, and firmware: As an initial step to ensuring their product offerings address the needs of the end user for SCADA cyber security.

1.3 Document organization

The content of each section is briefly summarized in Table 1- 1.

Table 1- 1 AGA 12, Part 1 Organization

SECTION OR APPENDIX	TITLE	SUMMARY	TYPE
1	Overview	Description of AGA 12 series, and the scope and purpose of AGA 12, Part 1.	Informative
2	Introduction	The need to protect SCADA communication systems and the cost of implementing this protection.	Informative
3	Steps to define cyber security goals	A guide to the steps a user should take to define cyber security goals and standards; to understand the vulnerabilities, threats and risks; and determine the best course of action.	Normative
4	Cryptographic system requirements	A general specification of the cryptographic system requirements for compliance, component hardware and software, performance, and design goals.	Normative

SECTION OR APPENDIX	TITLE	SUMMARY	TYPE
5	Technical references	List of references that are part of AGA 12, Part 1.	Normative
Appendix A	Bibliography	List of documents that a reader would find helpful in understanding AGA 12, Part 1.	Informative
Appendix B	Definition of terms and acronyms	Terms and acronyms used throughout the document.	Normative
Appendix C	SCADA fundamentals	Describes the basics of SCADA systems — background on system being protected	Informative
Appendix D	Cryptography fundamentals	Describes the basics of cryptography — what it is, what it does, what it does not do, and special issues relating to SCADA systems.	Informative
Appendix E	Challenges in applying cryptography to SCADA	Describes the challenge of providing integrity and confidentiality on a low-bandwidth network.	Informative
Appendix F	Cyber security practice fundamentals	Describes the fundamental processes to establish the InfoSec team, to write cyber security policies, and to perform assessments and audits.	Normative
Appendix G	Dealing with cyber attacks not addressed in the AGA 12 series	Describes the classes of attacks and security models in the AGA 12 series that are addressed and those not addressed.	Informative
Appendix H	Cryptographic system test plan	System test plan describing test and evaluation objectives, test requirements and evaluation criteria, interoperability testing, special test setup requirements, test reports, and test architecture and environment.	Normative

1.4 How to read this report

Because the AGA 12 Task Group sought to be precise and complete, reading AGA 12, Part 1 presents the reader with two challenges. First, the authors exerted considerable effort in being certain the terminology is unambiguous and consistent, making it necessary the reader understand the specific meanings associated with the terms used.

Second, the operability of this practice necessitates that all aspects of the subject of cryptography applied to SCADA communications be addressed, even though the reader

may not be interested in all of the topics.

The following sections address these challenges by first discussing terminology and then explaining the organization of the document.

1.4.1 Terminology

Because AGA 12, Part 1 brings together concepts from areas as diverse as cryptography, real-time operating systems, communication protocols, and corporate cyber security policy, meaningful discussion requires agreement on terminology. Appendix B is a complete set of definitions for terms used in AGA 12, Part 1.

While most readers will naturally consult the glossary of Appendix B on encountering unfamiliar terms, the AGA 12, Part 1 uses a number of quite common words with specific meanings. **The following is a subset of those definitions that readers should recognize as having specific meanings within the context of the report.**

May: The word “may,” equivalent to “is permitted,” is used to indicate a course of action permissible within the limits of this AGA 12, Part 1.

Must: The use of the word “must” is deprecated and shall not be used when stating mandatory requirements. The word “must” is used only when describing unavoidable situations.

Recommended: The word “recommended” is used to indicate flexibility of choice with a strong preference alternative.

Shall: The word “shall,” equivalent to “is required to,” is used to indicate mandatory requirements, strictly followed in order to conform to the AGA 12, Part 1 and from which no deviation is permitted.

Should: The word “should,” equivalent to “is recommended that,” is used to indicate the following.

- Among several possibilities one is recommended as particularly suitable, without mentioning or excluding others.
- That a certain course of action is preferred but not required.
- That (in the negative form) a certain course of action is deprecated but not prohibited.

An additional set of terms that is important to understand is “normative” and “informative.” Normative material is the set of requirements that are mandatory for the product or system to claim compliance with AGA 12, Part 1. Informative material is included to make the content of AGA 12, Part 1 easier to understand. As such, informative material might include suggestions for more efficient operation, explain parts of the AGA 12, Part 1, or supply the rationale for decisions that were made. Note that it is mandatory that products or systems claiming compliance with this document comply with all normative appendices or explicitly state and characterize areas of noncompliance.

1.4.2 Road map for readability

AGA 12, Part 1 is written to address the needs of several audiences. To use this document, readers should first consult the list in Table 1- 2, and identify which of these audience descriptions best describes them. Each reader then is directed to the sections that are likely to be of greatest interest, listed in the order in which they are read most easily. In addition to reading the recommended sections, each reader should read the

Preface and Executive Summary.

Table 1- 2 Document roadmap for readability

Audience	Need	Parts To Read
Senior executives	Set policies ensuring appropriate protection for SCADA systems.	Sections 1, 2, 3, and Appendix F.
Mid-level managers	Ensure the corporation complies with the security policies set by senior executives.	Sections 1, 2, 3, Appendix E, Appendix F and Appendix G.
Engineers and designers	Specify distribution and transmission company cryptographic protection.	Sections 1, 2, 3, 4, Appendix D, Appendix E, Appendix F, Appendix G and Appendix H.
Manufacturers	Understand the general requirements and cryptographic system test plan.	Sections 1, 2, 3, 4, Appendix D, Appendix E, Appendix F, Appendix G and Appendix H.
Consultants & system integrators	Advise SCADA engineers and designers on the design and operation of such systems to protect against cyber attack.	Sections 1, 2, 3, 4, Appendix D, Appendix E, Appendix F, Appendix G and Appendix H.
Cryptographic experts	Understand the special constraints of SCADA systems and to evaluate the work the AGA 12 Task Group has done.	Sections 1, 2, 3, 4, Appendix A, , Appendix E, Appendix F, Appendix G and Appendix H.
Certifying agencies	To validate compliance with AGA 12, Part 1.	Sections 1, 2, 3, 4, Appendix D, Appendix E, Appendix F, Appendix G and Appendix H.

2 Introduction (informative)

The objectives of this section are to make the reader aware that SCADA communications are at risk, that a uniform-based cryptographic system can protect SCADA communications and to outline a plan of action. Each of these topics is outlined below.

2.1 SCADA communication systems are at risk

In recognition of the importance of SCADA system operators understanding the risks from attacks on their system, AGA 12, Part 1 identifies both the threat agents (entities who might harm the system) and the kinds of attacks that might be mounted. The details of how particular attacks might adversely affect system operation are beyond the scope of this report. Part of the rationale for considering risks is the belief that SCADA system owners should understand the kinds of attacks that are possible and the reasonable probability that such attacks can occur.

2.1.1 Vulnerabilities can be exploited

No matter how much dedication or resources a threat agent may have, there is no risk unless there are vulnerabilities that can be exploited. Some companies that use SCADA systems assume that they have no vulnerabilities; that is, SCADA systems are inherently secure so that access by an intruder is not possible. Table 2- 1, which is not an exhaustive list, illustrates common assumptions and the situations that often are found to be more realistic.

Table 2- 1 Reality of the vulnerabilities

Assumption	Reality
We use leased lines, so nobody has access to our communications.	It's easy to tap these lines. The web site www.tscm.com/outsideplant.html shows many examples.
We use dial-up phone lines, but nobody knows the phone numbers.	A tap on outgoing lines or detailed billing records quickly reveals every phone number dialed by the master. "War dialer" software is available on the Internet to automatically dial banks of numbers and identify those that are answered by a modem.
We use dial-back modems so that unauthorized users cannot gain access.	Once the line is tapped, dial-back is easily defeated. Other known methods do not require tapping the line.
Our systems are protected by passwords.	Methods of stealing passwords are widely known. The easiest is to simply eavesdrop when the password is sent, in the clear, over the communication link. Dictionary "guessing" attacks are common also. Sharing passwords and/or never changing them are common and dangerous practices.

Assumption	Reality
We use frequency-hopping spread spectrum radio, the same as the military uses for secure communication.	There are simple methods to decode frequency-hopping sequences. The Wireless LAN Association specifically recommends using encryption on all networks, including spread spectrum. That's what the military uses — encryption.
We use a proprietary protocol so an eavesdropper couldn't understand our SCADA messages.	Even proprietary protocols are known more widely than many realize. Vendors, vendors' consultants, your current and former employees, and current and former employees of other companies using the same SCADA protocol will know the details. Manuals and software tools for analyzing protocols can be downloaded from the Internet.

Overall, the conclusion of the foregoing discussions suggests that there are credible vulnerabilities that threat agents could exploit.

With little effort, an attacker can scan the communication links between remote sites, as well as between remote sites and control centers. Access also can be gained through back channels used to establish field device operational settings and to modify field device software. In a control center, many SCADA systems write data to a master station database, which then is read by others to perform a wide variety of business functions. This interface also may be compromised, giving the attacker access to either SCADA operations or to sensitive data used by business operations.

2.1.2 Attackers have a range of capabilities and motives

Threat agents can arise from many groups of people. These potential attackers will have a wide range of capabilities, resources, organizational support, and motivations. Table 2- 2 includes a brief list of potential attackers, their capabilities and resources, and their motivation to initiate an attack. An attacker could be a disgruntled employee, an employee who recently was laid-off, a third-party maintenance contractor, a vendor supplying SCADA hardware and software, or a rogue state. All probably have the ability to access your SCADA system.

Table 2- 2 Capabilities and motivation to initiate an attack

Attacker/threat agent	Special capabilities/resources	Motivation
Hackers	Computer, spare time, dedication	Fun, challenge, fame
Organized crime	Computer skill	Financial gain
Traders	Computer skill	Financial gain

Attacker/threat agent	Special capabilities/resources	Motivation
Extremist groups	Computer skill, dedication	Harm groups they oppose
Terrorists	Computer skill, spying, money, organization	Terrorize, finance operations, economic damage
Foreign governments	SCADA expertise, large computers, cryptographers, intelligence agency, money, military	Strategic military and/or economic damage
Insiders, contractors	System access, confidential information	Revenge, union issue, grievance
Alliances of above groups	Combined resources of any above group	Alliance of convenience to advance own interest

2.1.3 A successful attack can have serious consequences

Because the AGA 12 Task Group does not wish to aid potential attackers with a detailed list of the types of damage that could be done by attacking a SCADA system, the following discussion only suggests questions that companies using these systems can investigate on their own. As this report suggests in Section 3 and Appendix F, one of the first steps that should be taken by a company that relies on SCADA is to assess its risks using well-known methodologies for this investigation. A systematic risk assessment will result in a list of vulnerabilities, as well as a quantitative ranking of the consequences of a successful exploitation of the vulnerability.

Based on the previous discussion, it is prudent to assume that an attacker can learn how an installed SCADA system operates. The ability to access and read SCADA data provides two important pieces of information to the attacker: Status data provides the information needed to understand the status of systems that control operations, and control data (settings) and commands provide the information needed to perform the control actions. Attackers can modify system software and firmware, as well as exploit undocumented commands and features in a field device. This situation implies that most of the changes that can be made by an authorized operator of the SCADA system can be made by an attacker too. Full development of the implications of this situation is the responsibility of the organization that relies on the SCADA system.

2.2 Cyber security, cost, and operating issues

Any introductory discussion of cryptographic protection of SCADA systems should address some of the most common concerns of companies that operate these control systems. During discussions that took place while AGA 12, Part 1 was under development, a number of concerns were raised frequently. The most common questions were:

1. Won't a known cryptography system freeze technology and be broken because it is known?
2. Won't it be expensive to add cryptography?
3. Won't cryptographic protection slow real time communication too much?
4. How can we tell how well AGA 12, Part 1-compliant equipment will work?

These issues are addressed briefly in the following sections.

2.2.1 A published cryptography system is secure and flexible

The concept of a published system that underlies secure transmission of data raises the twin concerns that, first, attackers who know the cryptographic system can attack it easily and that, second, it will freeze technology that should be allowed to evolve.

The experience of the cryptographic community has shown that publishing a cryptographic system does not weaken it. The reason is that cryptographic algorithms derive their security from a "key" or a number that the assailant does not know, rather than from a secret mechanism (see Appendix E).

An analogy: The mechanism of a standard combination lock is well-known, but the ability to open it easily depends on having the "combination," or a number that the assailant does not know.

AGA 12, Part 1 uses algorithms evaluated by NIST and by the NSA that were found to be "cryptographically secure." "Cryptographically secure" does NOT mean "unbreakable." Guessing the key can break all of these algorithms. However, it requires thousands to millions of years (depending on the key length) for state-of-the-art key-guessing systems to deduce the correct key. In contrast to relying on a single and widely reviewed system, users of proprietary codes, which have not been extensively reviewed, often find their systems are broken by hackers shortly after the system is deployed. The majority of codes proposed even by professional cryptographers is compromised by other professional cryptographers during the open review process.

Consequently, the AGA 12 Task Group proposes that the industry adopt a single cryptographic system rather than a diverse mix of systems that have not undergone public peer review.

The collective AGA 12, Part 1 approach, however, permits the introduction of new algorithms (cipher suites) and new technologies as they are validated in accordance with the practice specified in Section 4.1.

2.2.2 Cost impacts of AGA 12

Recognize that deploying cryptographic protection is a cost/benefit business decision like any other. If your risk assessment shows that the compromise of a particular SCADA facility is of minimal operational or economic consequence, it makes little economic sense to provide cryptographic protection for that facility. AGA 12, Part 1 does not discuss cost; rather, Section 3 and Appendix F describe a method to develop a solution that is proportional to risk.

The AGA 12 Task Group did not identify price points for cryptographic systems for two reasons. First, the AGA 12, Part 1 is flexible and allows vendors to differentiate products along many dimensions. Vendors may offer a product that has few options but targets a very specific SCADA system, at a correspondingly low price. Other vendors may offer products with extensive security options and flexibilities, at a correspondingly higher

price.

Second, it is difficult to predict prices. Because the trend is to install standard communication-based intelligent electronic devices, the economy of scale should result in competitively priced cryptographic solutions for SCADA communications.

Though AGA 12, Part 1 does not discuss costs in detail, it attempts to facilitate the lowest possible life-cycle cost. That is, any vendor that believes it can produce a marketable product at a lower price than those already in the market, may do so because these vendors have the complete functional specification for the product. The AGA 12 Task Group believes that market competition will produce lower cost products than would be available with a wide range of competing, proprietary products.

2.2.3 Operational impacts of AGA 12, Part 1

The specifications in AGA 12, Part 1 were developed to minimize the additional latency that encryption adds to communication time. Testing indicates that the increased delay caused by the relatively slow retrofit CM is small enough that it is acceptable to most SCADA operators. Individual SCADA system operators should decide on the trade-off between a security risk of using an unprotected system and the degradation in performance.

As with adding any device to a SCADA system, maintenance and failure issues should be addressed by careful selection of reliable electronic security system components.

2.2.4 Certifying and evaluating AGA 12 products

The requirements to certify AGA 12, Part 1 to products are addressed in Section 4.1.3, and the requirements to evaluate AGA 12, Part 1 products are addressed in Appendix H.

2.3 Practice for addressing the limitations of cryptographic protection

It is important to recognize that, despite its many benefits, cryptography is not a panacea. Rather, it should be viewed as an important component of a much larger tool kit. It is outside of the scope of AGA 12, Part 1 to provide a complete discussion of the types of attacks against which cryptographic protection is not effective. However, Appendix G does contain limited suggestions for methods of dealing with attacks against which cryptography is not effective. Although this list of possible attacks is not exhaustive, it should be of some help.

Following the risk-assessment procedures described in Section 3 and Appendix F should result in a list of vulnerabilities in your SCADA system. Good operating practices resulting from applying the procedures of AGA 12, Part 1 Section 3 and Appendix F should reduce the probabilities and/or the consequences of a successful attack.

2.4 Other considerations

Once a company has decided to investigate its level of SCADA cyber attack risk, the company should conduct a risk assessment to evaluate the business case for SCADA security and to develop security policies as required.

Risk assessments can be addressed in phases. As suggested earlier, there are formal risk-assessment methodologies that provide thorough and systematic approaches to

identifying and quantifying risks. This is the recommended approach to risk assessment. However, many companies start with a simple audit checklist for cyber security vulnerabilities or a penetration study. Even these simple initial first steps will indicate the need for protecting SCADA systems. These initial analyses often indicate the need for more formal risk evaluations. However, it is important to recognize that the simple audits do not provide a basis on which to make fundamental decisions, such as how much risk a company will accept or who is responsible for making the decision.

One of the important topics this report addresses is development of security policies. While practices often focus on hardware or specific operating procedures, policies often are not included.

3 Steps to define cyber security goals (normative)

To successfully secure an operational infrastructure, AGA 12, Part 1 recommends taking the following steps before purchasing and deploying any type of cyber security technology.

- Define the cyber security goals and practices.
- Understand the vulnerabilities, threats and risks that an organization may face.
- Determine the best course of action to mitigate the vulnerabilities, threats and risks to an acceptable level.
- After implementation, review immediately (and periodically thereafter) to determine if the vulnerabilities, threats and risks still exist, have changed, or if they were properly mitigated to an acceptable level.

Appendix F of AGA 12, Part 1 provides background and rationale to support the recommendations in Section 3 and adds more detailed recommendations.

A forthcoming addendum to AGA 12, Part 1 will contain a number of sample cyber security policies that the AGA 12 Task Group has developed for gas, water, wastewater, electricity and pipeline SCADA systems. Most of these security policies will be included as *informative*, meaning they are provided for reference. Some of these policies may be *normative*, meaning to claim compliance with AGA 12, Part 1 requires the end user and manufacturers to implement and adhere to the cyber security policies as written.

The *informative* cyber security policies were written as templates, meaning they are examples intended to be customized. They document policies that address vulnerabilities found within any business and provide a suggested list of practices and procedures that may reduce the risk if a particular vulnerability is exploited.

End users are encouraged to take ownership of the *informative* policies by reviewing them, modifying them to match their corporate needs and culture, and implementing them. The goal of a cyber security policy is to mitigate risk, but it is effective only if it is adhered to on a daily basis.

The following sections summarize the recommendations contained in AGA 12, Part 1.

3.1 Define the cyber security goals and practices

AGA 12, Part 1 recommends the formation of an InfoSec team that is responsible for defining and documenting security goals and standards applicable to all organizations within the utility. Operations, responsible for SCADA (including its cyber security,) should be a permanent member of the InfoSec team. AGA 12, Part 1 also recommends that a senior member of management be the team leader to ensure adequate participation and accountability of all applicable organizations.

As a minimum, AGA 12, Part 1 recommends that cyber security goals and standards address both departmental operating requirements and corporate business practice requirements. These security goals and standards should be extended to include all business partners, contractors, and vendors to ensure consistent treatment of information, transactions, and company resources. Special attention should be given to the practices that address information sensitivity and access control privileges granted to business partners and vendors assisting engineering, maintenance, and operations through outsourcing contracts and other agreements.

AGA 12, Part 1 recommends that all cyber security goals and practices be described clearly in cyber security policies. As a minimum, these policies should describe all cyber security requirements for choosing, installing, maintaining, and decommissioning software, hardware and information associated with the company's cyber system, including field operation's systems and networks. Each security policy should dictate the responsibilities, practices, and procedures of every employee, contractor, business partner, and third party that has access to the company's cyber system or performs some type of service affecting the system.

3.2 Understand the vulnerabilities, threats, and risks

AGA 12, Part 1 recommends that the InfoSec team make use of research findings from internal risk-management departments, failure-mode analysis and HAZOP reviews as related to cyber security and from external sources, such as government, industry, risk-management companies and vendors, to assist in understanding its vulnerabilities, threats and risks. Many organizations, including government agencies, industry associations, and vendors, have documented and are continuing to document vulnerabilities, threats and risks common to all utilities or the technology they deploy in their field operation networks.

AGA 12, Part 1 recommends that the InfoSec team conduct, or commission a third party (e.g., vendor) to conduct, a comprehensive assessment of the vulnerabilities, threats and risks unique to its field operation communication networks, the systems connected to these networks, and the business processes that rely on these networks.

3.3 AGA 12, Part 1 recommends two activities to determine the best course of action

- Conduct a preliminary action audit to develop a list of common-sense cyber security measures that should be implemented. Many organizations, including government agencies, industry associations, and vendors, are conducting seminars or producing tutorials or books (such as the proper settings on a firewall or a web server) that can be used to develop this list.
- Using the comprehensive assessment and analysis described in Section 3.2, the InfoSec team should evaluate and rank in order the risks to continuity of operations and business. AGA 12, Part 1 recommends that comparative lists be developed from the risk analysis; one based on cost effectiveness and one based on company priorities.

3.4 Perform post-implementation audits

AGA 12, Part 1 recommends that the InfoSec team be retained on a permanent basis to perform post-implementation audits at regular intervals. These audits should be performed to determine if the corrective actions installed have produced the desired results. If they have not, another round of assessment and analysis should be conducted until the weaknesses are mitigated to the desired level. Each audit should consider new vulnerabilities, threats and risks that have been identified, as well as changes to internal goals and standards.

4 Cryptographic system requirements (normative)

Section 4 addresses system compliance requirements, cryptographic system component requirements, cryptographic system performance requirements, and cryptographic system design goals.

The system requirements specified in Section 4 are derived from the normative security policies and practices specified in Section 3 and Appendix F. Additional background information is presented in Appendix E and Appendix G, to provide a better understanding of the cryptographic system requirements.

Figure 4-1 shows one example of how a cryptographic system can be configured. In this example, two types of CMs are shown. An SCM provides both authentication and encryption capabilities for SCADA channels. MCM provides authenticated access to maintenance ports on an IED and an RTU.

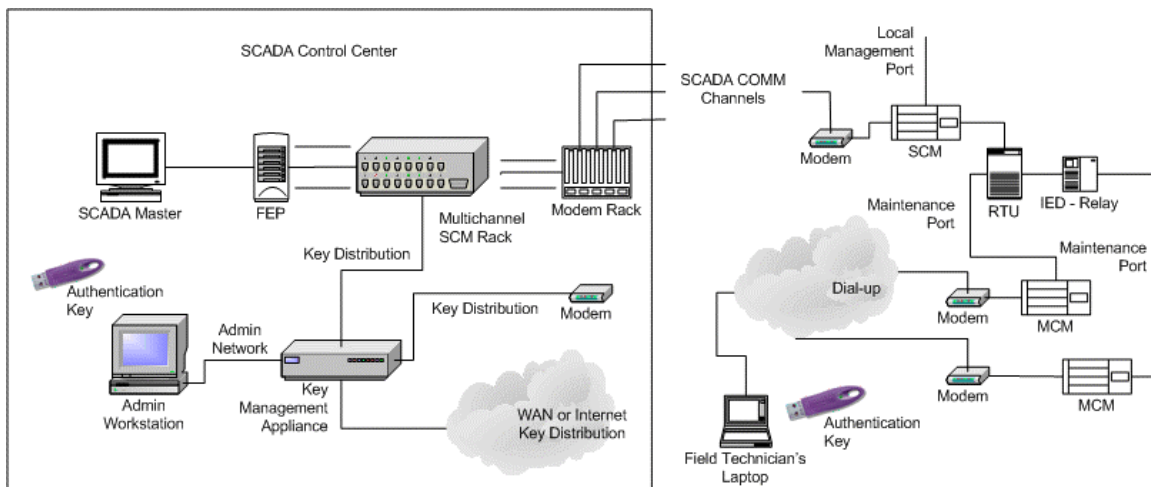


Figure 4-1 One example of a cryptographic system configuration

In this example, the SCADA master is connected to a FEP, which without AGA 12, Part 1-compliant security would be connected to a modem rack. An AGA-compliant rack-mounted SCM is installed between the FEP and the modem rack to provide both secure authentication and encryption on the SCADA communication channels. At the remote site, another AGA 12, Part 1-compliant SCM is installed between the modem and the RTU.

Continuing with this example, Figure 4-1 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 to satisfy the AGA 12, Part 1 requirement for two-factor authentication. In this example the technician dial-up goes through an auto-answer modem to an MCM, which in turn is connected to the maintenance port of the RTU as well as to an IED (perhaps a relay).

Although not shown for all SCMs and MCMs, the modules all have local management ports that are used to change cryptographic parameters.

In the control center, Figure 4-1 shows an AGA 12, Part 1-compliant administration workstation used to manage the cryptographic keys for the system. An AGA 12, Part 1-compliant key management appliance is used to distribute the keys to the rack-mounted SCM, to field SCMs, to field MCMs, and to other AGA 12, Part 1-compliant devices by

modem communications, WAN or Internet communications. Although not shown, the key management components should be defined within a separate security domain.

4.1 System compliance requirements

Cryptographic system compliance requirements are specified for AGA 12, Part 1 compliance, NIST FIPS PUB 140-2 compliance, cryptography compliance, and compliance certification.

4.1.1 AGA 12 compliance

It is mandatory that products or systems claiming compliance with the AGA 12 series comply with all applicable normative sections, appendices and addenda, or explicitly state and characterize areas of noncompliance.

Three addenda to AGA 12, Part 1 are planned: Key Management, Protection of Data at Rest, and Security Policies.

Three documents are planned to address specific implementation requirements.

- Asynchronous serial cryptographic system components shall comply with AGA 12, Part 2.
- Cryptographic system components IP shall comply with AGA 12, Part 3.
- Embedded cryptographic system components shall comply with AGA 12, Part 4.

4.1.2 NIST FIPS PUB 140-1 and 140-2 compliance

A device complies with AGA 12 if it meets all applicable normative sections, appendices, and addenda of the AGA 12 series and has either FIPS PUBs 140-1 or 140-2 certification.

FIPS PUB 140-2 superseded FIPS PUB 140-1 in May 2001. The primary differences between the two standards are the support of new algorithms (AES, RSA, and ECDSA); discontinued support of older algorithms; and the additional documentation manufacturers provide during a CM certification process. All CMs entering the market after May 2001 or updated to incorporate the newly supported algorithms shall be certified in accordance with FIPS PUB 140-2. However, any CM certified under FIPS PUB 140-1 before May 2001 remains valid for the purposes and implementation for which it was designed.

All AGA 12, Part 1-compliant CMs shall comply with the requirements shown in Table 4-1, which are extracted from FIPS PUB 140-2 [8]. Security levels in Table 4-1 are defined in Section 1 of FIPS PUB 140-2. The “recommendations and comments” in the second column of this table are FIPS PUB 140-2 requirements selected from the possible options as further specified in AGA 12, Part 1. Unless otherwise stated, CMs shall incorporate the details and documentation requirements in the corresponding FIPS PUB 140-2 section without modification.

Table 4- 1 FIPS PUB 140-2 requirements

FIPS PUB 140-2 section	AGA 12, Part 1 recommendations and comments
4.2 – Cryptographic module ports and interfaces	CM ports and interfaces shall satisfy security levels 3 and 4 (separate data and security parameter ports).
4.3.1 – Roles	The <i>User Role</i> may be assumed by machine, such as an intelligent electronic device, front end processor, or general purpose computer. The <i>Crypto Officer Role</i> may be assumed only by a properly authorized human. The <i>Maintenance Role</i> shall be provided.
4.3.2 – Services	Modules (SCM or MCM) shall support a bypass capability for user defined sessions using the mixed-mode function (see Section 4.2.2.2).
4.3.3 – Operator authentication	Security level 2 (role-based authentication) to control access to the module (SCM or MCM) is required. Security level 3 (identity-based authentication) is optional.
4.4 – Finite state model	<i>User states</i> in the model shall reflect normal operation of the modules (SCM or MCM). <i>Bypass states</i> and <i>maintenance states</i> are included because of the inclusion of those functions in previous sections of FIPS PUB 140-2.
4.5 – Physical security	Security level 2 (use of tamper-evident packaging) is required. Security level 3 (use of strong enclosures with tamper detection and response mechanisms for removable covers and doors) may be required when physical tampering cannot be observed in a timely fashion.
4.6 – Operational environment	Security level 2 (evaluated assurance level) is required.
4.8 –EMI/EMC	Security level 2 is required.
4.9.1 – Power up tests	Security level 2 is required.
4.10.2 – Delivery and operation	Security level 2, 3, and 4 (documentation and secure delivery) is required.

The bypass capability and state described in Table 4- 1 refer only to those situations in which one SCADA unit is communicating through a CM to another SCADA unit that is not protected by a CM; e.g., a SCADA host with a CM communicating with a field SCADA unit without a CM.

Mixed-mode operation allows the SCM deployed at the SCADA master to pass unencrypted communications between the SCADA master and specific RTUs. Mixed mode thus provides an alternately activated bypass capability as defined in FIPS PUB 140-2. If a bypass capability is implemented, FIPS PUB 140-2 requires “two independent internal actions shall be required to activate the capability ... (e.g., two different software or hardware flags are set” To meet FIPS PUB 140-2, if a vendor’s implementation supports mixed mode, the SCM shall include a hardware or software switch to enable mixed-mode operation (first of two flags), and a table (or equivalent) listing the SCADA addresses of specific RTUs to which communications are to be sent and received unencrypted (second of two flags). Also, if a vendor’s implementation supports mixed mode, the SCM shall indicate the status of the mixed-mode operation.

4.1.2.1 Cryptography compliance

Cryptography compliance requirements are specified for cryptographic hardware, cryptographic software, and cryptographic algorithm.

4.1.2.2 Cryptographic hardware compliance

AGA 12, Part 1 requires the following cryptographic hardware capabilities be implemented.

- Communication channel encryptor (a type of CM), authentication module (a CM that provides authentication), and user token² shall provide, as a minimum, FIPS PUBs 140-1 or 140-2 Level 2 tamper-evident physical enclosure and cryptographic boundary.
- HSM shall provide, at a minimum, FIPS PUBs 140-1 or 140-2 Level 3 tamper-active detection and prevention physical enclosure and cryptographic boundary.
- Cryptographic key materials shall be generated, exchanged, stored, utilized, and destroyed within FIPS PUBs 140-1- or 140-2-compliant cryptographic boundary.
- Cryptographic key generation requires the use of a FIPS-approved random number generator to produce key components and seed values. Only prime numbers generated and tested, consistent with ANSI X9.80 [12], shall be used to generate RSA-based public and private key pairs. In no case will the number be less than 1024 bits for RSA-based computations or 160 bits for Elliptic Curve, as defined in FIPS PUB 140-2 Annex A. A number shall be accepted as prime when a probabilistic algorithm that declares it prime is in error with a probability³ less than 2^{-100} .

²More explanation of user tokens is provided in D.9.1.

³The rate of failure probability is selected to be sufficiently small so that errors are extremely unlikely ever to occur in normal practice. Moreover, even if an error were to occur when one party tests a prime, subsequent tests by the same or other parties would detect the error with overwhelming probability.

- For communication channel encryptors, authentication modules, and user token, asymmetric private keys shall never be exposed outside of the cryptographic hardware device's FIPS PUBs 140-1- or 140-2-compliant cryptographic boundary.
- For HSMs, asymmetric private keys shall never be exposed in plaintext outside of the cryptographic hardware device's FIPS PUBs 140-1- or 140-2-compliant cryptographic boundary. HSM asymmetric private keys shall only be exposed outside of the cryptographic hardware for transfer to another HSM for disaster recovery purposes, or for operation of parallel control centers.⁴
- Symmetric keys shall never be exposed in plaintext outside of the cryptographic hardware device's FIPS PUBs 140-1- or 140-2-compliant cryptographic boundary.

4.1.2.3 Cryptographic software compliance

AGA 12, Part 1 does not recommend performing cryptography in a purely software environment. Performing cryptography in software exclusively exposes cryptographic tools and algorithms as well as keys to potential threats such as malicious code or intentional malicious actions by users. For this reason, AGA 12, Part 1 recommends as a minimum that a hardware token (smart card, USB or other uniquely identifiable device) be used as part of the User Identity and Authorization process.⁵

Cryptographic hardware requires the use of specific drivers and software, referred to as middleware, to interface the hardware to standard applications and IPs, including e-mail, browser, encryption/decryption, and digital signing clients. AGA 12, Part 1 recommends the use of industry reviewed, standards-based, cryptographic middleware, including Microsoft's CAPI and the industry standard PKCS.

4.1.2.4 Cryptographic algorithm compliance

AGA 12, Part 1 requires that all cryptographic algorithms have been through peer review and approved by NIST. AGA 12, Part 1 approved algorithms include:

- Encryption: AES with a minimum key length of 128 bits.
- Digital signing: RSA with a minimum key length of 1024 bits; and ECDSA with a minimum key length of 160 bits.
- Hashing: SHA-1.

4.1.3 Compliance certification

AGA 12, Part 1 recommends that CMs be certified by a member of the CMVP. Under this program, NIST accredits internationally recognized laboratories that are qualified to certify that components of the cryptographic system conform to FIPS. This assurance includes both the specifications and the adequacy with which the specification is implemented.

Obtaining FIPS PUB 140-2 certification is a significant commitment for manufacturers in

⁴One configuration for multiple control centers is a primary control center and one or more "hot" backups. The primary control center initiates queries and receives responses, while the backup control center only listens to the communications from the field. The backup control center can take over knowing the current status of field equipment if the primary center fails.

⁵This does not imply that a CM has a unique authentication port.

the forms of component selection, design criteria, testing and certification time, and their related costs. One of the certification criteria is that only released products may be submitted for CMVP final review. As such, it is likely that early products designed to comply with AGA 12, Part 1 and FIPS PUB 140-2 may be commercially available before they actually receive FIPS certification. Prior to receiving final certification, AGA 12, Part 1 recommends that product manufacturers provide the following:

- A written statement that their product is currently under CMVP review, or is about to go under CMVP review.
- An anticipated completion date of the CMVP review.

Once a product is certified, it will be listed on a NIST web site for public compliance verification (see <http://csrc.nist.gov/cryptval> [11]).

4.2 Cryptographic system component requirements

Cryptographic system component requirements are specified for management components, CM components, environmental and power supply requirements, and quality requirements.

4.2.1 Management components

The cryptographic management system shall, as a minimum, provide the capability to:

- Uniquely identify and authenticate operators accessing the management system.
- Uniquely identify and authenticate CMs that are managed by the management system, or use the services of the management system.
- Authorize operators and CMs using standards based, role-based access control (RBAC⁶) procedures.
- Configure and manage cryptographic system components.
- Generate, exchange, store, use, and destroy credentials and cryptographic keying materials within a cryptographic boundary that complies with FIPS PUBs 140-1 or 140-2 Level 2 or higher standard.
- Collect and report usage and forensic data to provide an audit trail of critical actions and events.
- Protect the confidentiality, integrity, and availability of data and information related to the cryptographic system.

4.2.2 Cryptographic module components

CM component requirements are specified for general requirements, SCADA communication channel encryption components, and maintenance communication channel protection components.

⁶RBAC is an alternative to Discretionary Access Control and Mandatory Access Control policies. The principle motivation behind RBAC is the desire to specify and enforce company-specific policies in a way that maps naturally to an organization's structure. Under RBAC, users are granted membership into roles based on their competencies and responsibilities. This basic concept has the advantage of simplifying the understanding and management of privileges.

4.2.2.1 General

All CM components shall, at a minimum, provide the capability to:

- Identify and authenticate CM components without operator action.
- Uniquely identify and authenticate operators accessing the CM components.
- Uniquely identify and authenticate a CM that is requesting services, such as session establishment.
- Authorize operators using RBAC.
- Generate, exchange, store, use, and destroy credentials and cryptographic keying materials within a cryptographic boundary that complies with FIPS PUBs 140-1 or 140-2 Level 2 or higher standard.
- Exhibit tamper evidence, and/or enable anti-tamper detection and prevention.
- Communicate through the management port for operator authentication, and CM configuration and management.
- Securely provision (loading of keying materials) and manage a CM both in-band (within the SCADA communication channel) and out-of-band (either remote or local update through a physically separate communication port or channel).
- Collect and make available usage and forensic data to the management system (see Section 4.2.1).
- CM's intrusion detection, as specified in Section 4.4.3, shall include an alarm output, which may be connected to an alarm point on the local RTU to alert the system operator that intrusion has been attempted.
- Monitor and terminate sessions when no activity occurs for a configurable period of time and/or event sequence.

4.2.2.2 SCADA Communication channel encryption components

As a minimum, SCM components shall provide, in addition to the general requirements (Section 4.2.2.1), the capability to:

- Authorize session establishment or reestablishment using RBAC.
- Operate in a mixed-mode⁷ communication topology.
- Operate in a multipoint, multidrop, point-to-point, and cascaded topology.
- Operate in broadcast or multicast modes.
- Pass through, in plaintext, communication system parameters (modem commands).
- Communicate through the plaintext port to SCADA devices, including control center equipment (a SCADA master or an FEP) and substation equipment (an RTU or local SCADA master).
- Communicate through the ciphertext port to SCADA communication equipment, including modems, routers, and radios.

⁷Mixed-mode is a topology in which some IEDs on a single communication channel are protected by CMs and others are not; for example, to facilitate deployment of CMs over time.

- Communicate through the management port for operator authentication, and communication channel encryptor configuration and management.

4.2.2.3 Maintenance communication channel protection components

As a minimum, MCM components⁸ shall provide, in addition to the general requirements (Section 4.2.2.1), the capability to:

- Authorize session establishment or reestablishment using multi-factor authentication and RBAC.⁹
- Communicate through the local port on the MCM to the maintenance ports of SCADA devices, including control center equipment (a SCADA master or an FEP) and substation equipment (an RTU, local SCADA master, or an IED).
- Encrypt messages once communication is established between the computer and the MCM.
- Use existing passwords in the IED and require minimal changes in the computer's existing remote access software.
- Provide authentication, independent of (or in parallel with) any authentication capabilities provided in the IED — such as IED password(s).
- Communicate through the MCM's remote port through the communication infrastructure (e.g., dial-up).
- Terminate the access if the USB authentication key (or smart card) is removed.
- Terminate the access if no activity is detected for a configurable period of time.
- Provide an external alarm output if the device fails to function, if tampering is detected, or if the power supply is lost.

4.2.3 Environmental and power supply requirements

AGA 12, Part 1 recommends that CMs and authentication modules installed in field sites be designed for an indoor substation environment as defined in IEEE STD™ 1613 [4]. The power supply shall have minimal power drain, with optional input voltage ratings of 120/240 vac, or 5 to 125 vdc.

4.2.4 Quality requirements

Quality requirements are defined for SCADA interoperability, scalability, reliability, availability, maintainability, and flexibility and expandability. AGA 12, Part 1 recommends that the phrase “shall not significantly degrade” used in the following subsections be quantified by the end user.

4.2.4.1 SCADA Interoperability

⁸Existing maintenance ports on RTUs, master stations and other IEDs generally have only simple password protection that is rarely changed. Access to these ports is generally through the dial-up telephone network. In some cases, the IED contain an integral auto-answer modem so that the phone line may be directly connected to the modem port. In other cases the IED does not have an internal modem and the maintenance port is a simple RS-232 serial port. In these cases an external auto-answer modem is needed.

⁹Existing dial-up software currently used for access to the maintenance ports may require modification to support two-factor authentication.