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.***

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.

---

[1]The 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 1uses 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 .

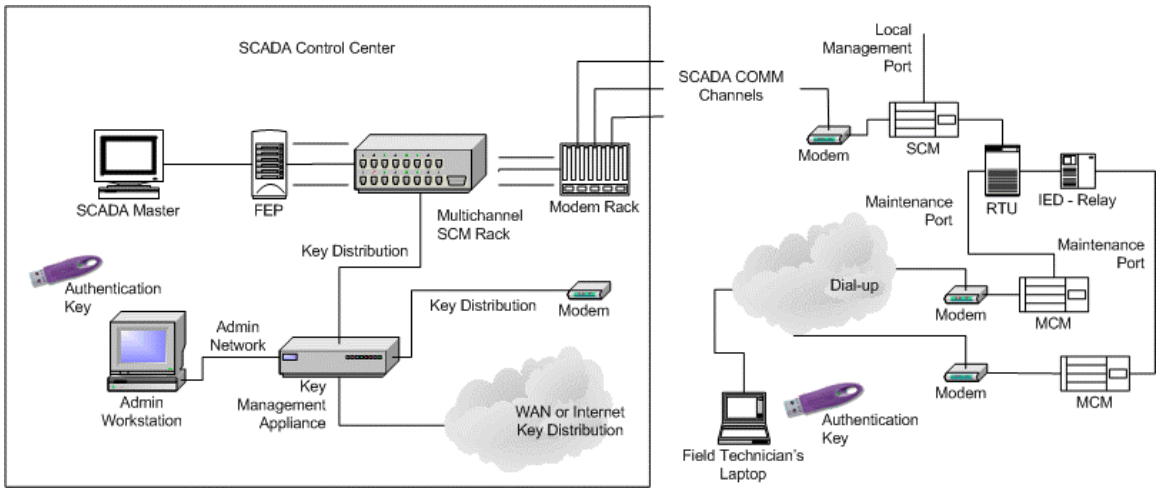


Figure 4-1 One example of a cryptographic system configuration

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 work station 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 *User Role* may be assumed by machine, such as an intelligent electronic device, front end processor, or general purpose computer. The *Crypto Officer Role* may be assumed only by a properly authorized human. The *Maintenance Role* 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	*User states* in the model shall reflect normal operation of the modules (SCM or MCM). *Bypass states* and *maintenance states* 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 token[2] 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 probability[3] less than 2 - 100.

---

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

[3]The 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

---

[4]One 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.

[5]This 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 (RBAC[6]) 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.

---

[6]RBAC 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-mode[7] 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.

[7]Mixed-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 components[8] 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

---

[8]Existing 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.

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

The cryptographic system or its components shall not degrade the capability of IEDs to interoperate[10] over networks on which they were designed to interoperate.

4.2.4.2 Scalability

The cryptographic system or its components shall not significantly degrade the scalability[11] of networks designed to operate without cryptographic protection.

4.2.4.3 Reliability

The cryptographic system or its components shall not significantly degrade the reliability of networks designed to operate without cryptographic protection.

4.2.4.4 Availability

The cryptographic system or its components shall not significantly degrade the availability of networks designed to operate without cryptographic protection.

4.2.4.5 Maintainability

The cryptographic system or its components shall not significantly degrade the maintainability of networks designed to operate without cryptographic protection.

4.2.4.6 Flexibility and expandability

The cryptographic system or its components shall not significantly degrade the flexibility and expandability of networks designed to operate without cryptographic protection.

4.3 Cryptographic system performance requirements

Cryptographic system performance requirements are specified for latency and cryptographic interoperability.

4.3.1 SCADA system response time

Communication channel encryption components shall not degrade the response time performance of the SCADA system below a user's defined acceptable level.[12]

4.3.2 Cryptographic interoperability

AGA 12 enforces limited cryptographic interoperability[13] by requiring all compliant components to exchange encrypted messages using at least one common cryptographic algorithm and to exchange session keys using at least one common key exchange

---

[10]Interoperability requires that cryptographic modules transcend products and networks.

[11]Scalability defines how capacity and load affect performance.

[12]From surveys, supported by discussion with users, a general rule-of-thumb is that the introduction of communication channel encryption should not introduce more than a 20 percent reduction in polling frequency. For example, if SCADA polling was set for 5-second intervals, the introduction of communication channel encryption would require that polling be set for 6-second intervals.

[13]A common cryptographic protocol is specified in subsequent documents of the AGA 12 series to define a design baseline for cryptographic interoperability. The cryptographic protocol is tailored for the operating environment addressed in each document (AGA 12, Part 2; AGA 12, Part 3; and AGA 12, Part 4).

method. While operating within one session, AGA 12, Part 1 requires at least one mode in which the shared session key, as a minimum, shall be used for encryption and decryption of SCADA messages between CMs at the master station and at the remote locations.

4.4 Cryptographic system design goals

Cryptographic system design goals are, from a user's point-of-view, described for key management, external interfaces to the SCADA system, and intrusion detection and forensics.

4.4.1 Key management

AGA 12, Part 1 recommends that a secure key management system, based on industry standards, be implemented to manage the keys for the cryptographic system. The key management system[14] shall be designed to achieve the following objectives:

- To establish and maintain an acceptable level of security (determined as an outcome of risk assessment of the company [see Section 3 and Appendix F]) throughout the life of the cryptographic system.
- To minimize, consistent with security policy, the burden imposed by key management on SCADA operations.
- To minimize the inconvenience and complexity imposed on the user.

4.4.2 External communication interfaces to the SCADA system

External communication interfaces to the SCADA system include those to a SCADA master in a control center[15]; to the SCADA system to and from business systems outside a control center; to a local SCADA master in a compressor station, an electric power substation, etc.; and to an RTU in a regulator station or outside the station (e.g., pole-top RTU).[16] The communication interfaces are typically serial asynchronous links operating over leased lines, dial-up lines, or radio links. There is a definite trend to use networked SCADA systems over intranets using IP. It is now recognized that any of these links are vulnerable to cyber attack. Mitigation of this threat, where it occurs, will require a combination of encryption and authentication hardware/software on each of the vulnerable interfaces.

4.4.2.1 Control center communication interface

A SCADA master in a control center (or its backup) represents a repository of data used by other control center business functions. Communication access to the SCADA master

---

[14]A comprehensive specification of the key management system will be published in AGA 12, Part 1, Addendum 1.

[15]There are at least two scenarios addressed by AGA 12, Part 1. First is the scenario that the backup control center is running in a shadow or hot mode. In this case, there is nothing special about switch-over. Second is the scenario that the backup control center is operating in a standby mode. In this case, when switch-over begins, there is nothing special about the CM requirements — they are the same as those for the primary control center CMs.

[16]AGA 12, Part 1 addresses common SCADA requirements for gas, electricity, water, wastewater and pipeline systems. The term station or substation, including its qualifier, is used generically to address all stations.

should be protected from cyber attack.

- If protection against cyber attack is provided for business functions that have access to the SCADA master, based on a risk assessment, a determination will be made as to whether cryptographic protection of this interface is required. If required, AGA 12, Part 1 requirements defined for the cryptographic system apply.
- CMs implemented on these communication interfaces should not degrade the functional or performance capability of the business function that has authority to access the SCADA master.

4.4.2.2 Local SCADA master communication interface

Local[17] SCADA masters in a substation represent a repository of data used by operational personnel to perform authorized tasks. Communication access to the local SCADA master should be protected from cyber attack.

- CMs implemented on these communication interfaces should not degrade the functional or performance capability of the operational function that has authority to access the local SCADA master.
- Local IEDs that communicate with a local SCADA master in general may not require cryptographic protection over this interface and, therefore, are outside the scope of AGA 12, Part 1.[18]

4.4.2.3 RTU communication interface

RTUs in a substation or external to a substation represent a repository of data used by operational personnel to perform authorized tasks. Communication access to RTUs should be protected from tampering.

- CMs implemented on these communication interfaces should not degrade the functional or performance capability of the operational function that has authority to access RTUs.
- Local IEDs that communicate with RTUs in general may not require cryptographic protection over this interface and, therefore, are outside the scope of AGA 12.[19]

4.4.3 Intrusion detection and forensics

AGA 12, Part 1 recommends that SCADA systems integrate and use an IDS to detect cyber attacks and record the information needed to prosecute the attacker.

A fundamental tool for intrusion detection is the audit record. AGA 12, Part 1 recommends either of two approaches to record the outgoing activity by users as input to the IDS:

---

[17]The qualifier “local” means inside the substation.

[18]Although outside the scope of AGA 12, Part 1, there may be special requirements in the AGA 12 series documents that require local SCADA master communication protection within a substation.

[19]Although outside the scope of AGA 12, Part 1, there may be special requirements in the AGA 12 series documents that require local RTU communication protection within a substation.

Native audit records: Virtually all multi-user operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.

Detection-specific audit records: A collection facility can be implemented that generates audit records containing only that information required by IDS. One advantage of such an approach is that it could be made vendor-independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

Procurement needs to incorporate the requirements derived from the utility's firewall filtering policy into the intrusion detection filters for operation's SCADA networks.

AGA 12, Part 1 recommends a "deny-everything-not-specifically-allowed" for this network. "Deny-everything" policy makes intrusion detection easier by setting an alarm for violations.

Corporate and manufacturer-provided IDS systems may not be able to detect intrusions against AGA 12-compliant security for SCADA communications. In such cases, AGA 12, Part 1 recommends using information recorded in AGA 12, Part 1's specified forensic counters to detect an intrusion or tampering.

5 Technical references (normative)

[1] DNP Technical Bulletin 2002-x, “Message Authentication Object.”

[2] IEEE Std 100™ “The Authoritative Dictionary of IEEE Standard Terms”, Seventh Edition.

[3] IEEE Std C37.115™-2003: “IEEE Standard Test Method for Use in the Evaluation of Message Communications Between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System.”

[4] IEEE Std1613™: “IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations.”

[5] IEEE Std 1646™-2004: “IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.”

[6] Internet Security Glossary (RFC 2828), “The Internet Society.”

[7] National Institute of Standards and Technology FIPS PUB 140-1, “Security Requirements for Cryptographic Modules.”

[8] National Institute of Standards and Technology FIPS PUB 140-2 “Security Requirements for Cryptographic Modules”

[9] National Institute of Standards and Technology FIPS PUB 180-2, “Secure Hash Standard.”

[10] National Institute of Standards and Technology FIPS PUB 197, “Advanced Encryption Standard.”

[11] National Institute of Standards and Technology SP 800-38A, “Recommendation for Block Cipher Modes of Operation.”

[12] American National Standards for Financial Services, ANSI X9.80-2001, “Prime Number Generation, Primality Testing, and Primality Certificates.”

Appendix A Bibliography (informative)

Appendix A includes an informative list of books and other documents that were used to develop AGA 12, Part 1 and a URL to web sites that provide information discussed in AGA 12, Part 1. Bibliography numbering is continuous over the two sub-sections.

A.1 Books

NIST's FIPS PUB 140-2 (Reference [8] in Section 5) provides detailed guidance on the requirements governmental agencies should impose on their cryptographic modules. Many private companies use the FIPS guidelines because the guidelines were developed by expert cryptographers and deemed adequate to protect federal information. That said, the following books offer additional insight into the requirements and rationale of the government specification.

[1] Cegrell, Torsten (1986) "Power System Control Technology," Prentice-Hall International (UK) Ltd.

[2] Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) "Handbook of Applied Cryptography," CRC Press. Note: Menezes, et al., provide a readable discussion on the details of many areas of cryptography and attacks, but this book also pre-dates the Advanced Encryption Standard (AES) specified in FIPS PUB 197.

[3] Schneier, Bruce (1999) "Applied Cryptography: Protocols, Algorithms & Source Code in C," Addison Wesley. Note: Schneier provides a readable, very detailed discussion of cryptography and protocols, but with little insight into how to deploy it in control systems.

[4] Smith, Richard E. (1997) "Internet Cryptography," Addison Wesley. Note: Smith provides a readable introduction to the subject of cryptography applied to the Internet, with examples of commercial deployment. Much of this discussion can be applied to control systems with some modification. Since this book predates AES, visiting the AES web site will provide more recent details.

[5] Stuart G. Stubblebine and Virgil D. Gligor. "On Message Integrity in Cryptographic Protocols," proceedings of the 1992 IEEE Symposium on Research in Security and Privacy, pp. 85-104, 1992.

A.2 Related standards

The following standards include useful information for understanding the requirements in AGA 12, Part 1, but they are not normative in the sense that they are incorporated in this practice. BS 7799-2 and ISO/IEC 17799 include extensive discussion on security practices that are summarized in AGA 12, Part 1.

[6] BS 7799-2: 2002, Information security management systems – specification with guidance for use.

[7] ISO/IEC 17799:2000, Information technology – Code of practice for

information security management.

[8] NIST Special Publication 800-38A: 2001 (expanded discussion on a recommendation for block cipher modes of operation)

A.3 Web sites

The following web sites are referenced in AGA 12, Part 1.

[9] AES home page: http://csrd.nist.gov/CryptoToolkit/aes/

[10] Example threats: www.tscm.com/outsideplant.html/

[11] NIST web site for public compliance verification: http://csrc.nist.gov/cryptval/

[12] NIST web site for cyber security documents: http://csrc.nist.gov/publications/

[13] National Security Agency web site for cyber security documents: www.nsa.gov/isso/

[14] Informational Technical Assurance Framework Forum for cyber security documents: www.iatf.net/

[15] The Committee on National Security Systems for cyber security documents: www.nstissc.gov

[16] Stream ciphers: www.disappearing-inc.com/S/streamciphers.html/

[17] AGA 12 web site: http://gtiservice.org/security/index.shtml

[18] U.S. Department of Energy, “21 Steps to Security”: www.ea.doe.gov/pdfs/21stepsbooklet.pdf

[19] American Petroleum Institute, API Publication 1164 (SCADA Security): www.api.org

[20] Instrumentation, Systems and Automation, ISA-TR99.00.01-2004: Security Technologies for Manufacturing and Control Systems: www.isa.org

[21] ISA-TR99.00.02-2004: Integrating Electronic Security into the Manufacturing and Control Systems Environment: www.isa.org

[22] Urgent Action Standard – 1200 Cyber Security: www.nerc.com/~filez/standards-cyber.html

Appendix B Definition of terms, acronyms and abbreviations (normative)

In Table B- 1 and Table B- 2, the numbers in brackets indicate the source from which a term or abbreviation was taken.

Sources for definitions:

[1] FIPS PUB 140-2, (2001), "Security Requirements for Cryptographic Modules, Section 2," Glossary of terms and acronyms, National Institute of Standards and Technology.

[2] IEEE 100™, "The Authoritative Dictionary of IEEE Standards Terms", 7th ed., Institute of Electrical and Electronics Engineers.

[3] DNP Technical Bulletin 2002-x, "Message Authentication Object."

[4] NIST SP 800-38A, "Recommendation for Block Cipher Modes of Operation."

[5] RFC 793, "Transmission Control Protocol," September 1981.

[6] RFC 2828, "Internet Security Glossary."

[7] Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997), "Handbook of Applied Cryptography," CRC Press.

[8] Schneier, Bruce: "Applied Cryptography," Second Edition, John Wiley & Sons, 1996.

[9] FIPS PUB 198, (2002), "The Keyed-Hash Message Authentication Code (HMAC)".

[10] FIPS PUB 200, (2005), "Minimum Security Requirements for Federal Information and Information Systems," Glossary of terms, National Institute of Standards and Technology.

B.1 Definition of terms

Table B- 1 Definition of Terms

Term	Definition
a priori	Latin phrase meaning "in advance;" "from something prior." Here it means the sender and recipient exchanged a common secret quantity (e.g., key) prior to exchanging encrypted messages.
Access control	The restriction of entry or use, to all or part of, any physical, functional, or logical unit.
Accountability	A property that ensures that the actions of an entity may be traced uniquely to that entity.
AGA 12 series	A series of specifications and practices published by the American Gas Association, which comprise a series of documents. AGA 12, Part 1 includes background information, general security policies, and the cryptographic system test plan. AGA 12, Part 2 includes requirements to retrofit existing asynchronous serial communications. AGA 12, Part 3 and subsequent documents will

Term	Definition
	address other configurations.
Approved	FIPS-approved and/or NIST-recommended. [1]
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. [1]
Authentication	A process that establishes the origin of information, or validates an entity's identity[20].
Authentication code	A cryptographic checksum based on an approved security function (also known as a "message authentication code"). [1]
Authorization	The right or a permission that is granted to a system entity to access a system resource.
Availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
b-bits	block of length 'b' bits
Backup	A copy of information to facilitate recovery, if necessary.
Bandwidth	The rate at which a data path (e.g., a channel) carries data, measured in bits per second.
Block	A group of contiguous characters formed for transmission purposes.
Broadcast mode	Concurrent transfer mode of information to all connected receivers with one message from the information source. Contrast: unicast and multicast modes.
Can	The word "can," equivalent to "is able to," is used to indicate possibility and capability, whether material or physical.

[20]The AGA 12 Task Group found that "authentication" has two distinct meanings. One is authentication of one CM to another, simply establishing that the module is talking to the module to which it believes it is talking. The other meaning of authentication is establishing that the CM indeed is really associated with domain (i.e., user defined name) identity with which it is claimed to be associated.

Term	Definition
Certificate	See “public key certificate.”
Certificate authority	The entity in a PKI that is responsible for issuing certificates and exacting compliance to a PKI policy.
Cipher Block Chaining (CBC)	An encryption mode in which the plaintext of the current block is XORed with the previous ciphertext block before it is encrypted. [8]
Ciphertext	Data in its encrypted form.
Ciphertext port	The CM communication port connected to a protected communication link. Communication on this port may be in plaintext or ciphertext.
Cleartext	Unencrypted data without format additions or changes, such as framing or padding.
Client	A device or program requesting a service.
Closed session	The session has been terminated and a new key is required for the next session.
Commissioning	The process of installing cryptographic protection on a system or portion of a system that has not been previously protected by cryptography.
Compromise	The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). [1]
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Control information	Information that is entered into a cryptographic module for the purposes of directing the operation of the module. [1]
Counter (CTR)	An encryption mode, in which a set of input blocks, called counters, is fed to the cipher to produce a sequence of output blocks that are XORed with the plaintext to produce the ciphertext.
Critical Security Parameter (CSP)	Security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module. [1]
Cryptographic boundary	An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module. [1]

Term	Definition
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. [1]
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 that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. [1]
Cryptographic module security policy	A precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor. [1]
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. [7]
Cryptoperiod	The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.
Cryptosystem	A collective of keys, algorithms, hardware, software and security policies that are employed to provide cryptographic services to an organization.
Cyber attack	Exploitation of the software vulnerabilities of information technology-based control components.
Cyclic Redundancy Check (CRC)	A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service when accidental changes to data are expected. Sometimes called “cyclic redundancy code.”
Decryption	The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
Denial-of-Service (DoS)	The prevention of authorized access to a system resource or the delaying of system operations and functions. (See “interruption.”)
Digital signature	The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation. [1]

Term	Definition
Electronic codebook (ECB)	A block cipher mode in which a plaintext block is used directly as input to the encryption algorithm and the resultant output block is used directly as ciphertext.
Emulate	To represent a system by a model that accepts the same inputs and produces the same outputs as the system represented. For example, to emulate an 8-bit computer with a 32-bit computer.
Encryption	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. [6]
Encryption appliance	Network-attached devices that offload encryption from a computer’s CPU and main memory. Examples of encryption appliances are a communication channel encryptor for serial communications, a VPN gateway, or an SSL accelerator or gateway.
Entity	An individual, organization, device or process.
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. [1]
Hardware	The physical equipment within the cryptographic boundary used to process programs and data. [1]
Hardware Security Module (HSM)	A special CM used to generate and store key materials and is part (or, in some cases, all) of a key escrow system.
Hash function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: It is computationally infeasible to find any input that map to any pre-specified output, and It is computationally infeasible to find any two distinct inputs that map to the same output.
Informative	Information included that makes the content easier to understand.
Initialization Vector (IV)	A vector used in defining the starting point of an encryption process within a cryptographic algorithm. [1]
Input data	Information that is entered into a cryptographic module for the purposes of transformation or computation using an approved security function. [1]
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. [1]

Term	Definition
Intelligent Electronic Device (IED)	Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers).
Interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. [1]
Interruption	Degrading or destroying the communication links or device using message flooding, generation of invalid messages, or physical attacks on the communication system. Most commonly known as DoS or DDoS if multiple attackers are involved.
Key [alpha order: put all words beginning with "key" together, alphabetized according to second word]	See "cryptographic key."
Key component	See "cryptographic key component."
Key confirmation	A process used to validate the accuracy and authenticity of a parameter used in the encryption or decryption function.
Key escrow system	Software, devices, and procedures used to generate, store, and retrieve securely cryptographic keys and key materials for the purposes of installation, maintenance, and backup.
Key establishment	The process by which cryptographic keys are distributed securely among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [1]
Key management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [1]
Key pair	A public key and its corresponding private key. A key pair is used with a public key algorithm.
Keyed-Hash Message Authentication Code (HMAC)	A mechanism for message authentication using cryptographic hash functions, in combination with a shared secret key. [4]
Keying material	A string of numbers and/or characters, identically having a high degree of randomness or unpredictability, used to carry out an agreed upon logical function.

Term	Definition
Latency	The time it takes for a packet of data to cross a network connection, from sender to receiver.
Local	Inside the substation.
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. Remote access via dial-up phone lines requires an external or internal automatic answering modem.
Management port	The physical or virtual access mechanism (interface) on a cryptographic module through which configuration and cryptographic parameters may be set.
Master	A device that initiates communications requests to gather data or perform controls. [2]
Master key	See “cryptographic key component. “
May	The word “may,” equivalent to “is permitted,” is used to indicate a course of action permissible.
Message	An ordered series of characters used to convey information.
Message Authentication Code (MAC)	Data that is associated with authenticated information that allows an entity to verify the integrity of the information.
Modification	The alteration of data or information; in the adverse situation, the alteration results in a condition other than intended by the originator.
Multicast mode	Concurrent transfer mode of information to a predefined subset of all connected receivers with one message from the information source. Contrast: unicast and broadcast modes.
Multi-factor authentication	A mechanism that employs more than one means to validate the identity of an entity.
Must	The use of the word “must” is deprecated and shall not be used when stating mandatory requirements. The word “must” is used to describe unavoidable situations only.
n-bit	Quantity of length “n” bits
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.

Term	Definition
Normative	A specification of requirements that is mandatory for the product or system to claim compliance.
Operational use	A stage in the life cycle of keying material; a stage whereby keying material is used for standard cryptographic purposes.
Operator, cryptographic	An individual accessing a cryptographic module or a process operating on behalf of the individual, regardless of the assumed role. [1]
Operator, SCADA	An individual in the utility control center who is responsible for online SCADA system control.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [1]
Plaintext	Unencrypted data with format additions or changes, such as framing or padding.
Plaintext key	An unencrypted cryptographic key. [1]
Plaintext port	The cryptographic module communications port connected to a protected device. All communications on this port are in cleartext.
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). [1]
Private key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. [1]
Proof-of-Possession (PoP)	A verification process to prove that the owner of a key pair actually has the private key associated with the public key.
Public key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.) [1]
Public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys — a public key and a private key. The two keys have the property that deriving the private key from the public key is not computationally feasible. [1]
Public key certificate	A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. [1]
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates.

Term	Definition
Recommended	The word “recommended” is used to indicate flexibility of choice with a strong preference alternative.
Removable cover	A cover designed to permit physical access to the contents of a cryptographic module. [1]
Replay	Recording message traffic and “playing it back” to a device later in order to make it do what you want. [3]
Requests for Comments (RFC)	The RFC document series is a set of technical and organizational notes about the Internet, which discuss many aspects of computer networking, including protocols, procedures, programs, and concepts. The official specification documents of the Internet Protocol suite are recorded and published as standards track RFCs. The RFC publication process plays an important role in the Internet standards process.
Repudiation	The ability to deny that a transaction took place (e.g., an individual could claim “I never performed that action”). [3]
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [10]
Role	A set of transactions that a user or set of users can perform within the context of an organization.
RSA	The public key algorithm invented by Rivest, Shamir, and Adleman.
SCADA	See “supervisory control and data acquisition system.”
Secret key	A cryptographic parameter that is held private by one or more entities to limit the ability to communicate or access that group or entity.
Secure Hash Standard (SHS)	The U.S. government standard (FIPS PUB 180-2) that specifies four secure hash algorithms (SHA-1, SHA-256, SHA-384, and SHA-512) that produce a fixed-length hash result for input data of any length less than 2**64 bits (for SHA-1 and SHA-256) or 2**128 bits (for SHA-384 and SHA-512).
Security boundary	An explicitly defined continuous perimeter that establishes the physical or logical bounds of a security domain.
Security domain	A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (e.g., hierarchically) to form larger domains.
Security policy	See “Cryptographic module security policy.”

Term	Definition
Server	A device or computer system that is dedicated to providing specific facilities to other devices attached to the network.
Session	A period defined either by an amount of time, a number of messages, or a user-initiated change during which two CMs operate using specific parameters.
Session establishment key	Cryptographic value(s) used to set up the parameters that secure the communications between two devices or persons.
SHA-1, SHA-256, SHA-384, and SHA-512	See “Secure Hash Standard.”
Shall	Equivalent to “is required to,” and used to indicate mandatory requirements, strictly to be followed in order to conform to the system and from which no deviation is permitted.
Shared secret	A value that is generated during a key agreement process. The shared secret is typically used to derive keying material for a symmetric key algorithm.
Should	Equivalent to “is recommended that,” and used to indicate several possibilities recommended as particularly suitable, without mentioning or excluding other, that a certain course of action is preferred but not required or that (in the negative form) a certain course of action is deprecated but not prohibited.
Slave	A device that gathers data or performs control operations in response to requests from the master, and sends response messages in return. A slave device may also generate unsolicited responses.
Software	The programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be written dynamically and modified during execution. [1]
Split knowledge	A process by which a cryptographic key is divided into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key. [1]
Spoof	Pretending to be an authorized user. [3]
Status information	Information that is output from a cryptographic module for the purpose of indicating certain operational characteristics or states of the module.
Substation or station	The term, including its qualifier, is used to address generically all remote sites housing devices that control transmission and distribution of gas, electricity, water, wastewater, etc. Examples are electric power substations, pumping stations, compressor

Term	Definition
	stations, and gate stations.
Supervisory Control And Data Acquisition (SCADA) system	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.
Symmetric key	A single parameter is used to both encrypt and decrypt a message or object.
Synchronized sequence numbers (SYN)	Synchronized control flag in TCP header used to indicate the start of the process to establish a TCP connection; also refers to the message containing the set control flag. [5]
System software	The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs and data. [1]
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
Throughput	The total capability of equipment to process or transmit data during a specified time period.
Traffic analysis	Listening to messages, and without understanding their content, inferring information from the fact that certain messages are always sent when certain real-life events happen (e.g., closing a breaker). [3]
Trusted path	A communication link that has been certified to a specific level of security or risk avoidance.
Unauthorized disclosure	An event involving the exposure of information to entities not authorized to access the information.
User	An individual or process acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. [1]
User token	A hardware or software object consisting of an identity and, optionally, a set of associated privileges.

Term	Definition
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.
Zeroization	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of data. [1]

B.2 Definition of acronyms and abbreviations

Table B- 2 Definitions of Acronyms and Abbreviations

Acronym/Abbreviation	Definition
3DES	Triple Data Encryption Standard [1]
A/D	Analog/Digital (used in the context of analog to digital conversion)
AEP	Awareness Education Plan
AES	Advanced Encryption Standard (specified in FIPS PUB 197)
AGA	American Gas Association
ANSI	American National Standards Institute
API	Application Program Interface [1]
BCP	Business Continuity Plan
CAPI	Common Application Programming Interface
CBC	Cipher Block Chaining [4] [6]
CM	Cryptographic Module [1]
CMVP	Cryptographic Module Validation Program [1]
CPU	Computer Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CRM	Cryptographic Reference Model
CSP	Critical Security Parameter [1]
CSTP	Cryptographic System Test Plan
CTR	counter (as used in the block cipher function) [4]
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DES	Data Encryption Standard [1]
DiD	Defense-in-Depth

Acronym/Abbreviation	Definition
DNP	Distributed Network Protocol
DoC/NIST	U.S. Department of Commerce/National Institute of Standards and Technology
DOE	U.S. Department of Energy
DoS	Denial of Service
DUT	Device Under Test
ECB	Electronic codebook [4] [6]
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electronically Erasable Programmable Read-Only Memory [1]
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory [1]
FCC	Federal Communications Commission [1]
FEP	Front End Processor
FIPS	Federal Information Processing Standard [1]
FIPS PUB	FIPS Publication [1]
FLASH	Flash memory
GUI	Graphical User Interface
HAZOP	Hazardous Operations
HMAC	Keyed-Hashed Message Authentication Code [9]
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
I&A	Identification & Authentication
IDS	Intrusion Detection System
IEC	International Electro-technical Committee
IED	Intelligent Electronic Device [2]

Acronym/Abbreviation	Definition
IEEE	Institute of Electrical and Electronics Engineers, Inc.
InfoSec	Information Security (as used in the context of a InfoSec team)
IP	Internet Protocol
IRT	Incident Response Team
ISA-TR	Instrumentation, Systems, and Automation Society Technical Report
ISO	International Standards Organization
IT	Information Technology
IV	Initialization Vector [1]
KAT	Known Answer Test
key	Cryptographic key
key component	Cryptographic key component
LAN	Local Area Network
MAC	Message Authentication Code
MAS	Multiple Address System
MCM	Maintenance Cryptographic Module
MCT	Monte Carlo Tests
MPH	Messages Per Hour
NERC	North American Electric Reliability Council
NIST	National Institute of Standards and Technology [1]
NIST SP	National Institute of Standards and Technology Special Publication
NSA	National Security Agency
OCSP	Online Certificate Status Provider
OFB	Output Feedback (as used in the block cipher function)
PAA	Preliminary Action Audit

Acronym/Abbreviation	Definition
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PoP	Proof-of-Possession
PPP	Point-to-Point Protocol
PROM	Programmable Read-Only Memory [1]
PSTN	Public Switched Telephone Network
PT	Pre-Transmission (as used in communication channels)
PTA	Penetration Test Assessment
PUB	Publication
RBAC	Role-Based Access Control
RF	radiofrequency
RFC	Requests for Comments
ROM	Read-Only Memory [1]
RSA	Rivest, Shamir, and Adleman (a public key algorithm)
RST	Reset flag, TCP header
RTU	Remote Terminal Unit [2]
SAA	Security Architecture Analysis
SCA	Successive Compromise Analysis
SCADA	Supervisory Control And Data Acquisition System [2]
SCM	SCADA Cryptographic Module
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm

Acronym/Abbreviation	Definition
SHS	Secure Hash Standard
SSL	Secure Socket Layer
SUT	System Under Test
SYN	Synchronized sequence numbers [5]
TCP	Transport Communication Protocol
TLA	Three Layer Analysis
URL	Uniform Resource Locator [1]
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
XOR	Exclusive OR Operation

Appendix C SCADA fundamentals (informative)

Businesses always have been faced with the need to monitor and control continuous processes, both large and small. In most simple cases, this means the process is equipped with some kind of instrumentation for monitoring and some kind of actuating (executing) device for control. Using these tools, the local or remote operators can control the process for which they are responsible and keep it running 24 hours a day, seven days a week.

SCADA[21] systems were developed to reduce labor costs and permit system-wide monitoring and remote control from a central location. At each remote site, an RTU is connected by local wiring to the field devices to be controlled and monitored. The RTU also has a communication port, which is used to communicate with the control center over a communication link. The communication link can be dial-up phone, leased line, spread spectrum radio, etc., depending on cost, availability, and operating constraints. Using the communication links from the control center, an operator can monitor and control many field installations using SCADA.

SCADA systems have been in place since the 1930s. They have an operational life cycle on the order of 15 to 30 years. Most SCADA communications in this installed base operate at very low speeds — on the order of 300 to 9600 bits per second. SCADA equipment at the field sites has to operate with very high reliability in a hostile environment; e.g., extreme temperature ranges. These systems were designed and installed at a time when there was little concern about communication security.

The environmental characteristics of SCADA field sites (electric utility transmission and distribution substations, gas gate stations and pressure-reducing stations, pump stations, and pole-top field devices) are not addressed further in this appendix.

C.1 Characteristics of SCADA

SCADA functions include data acquisition, monitoring and event processing, control functions, disturbance data collection and analysis, and reports and calculations.[22] SCADA systems are implemented as distributed process control systems that operate on the order of seconds or 10's of seconds, depending on their primary role. Real-time control and protection of equipment at the remote site is a local requirement (and requires response in the order of milliseconds in some cases); it is not a SCADA requirement.

C.1.1 Data acquisition

The basic information with regard to gas, electricity, water, wastewater, pipeline transmission and distribution operations is collected by field instruments and control devices located at sites remote from the operator's control center. Data also may be

---

[21]Pronounced /SKAY da/

[22]The characteristics of SCADA are based on material presented in the book "Power System Control Technology" by Torsten Cegrell, 1986 Prentice-Hall International (UK) Ltd. The concepts presented have been modified to be applicable to gas, water, wastewater, and pipeline process control applications.

entered manually or calculated and are treated exactly like the automatically collected data. For instance, the operator can enter data from passive systems without data acquisition equipment after the data are received by telephone, fax, or some other device.

C.1.2 Status indications

The status of field devices, alarm signals, and other signals is represented by means of "status indication." These status indications are contact closings connected to digital input boards in the RTU. Normally, there are both single bit (1-bit) and double bit (2-bit) status indications. There may also be three-bit status indications in which the third bit indicates if there has been a fast CLOSED-OPEN-CLOSED sequence of status changes between the scans, such as with automatic reclosing of circuit breakers.

Status indications normally are transmitted from RTUs on the next status scan request. There is also a complete scan at start-up and restart of the control system. Some control systems have other scanning schemes in place.

C.1.3 Measured values

Measured values of various inputs are collected by the RTUs. Two types of values are normally collected:

- Analog values, transformed via an A/D converter to a binary format.
- Digitally coded values, also in binary format.

The binary formatted values are sent to the control center, usually on each scan of the RTU of analog inputs.

The values also need to be scaled into engineering format before being presented to an operator on a GUI or used in an application program. Scaling is generally linear, but sometimes nonlinear scaling is required. Scaling commonly is implemented as a function of the FEP at the control center. The FEP does the scaling as the values are received, and the scaled values then are stored in the database. In some systems, the values are scaled when they are retrieved from the database and not when they are stored.

Scanning of measured values is done either cyclically or on a report-by-exception basis, where individual dead-bands are set for each measuring point and transmission occurs when the value has changed more than the dead-band since the last report. The latter method typically is used to reduce communication channel loading. It also involves a cyclic scan at startup or restart.

Dead-bands can be stored centrally and transferred at start-up to the RTUs and when the operator or control system engineer changes them.

C.1.4 Monitoring and event reporting

Acquired process control data is monitored automatically to ensure that measured and calculated values lie within permissible limits. The measured values are monitored with regard to rate-of-change and for continuous trend monitoring. They also are recorded for post-fault analysis. Status indications are monitored with regard to changes and may be time tagged by the RTU if it contains an internal clock.

Monitoring these data may have various objectives and, of course, differs between different data. If the monitoring detects a violation of limits and changes of status indications, event processing reports such events to the operators.

C.1.5 Status monitoring

Each status indication is compared with the previous value stored in the database. An alarm is generated, and the attributes or properties of the alarm are sent as a message – a report – when the status changes. Usually, the status is monitored against a pre-set "normal" status, thus creating a normal/off-normal operational state of the device that can be presented to the operator. The reporting of status changes can be delayed by a number of seconds. This is useful for suppressing transient alarm signals and temporary intermediate positions of two-state devices.

In addition, special delaying schemes often are implemented to detect, for instance, automatic reclosure operations by combining electric circuit breaker changes and status signals for the automatic equipment itself. In the case of a successful reclosure of local automatic equipment, alarms are suppressed.

C.1.5.1 Limit-value monitoring

Each measured value often can be monitored against a set of limit values. Limits can be introduced on both sides of a typical, or reasonable, value. This value may correspond to the physical quantity or the normal zone of that physical value. Some possible reasons for their existence follow.

- Upper and lower reasonable limits are used for specifying a range within which a reasonable value should appear. If the limit is violated, there is a failure in the control system itself.
- Upper and lower alarm limits are used to specify operating limitations. Violation of an alarm limit normally results in an alarm message to the operator.
- Upper and lower warning limits are used to alert the operator, enabling intervention before an alarm limit is exceeded.
- Zero-value limit is used to specify a dead-band around the zero value. A value inside the zero dead-band can then be regarded as zero and does not make the violation subject to event processing.

There are various solutions for implementing limit-value monitoring. It can be implemented at the control center or remotely. The more advanced remote data collection schemes always use limit-value monitoring. When implemented in the control center, the monitoring usually is carried out in connection with updating values in the database.

The limit values are specified individually for each measuring point and can be changed by the operator at the GUI. When limit-value monitoring is performed remotely, the new limits are transferred to the RTU via the SCADA communication network.

C.1.5.2 Trend monitoring

There are many types of monitoring of trends in measured values. Some possibilities are:

- Rate-of-change detection for trend detection.
- Presentation of values in curve displays. This often is combined with some sort of algorithm for extrapolation; e.g., load forecasting and trends for levels of water reservoirs.

C.1.5.3 Data-quality analysis

All data collection and monitoring functions normally result in a set of status flags associated with the individual data. These flags constitute data-quality attributes associated with the individual data as it is presented to the operator. Some commonly used data-quality attributes are blocked for updating, blocked, substituted, manually entered, out of limit (reasonable/alarm/warning/zero), alarm state, and unacknowledged.

C.1.5.4 Alarm processing

At remote sites, automatic (not operator-initiated) changes may occur on critical pieces of equipment. These changes of state are detected by the master station during the next systems scan and are presented immediately to the operator as alarms on the GUI and logged with a time tag showing when the event occurred. In the case of a major disruption, many alarms may be generated in rapid sequence. The operator's GUI presents them all as alarms only. In some more advanced SCADA systems, alarm-processing software may be employed to establish the root cause of the incident.

C.1.6 Control functions

Control functions are grouped into four subclasses: individual device control, control messages to regulating equipment, sequential control schemes, and automatic control schemes.

C.1.6.1 Individual device control

"ON/OFF," "START/STOP" or "TRIP/CLOSE" commands are used to control simple on/off devices.

C.1.6.2 Messages to regulating equipment

Transmission of messages to regulating equipment represents a more advanced control function and is performed on an as-needed basis. Applications include RAISE/LOWER regulation and set-point adjustment.

As an example of "RAISE/LOWER" control, the operator selects the control point of a regulating valve controlled by an RTU and issues a single "RAISE" or "LOWER" command, which incrementally will raise or lower the flow. The operator observes the change of flow in the analog value and issues another command if additional change is needed.

In the case of set-point regulation, the operator sends a new set point to an RTU control function. The new value is checked against predetermined limits to prevent abnormal values from being entered. The RTU responds with the new set point, which it has implemented.

C.1.6.3 Sequential control schemes

Sequential control means that a series of correlated individual control commands are executed. Sequential control schemes permit a sequence of such control commands to be executed automatically in predefined order, including suitable logical checks and time delays. Typically, only one operator command is required to initiate the control sequence.

C.1.6.4 Automatic control schemes

Automatically initiated commands are represented by closed control loops.

C.2 SCADA communication systems

SCADA is implemented always as a distributed process control system. Data acquisition and control are performed by RTUs and by field devices that include functions for communication or signaling.

C.2.1 Dedicated communication channel configurations

Dedicated communication channel configurations may be implemented in any of several arrangements as shown in Figure C-1 through Figure C-4.

The equipment shown in the control center is a simple example. The operator and engineer displays are interfaced to a master station, that, in turn, is interfaced to an FEP, which is connected to communication modems – one for every dedicated communication channel. Some smaller control systems combine the FEP with the master station. Others incorporate the display system in workstations that include the master station and FEP functions.

The point-to-point configuration (Figure C-1) is functionally the simplest type; however, the method is rather expensive because a unique channel and separate communication equipment are necessary for each line. In a series configuration (Figure C-2), a number of RTUs or field devices share the same channel. This has an impact on the efficiency and complexity of SCADA operations. In the series star configuration (Figure C-3), several channels are concentrated on one RTU. In the multi-drop or party line configuration (Figure C-4), the control center master station is connected to more than one RTU by one common path. Figure C-4 also shows in the configuration that a multi-drop may include a splitter so that two or more RTUs can share a single modem.

These basic configurations can be combined into more complex communication networks. Beyond the basic components mentioned, it would be possible to use dedicated communication computers to handle communication exchange, message switching, buffering of messages, etc.

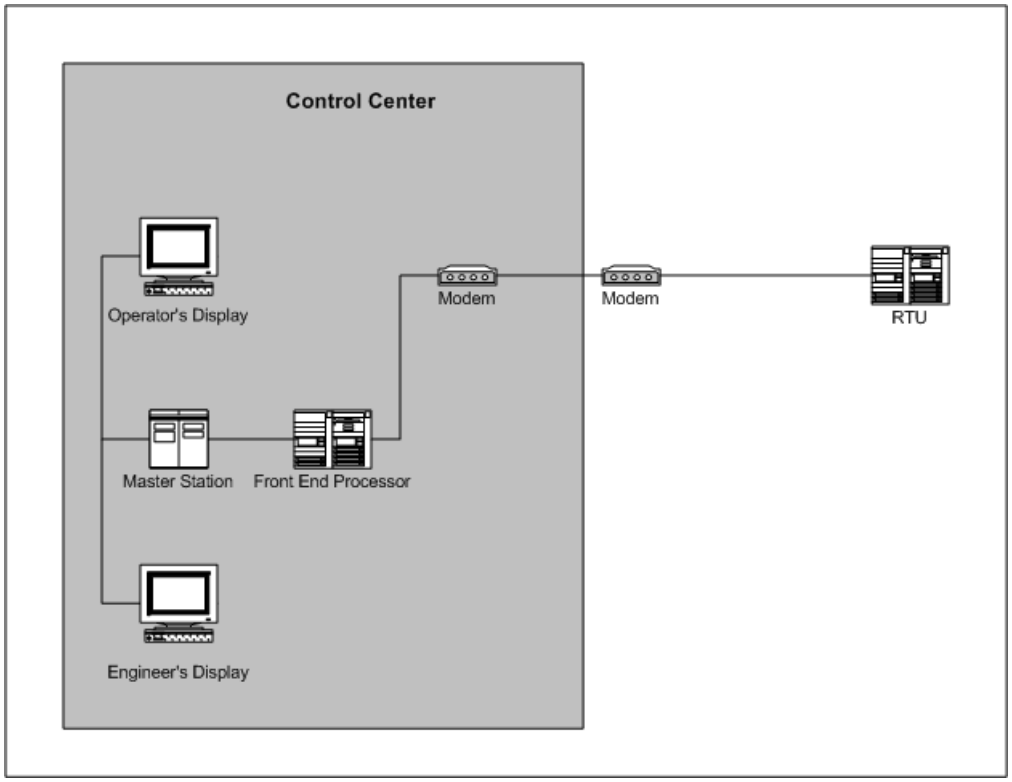


Figure C-1 SCADA system can be configured point-to-point

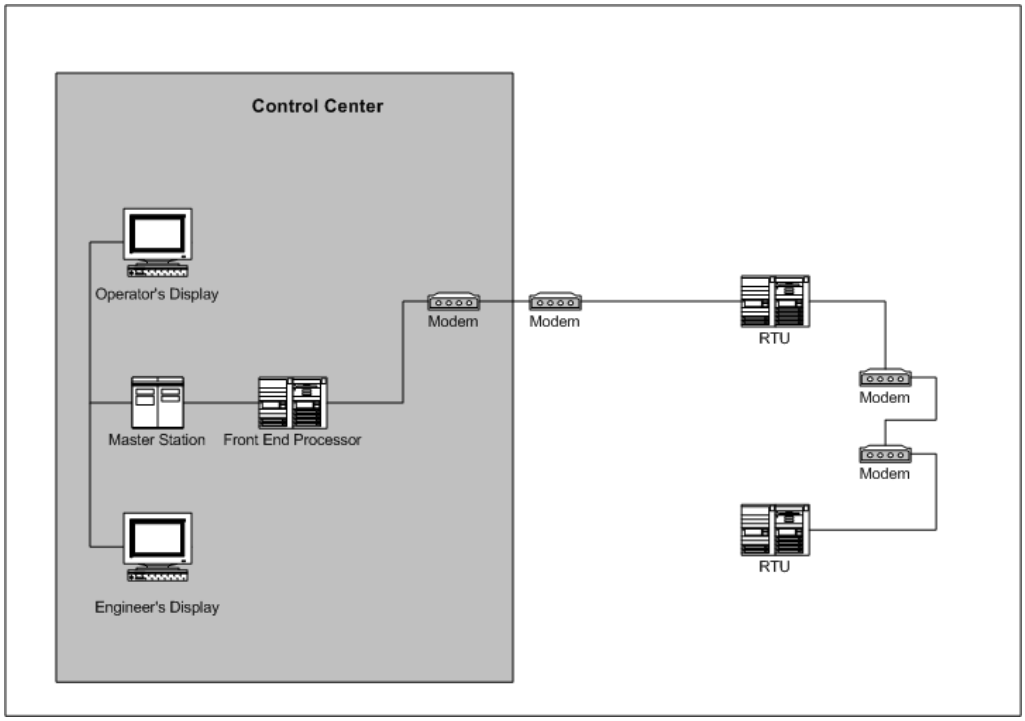


Figure C-2 SCADA system can include RTUs connected in series

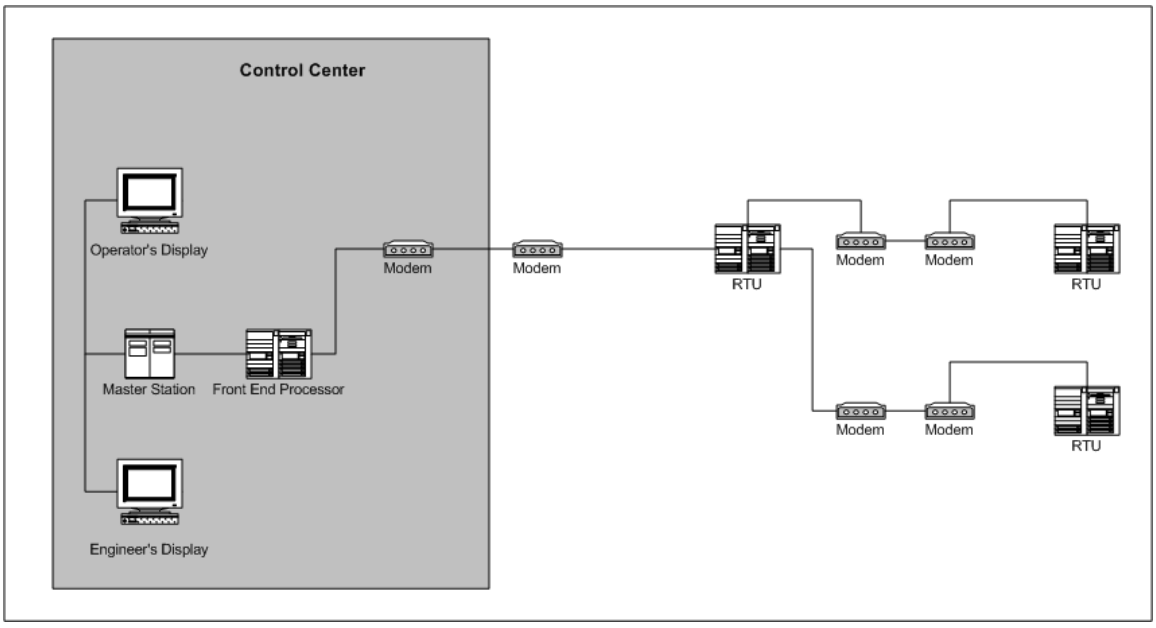


Figure C-3 SCADA systems can include RTUs connected in a series-star configuration

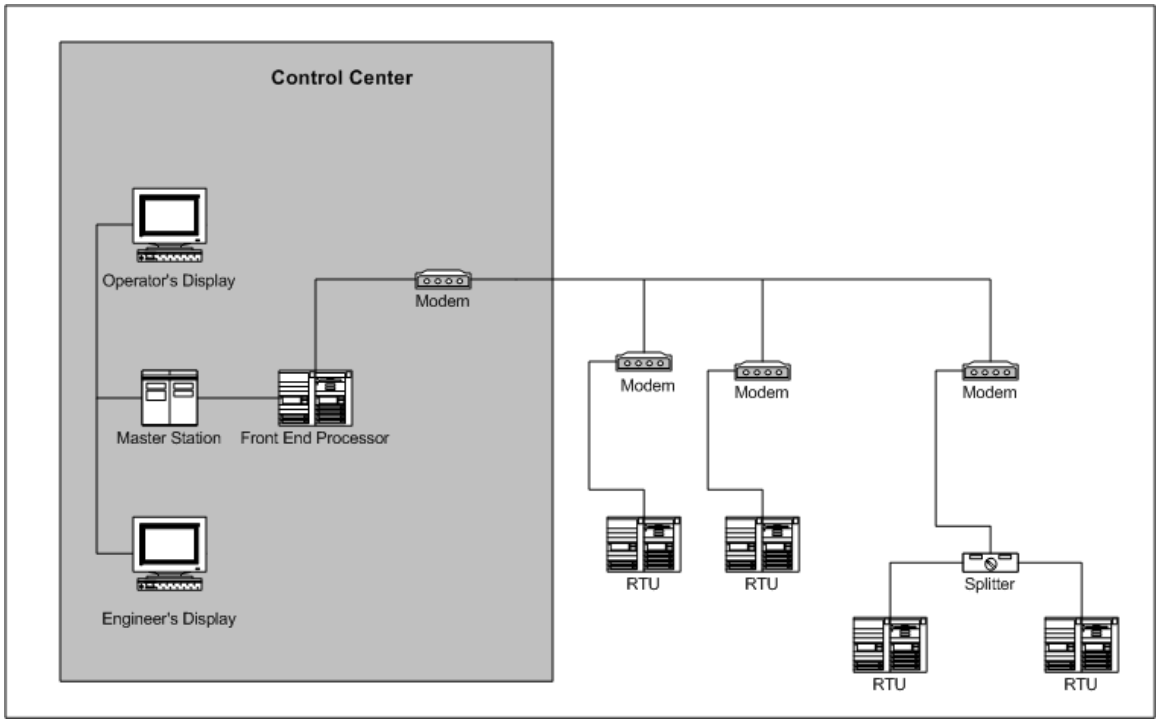


Figure C-4 SCADA system with RTUs in a multi-drop architecture

C.2.2 Native communication protocols

Different principles were described above to establish communication between two entities — a sender and a receiver of data. All these fundamentals are parts of rules, which make the two entities able to understand each other. A set of rules defining a communication procedure is called a “communication protocol.” Without a communication protocol, the two entities would not be able to understand each other; they would not agree on how to start and maintain a dialogue. A communication protocol defines, for example, the following.

- The structure of messages.
- Dialog rules and acknowledgement procedures.
- Establishment of error detection and correction.
- Recovery rules.

C.2.3 Communication links

A communication link connects two pieces of equipment that are going to communicate with each other. The link is the path for the movement of data. Typical communication links used for SCADA include leased lines, dial-up phone lines, Internet, radio, microwave, and satellite. Some SCADA systems provide broadcast or multicast capabilities and a few provide message store and forward capability.

Some SCADA systems use two or more communication links to provide backup communication should the primary link be compromised or fail. Some systems also use a backup control center. Should a problem develop with the primary control center, the “hot” backup can take over because it knows the status of the field equipment. If the backup control center is in the listen mode, it will have received and logged all of the messages sent in either direction. If it does not receive all of the messages, it should force a scan of all substations to update its database.

Figure C-5 shows some of the ways to communicate between equipment used to control gas or electricity transmission. Gas transmission RTUs are located in gate stations where gas pressure is reduced and gas is distributed to customers. In electricity systems, RTUs are located in transmission and distribution substations. Analogous systems can be described for water, wastewater, and other pipeline systems.

Figure C-5 shows that each control center can be configured so that FEP communication is through a modem or includes a WAN card if SCADA communication is over the enterprise WAN. A remote access computer can communicate over the enterprise WAN or over the PSTN using a dial-up modem.

RTUs and other IEDs may also include WAN cards for communications. If the PSTN is shared, each remote site needs an auto-answer modem and port switch[23] in order to communicate with the RTU or IED.

Figure C-5 shows sensors and actuators connected to RTUs. Although not shown, sensors and actuators also are connected to IEDs. Field data from sensors and actuators may transverse insecure channels and, consequently, cannot be trusted. Moreover, the integrity of controls to output devices cannot be guaranteed if those devices are connected by insecure channels or if there are unprotected back doors to

[23] A port switch is needed only if the port is shared.

those devices.

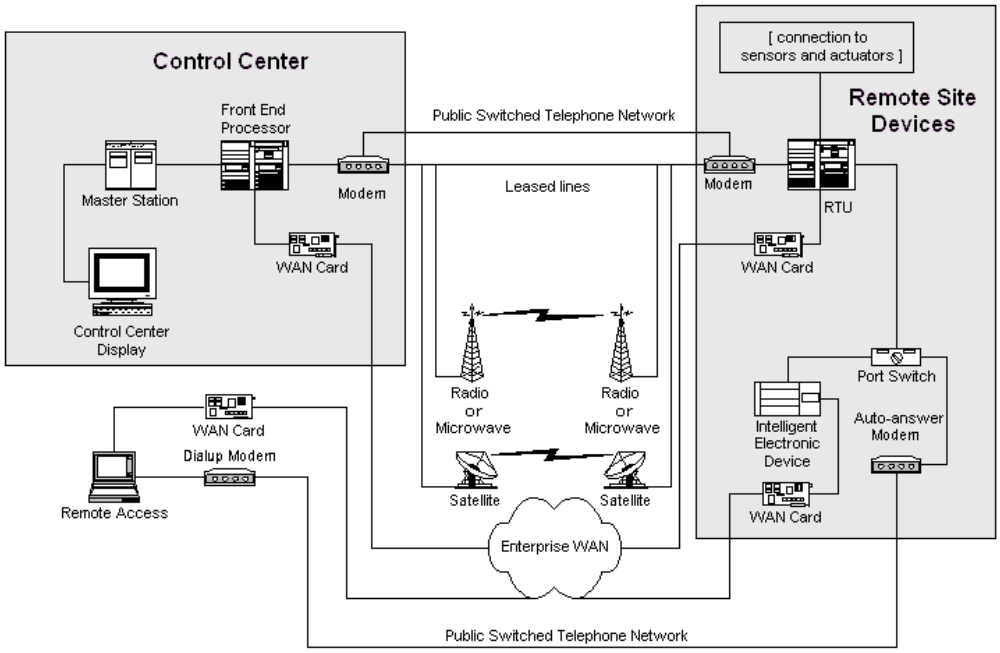


Figure C-5 Example of communication links

Appendix D Cryptography fundamentals (informative)

Cryptography is a science that is used to protect information. The most common meaning is privacy or confidentiality,[24] which ensures that unauthorized parties cannot read or understand the content of the information. Two additional requirements addressed by AGA 12, Part 1 are integrity, meaning the information has not been altered, and authentication, meaning the information was sent by the party that claims to have sent it.

Appendix D will familiarize the reader with some of the important terms and concepts of cryptography in general — symmetric or one-key cryptography, split key, and asymmetric key, which is the use of related key pairs. Symmetric cryptography is the classical genre of cryptography in which the sender and the recipient both have, *a priori*, a common secret quantity. This common secret can be a single value or a complex pool of numbers related to functions and ideas. It is the use of this *a priori* secret quantity in developing a secure functioning cryptographic system that is the focus of symmetric cryptography.[25] Asymmetric cryptography uses two mathematically paired keys; whatever one key encrypts the other key decrypts. Each class of cryptography (symmetric and asymmetric) has its strengths and weaknesses, which are addressed in the AGA 12 series to provide the best balance of protection, cost, and complexity.

D.1 First considerations

The use of cryptography (encryption) provides several benefits, but it is performed primarily for message confidentiality and authentication. Encryption provides message confidentiality by rendering information unreadable to anyone but the intended recipient(s). Authentication, as applied to people or devices, seeks to ensure that a message has been sent by a known party or device. Integrity checking also can be applied to the contents of a message in which encryption has been used to ensure that any alteration to the contents during transmission of the message can be detected.

Plaintext is text presumed understandable to anyone who should view it.[26] Encryption changes plaintext to ***ciphertext***, which is text that is not interpretable by any unauthorized person who should happen to see it. A cryptographic algorithm is the set of rules used to transform the plaintext into ciphertext.[27]

Consider for example a simple plaintext/ciphertext alphabet pair, where the string of

---

[24]Privacy refers to an individual's desire to limit the disclosure of information. Confidentiality refers to the condition in which information is shared or released in a controlled manner. Cryptography provides confidentiality that supports the privacy desired.

[25]Appendix D is based on the book "Cryptography Demystified" by John E. Hershey, McGraw-Hill TELECOM 2003. The basic terms and concepts described by Hershey have been tailored for AGA 12 application.

[26]A message containing a string of binary numbers (all ones and zeros) also is called plaintext.

[27]Many algorithms use a keying variable to establish how the plaintext is transformed into ciphertext.

characters “DOG” in plaintext is “GRJ” in ciphertext.[28] This particular *cryptographic algorithm* substitutes, letter-for-letter, an agreed-on ciphertext letter for each plaintext letter. In an elementary way, three ingredients one needs to operate a cryptographic system are the cryptographic algorithm, the keying variable, and the plaintext from the sender. With these three ingredients, it is possible to generate the ciphertext for the recipient. In theory, to decipher a secure system, one should know each of these three elements; although a standard assumption is that the adversary knows everything except the keying variable. However, don’t be complacent — keep in mind the following tenets:

- The fact that a cryptographic principle has a large number of keying variables does not guarantee that the cryptographic principle is a good choice for building a secure cryptographic system.
- The fact that a cryptographic principle is complex does not guarantee that the cryptographic principle is a good choice for building a cryptographic system.

D.2 Digitization of plaintext

The study of plaintext (the statistics, patterns, and other characteristics) is one of the most important considerations of cryptography. Appendix C describes a generic SCADA system and Appendix G maps the vulnerabilities of this SCADA system to the threats that can be addressed by a cryptographic system.

Simply put, SCADA systems run on bits, which in the native SCADA protocol are digitized into a stream of bits and, in some cases, the stream is grouped into bytes (8 bits per byte).

D.3 Conversion of plaintext to ciphertext — the keytext generator

Figure D-1 shows an example of a module that generates keytext (a stream of ones and zeros) that is XORed bit by bit to a stream of plaintext to form a stream of ciphertext. It is important that the key generator appear to have no memory; that is, the output at any time should appear to be independent of what has preceded it. If this independence is lacking, the preceding keytext bits might help predict the current keytext bits.

[28]This is commonly known as the “Caesar Cipher” or an extension of the Caesar Cipher, which is discussed at length by Hershey.

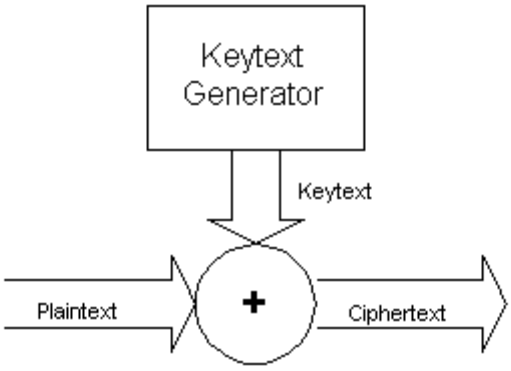


Figure D-1 Conversion of plaintext to ciphertext

There are two extremely important considerations. First, the same keytext should never be used to encipher two different plaintexts. If this is done, a classic and serious cryptographic error occurs, which is called a “problem of depth” in the literature. The second consideration is that an inquiry should be made into the quality of the randomness of the keytext. Are ones and zeros equally probable or is the distribution biased?

There are other requirements, however, for a cryptographic system that uses a keytext generator and is operated in a potentially hostile environment.

D.3.1 The secret keying variable

The cryptographic system should provide security even under the assumption that its design is known.

This is required because the security of the cryptographic system should not rest solely with its design, because eventually the design will become known. The security, therefore, depends on something else — a key or keying variable that is easily changed. The key is a secret quantity that is inserted into a publicly known cryptographic system that configures or sets the cryptographic keytext generator in a unique state. This state presumably is not known to any parties except those possessing the secret.

D.3.2 Matched plaintext and ciphertext will not compromise the keying variable

The cryptographic system should provide security under the assumption that the opposition may amass as much matched plaintext and ciphertext as desired.

This can be stated in a number of equivalent ways. One way is to say that the prediction of the keytext bit at any given time is not aided by the knowledge of the keytext bits preceding it. Another way is to say that the matched plaintext and ciphertext do not affect the security of the secret keying variable generation process.

D.4 Block cipher function — modern keystone

Modern one-key commercial cryptography is built around a component called the “block

cipher function."[29] The block cipher function is endorsed by the U.S. Department of Commerce's National Bureau of Standards, which defined the DES, published as FIPS PUB number 46 in 1977. A more robust extension of DES was published as 3DES. In 2001, FIPS PUB 197, "AES" was published. AES uses, at minimum a 128 bit keying variable and is AGA 12, Part 1's algorithm of choice.

Four confidentiality modes are described: electronic codebook mode, counter mode, output feedback mode, and cipher block chaining mode.

D.4.1 Electronic codebook mode

The simplest, most basic method for operating the block cipher function is the ECB mode. This mode uses the block cipher function to encrypt or decrypt a b-bit input block under the control of a secret keying variable. ECB mode is one of only two modes that use the block cipher function in the decrypt mode for decryption. In ECB mode, the same b-bit input block yields the same b-bit output block for the same keying variable. As such, ECB mode is not a suitable confidentiality mode for the encryption of most SCADA message traffic. However, the mode is well-suited for encrypting secret keying variables or other cryptographic variables that should be transmitted securely.

ECB mode also may be useful for key updating. Key updating is a technique in which a keying variable is operated using a one-way function to refresh the pool of variables used in the computation and to avoid the risk of collecting data strings that might repeat.

D.4.2 Counter mode

The CTR mode is essentially a coupling of a counter or other suitable finite-state sequential machine with the ECB mode. In the CTR mode, the cipher function is operated in the encrypt mode and its input block is filled with a setting that is changed successively. In the case of a counter, the setting is simply incremented. As long as the same setting is not used twice, the keytext generated by the block cipher function will not repeat and cause a depth situation. It's important to realize that anything that can be done to reduce the predictability, or the ability to determine a likely value or even a range of values, should be attempted.

D.4.3 Output feedback mode

The OFB mode uses the block cipher function operating in the encrypt mode, and its starting point is determined by a b-bit IV that is loaded into the block cipher function's input register before encryption is initiated. The b-bits produced by the first encryption and delivered to the output block are used as keytext and the next contents of the input register. Therefore, the encryption proceeds, using the output block contents as keytext and IV for the next cycle. This vector value also is referred to as "salt."

D.4.4 Cipher block chaining

CBC is an encryption mode that XORs the plaintext block with the previous ciphertext block before using the block cipher function. For the first block, the IV value is used during the first XOR. With the requirement that the IV be unique, repeating the same plaintext input results in different ciphertext outputs.

---

[29] See NIST Special Publication 800-38A 2001 Edition for an expanded discussion on a recommendation for block cipher modes of operation.

D.5 Hashing to achieve integrity

Hashing is the process of converting a variable length message into a fixed length representation of the original message, called a “message digest.” Hashing functions use a mathematical algorithm that statistically guarantees that no two messages will result in the same message digest unless the two messages are identical. Hashing is used to guarantee the integrity of the message.

When a message is created, both the message and its message digest are sent to the recipient. Upon receiving the message, the recipient hashes the messages to create another message digest. The two message digests then are compared, and if they are identical, it provides a very high probability that the original message was not altered.

D.6 Methods to achieve authentication

The most basic form of cryptographic message authentication combines a hashing function with a pre-shared secret value or code. This form of authentication, depending on the implementation, is known as a MAC. This process also may be used as part of challenge/response process. A more advanced form of authentication combines hashing, encryption, and a private key value (as in a public/private key pair) that is known as “digital signing” (see Section D.7.2).

D.7 Cryptographic keys and systems

The difference between symmetric and asymmetric keys is due to the algorithms that use them.

- For equivalent cryptographic strength, symmetric keys are shorter than asymmetric keys.
- Symmetric keys are easier to create than asymmetric keys; symmetric keys usually need to meet randomness requirements only (if there are no known weak keys), whereas asymmetric keys are evaluated further after generation; e.g., by prime number tests.
- Symmetric algorithms are generally faster that asymmetric algorithms.
- A symmetric cryptosystem requires that the secret key be shared securely between authorized users before it can be used; e.g., usually by a trusted third party.
- An asymmetric cryptosystem requires either the ability to transfer the public key (e.g., as part of the communication setup) or the distribution of public keys by a trusted third party.
- Symmetric keys can be used to authenticate messages or as part of a challenge/response method by producing message authentication codes (e.g., keyed-HMAC).
- Symmetric keys cannot be used to provide unique authentication of a key holder.
- Asymmetric keys can be used to authenticate messages or as part of a challenge/response method by encrypting the private key; decryption with the public key confirms that the sender possesses the private key and produced the encrypted message.

- Most important, asymmetric keys can be used to provide unique authentication of a key holder, given that only one entity holds the private key.
- Asymmetric cryptosystems can be used to recognize unknown entities through a certification by a trusted third party.

One of the most well-known examples of how the two classes of cryptography are used together is SSL, which is an Internet protocol for establishing and conducting a secured session between a client computer and a web server. SSL uses a form of asymmetric cryptography called “public key cryptography” to identify the server (and sometimes the client) and to establish a secure session by sharing a symmetric key between the two computers. Once the symmetric key has been shared, SSL uses symmetric cryptography to encrypt the actual session.

Generally, cryptographic keys are used in one of the two cryptographic functions: encryption or digital signing. The same key should never be used for both functions.

D.7.1 Use of cryptographic keys for encryption

Encryption keys may be subdivided by their life expectancy.

D.7.1.1 Long-lived keys

Encryption keys used to protect data at rest have an additional characteristic of needing access over time. This can be accomplished in several ways. One method is by the secure storage of the keys or key fragments used to generate access to a given data object. This is simple in theory, but difficult in practice. The sheer volume of keys is one constraint and the protection of that volume also is difficult. A second mechanism is called “constructive key” and is described in ANSI X9.69 [12]. This process constructs the key at a point of origin and does not require the continued archiving of individual keys. Instead, this process leaves a series of instructions for the re-creation of the key. There are several methodologies available, all of which result in the 100-percent recoverability of the data by the system owner.

The simple creation of a unique key for each unique object can be difficult because if an individual encryption key, not supported by a recovery system, is lost or damaged, any data that was encrypted with it could be lost forever. For this reason, long-lived encryption keys need to be protected and managed to mitigate the possibility of data loss and, at the same time, have the ability to refresh or rekey the cryptographic system over time.

This is accomplished typically by establishing procedures for requesting and securely escrowing long-lived encryption keys or the key fragments in split key systems. If a key is lost or compromised (unauthorized disclosure), procedures should be in place to provide the authorized user with a copy of the original key or, if applicable, a new key. This way data can be decrypted and re-encrypted, or in the case of constructive key, the key pool can be updated.

D.7.1.2 Short-lived keys

Encryption keys used for short-lived or transient data, such as SSL sessions, link encryption, or VPN tunneling, typically are referred to as “session keys.” Session keys are created as needed, typically by automated processes. Once the transient data reaches its final destination or a session closes, session keys usually are destroyed, and there is no need to escrow the session keys.

D.7.2 Use of cryptographic keys for digital signing

Digital signing keys are used to generate digital signatures, which are used to verify authenticity of the sender of data, as well as to verify the integrity of the data object. The ability to use digital signatures for authentication can be compromised by the existence of a backup private key or multiple copies (one at home and another at work), and by exposure of a private key to malicious software. This also is why a signature key should not be used for encryption.

Data objects may be signed digitally by encrypting the data object's message digest with the private key and appending the encrypted digest and the sender's digital certificate to the data object. Digitally signed objects may be verified by decrypting the data object's message digest with the sender's public key, then comparing the decrypted message digest to a computed message digest of the data object. If the two message digests match, it proves the data object's integrity, and it proves the sender encrypted the original message digest with a private key that is related mathematically to the sender's public key. This process also is known as "proof-of-use" of the private key. "Proof of possession," which is equally important, is another matter entirely and may involve hardware tokens and liability agreements.

D.7.3 Use of digital certificates

Digital certificates are special-purpose data objects, or files, that link an identity to a public key. Digital certificates are used to identify an individual or a resource, such as a web server, a SCADA device, and other non-SCADA IEDs. A trusted third party, called a CA, digitally signs digital certificates. CAs may exist within a company or department, and they also are available publicly through a licensed trusted third party or a government agency, for example. CAs are responsible for verifying the identity of the certificate holder before the certificate is created. Once the certificate is created, CAs provide status information about the certificate, typically by posting on the Internet a CRL or providing an online service such as an OCSP on the Internet to indicate if the certificate is valid or has been revoked.

D.8 Cryptographic algorithms

Algorithms are mathematical formulas or processes used to perform a given task. In cryptography, there are a number of algorithm types, including those that perform encryption and decryption, integrity validation, authentication, key generation, and key exchange. Algorithms should be tested and validated by the cryptographic community to ensure that they function as advertised and do not contain any flaws or backdoors that would allow an attacker to defeat the algorithm's stated capabilities. Any algorithm that has not undergone a public peer review has a lower probability of success.

D.9 Cryptographic hardware

The integrity of a cryptosystem relies on the secrecy of the cryptographic keys. If keys are not protected, they may be exposed to malicious use possibly resulting in the compromise of sensitive information or the forgery of high-value transactions. Two of the most common operational security breaches in cryptosystems involve storing cryptographic keys on computer disks and permitting algorithms to execute in a computer's main memory, both of which expose the keys.

Cryptographic hardware is designed to protect or enhance a cryptosystem by providing a

cryptographic boundary around a key generation engine and a key storage area, or by offloading algorithm execution from the computer program unit and main memory. Examples of cryptographic hardware follow.

- HSM used by server-class computers to provide secure key generation, temporary key storage, digital signing, and encryption (link encryption, key encryption, and key exchange). HSMs are implemented on PCI and PCMCIA cards, SCSI-attached devices, and network-attached devices.
- Encryption appliances are network-attached devices that offload encryption from a computer's CPU and main memory. Examples of encryption appliances are a communication channel encryptor for serial communications, a VPN gateway and an SSL accelerator or gateway.
- Cryptographic user tokens provide secure cryptographic services for key generation, key portability, digital certificate portability, and on-board digital signing and encryption. User tokens are implemented on PCMCIA cards, smart cards, USB tokens, and Firewire tokens.

D.9.1 User token — the emerging technology

A security token is a software/hardware object consisting of an identity, and it may include an associated set of privileges. It is the basic mechanism for implementing security models.

A way to authenticate users is to provide them with hardware security tokens that contain the secrets required for authentication. Smart cards (and to a lesser extent, USB tokens) are an emerging authentication technology for large companies that require users to present a physical object (hardware token) that contains their identities and a PIN, creating two-factor authentication.

One of the key problems with user-name identification and password credentials is that the human factor threatens the overall security of such a solution. Passwords are easy to guess if users select simple passwords and easy to steal if users write them down. Moreover, users may share passwords for convenience or may simply forget complicated passwords. The authorized owner of these credentials may not know that his credentials have been stolen and misused unless the malicious user employs them to alter existing information. If stolen credentials are used solely for read-only or copy/extract operations, it might never be noticed.

Using a physical token provides two advantages: the secure storage and transportation of credentials and other secrets, and a way to ensure the uniqueness of that information. However, access to these credentials still requires a password or PIN, so the human factor still exists. The only difference is that it is more difficult to steal the information because the authorized user possesses both the physical token and the password. While password theft might never be noticed, token theft is discovered earlier because the token is in the physical possession of the authorized user who wishes to log on to the system.

D.9.2 Desirable features in cryptographic hardware

Examples of specific features that are desirable in cryptographic hardware are:

- Cryptographic-quality key generation using a FIPS-approved random number generator to produce key components and seed values, and the use of high-order prime numbers for the generation of RSA-based digital signing key pairs.

- For cryptographic user tokens applied to encryption appliances, the cryptographic hardware should never allow the private keys to be exposed outside of the device's secured boundary. For HSMs, private keys should never be exposed outside of the device's cryptographic boundary in plaintext.
- For cryptographic user tokens and encryption appliances, the cryptographic hardware should provide as a minimum a tamper-evident physical enclosure that complies with FIPS PUBs 140-1 or 140-2 Level 2. For HSMs, the cryptographic hardware should provide as a minimum FIPS PUBs 140-1 or 140-2 Level 3 tamper-active protective cryptographic boundary.
- For HSMs and encryption appliances, the cryptographic hardware should provide a clearly defined trusted path for loading keys.
- For HSM and cryptographic user tokens, the cryptographic hardware should use industry-compliant cryptographic APIs (such as CAPI and PKCS), for use with standard computer operating systems and Internet protocol.

Appendix E Challenges in applying cryptography to SCADA communications (informative)

Several challenges arise in designing a cryptographic protocol to protect SCADA communications that are unique to this context. This appendix discusses a number of these challenges:

- Encrypting repetitive messages.
- Minimizing delays due to cryptographic protection.
- Ensuring integrity with minimal latency.
- Accommodating various SCADA poll and retry strategies.
- Avoiding communication channel collisions.
- Supporting mixed-mode deployments.
- Supporting broadcast messages.
- Incorporating key management.

E.1 Encryption of repetitive messages

SCADA communication is of a repetitive nature. For many systems, the same status request results in the same or very similar responses. Information can be gained by tracking the status reports from field equipment. Even if the SCADA protocol is unknown, the appearance of a message significantly different from the majority of messages can indicate an alteration of the status quo or perhaps the heightened status of the message content. The selection of an encryption algorithm and mode of operation needs to take into account that there will be many repetitive messages with different messages interspersed occasionally. Specifically, each encrypted message needs to appear different, even though the underlying cleartext message may be the same or, alternatively, each message should look the same regardless of content. This can be achieved, for example, by padding and/or framing.

E.2 Minimizing delays due to cryptographic protection

Many messages sent by one SCADA unit (e.g., the host) are received at the same time via direct connections, such as leased lines. Time limits enable recovery from incomplete messages; for example, if a message was not completely sent, the timeout permits the SCADA unit once again to be ready for an incoming message. Longer timeouts are used by the host to recognize when a remote unit has had “enough” time to respond and the host should stop waiting for a response. When cryptographically protecting the SCADA message, the message is transferred to the CM, encrypted, transmitted to the remote CM, decrypted, and then transmitted to the receiving SCADA unit. This process of encrypting and decrypting SCADA messages adds to the amount of time required to receive a sent message. The cryptographic protection implementation strategy selected should minimize the time added (or “latency”) to the transmission of a SCADA message.

E.3 Assuring integrity with minimal latency

A significant security property for SCADA communication is data integrity, or simply

integrity. Integrity for SCADA communication refers to the assurance that an adversary cannot modify SCADA commands or responses, insert new commands or responses, and destroy commands or responses without detection. The primary challenge in protecting SCADA communication over slow communication links, such as serial lines, is how to assure integrity while minimizing additional latency and communications overhead that can be introduced by a security protocol.

Most SCADA protocols use a 16- or 32-bit CRC at the end of a message to detect communication channel errors. CRCs provide good detection of the burst errors caused by environmental interference that are typical of serial lines. If CRCs were used to verify encrypted messages (transmitted unencrypted and appended to the encrypted data), an attacker easily could calculate new CRCs. If CRCs are calculated for the original message, as is the SCADA message CRC, they offer very little protection against malicious modifications made by an adversary when stream ciphers are used. First, if the adversary knows or can guess the plaintext, it can compute the CRC because it is a deterministic function of the plaintext alone. Second, CRCs are linear; that is, the bit difference between the CRCs of two messages depends only on the bit difference between the two messages.[30] Thus, an adversary who can modify a part of the ciphertext of a message can calculate the corresponding change needed to the ciphertext of the CRC to make the underlying CRC appear to be valid for the modified message. These illustrated weaknesses of CRCs suggest that a solution to protect SCADA communication should not rely entirely on the CRC for integrity.

It should be noted that CRCs encrypted by a block cipher are more resistant to direct modification than they would be by any NIST-approved stream cipher. This is because when block ciphers encrypt a message, they change the location of bits (technically, “diffuse”) within the encrypted block, making it more difficult to alter the message. However, they afford no more security than a randomly generated value; i.e., a possibility of $1/2^n$ of a correct CRC value occurring for an n-bit CRC.

The problem of assuring integrity while minimizing latency can be broken down into two sub-problems: intra-message integrity and inter-message integrity. Intra-message integrity, or simply message integrity, refers to ensuring that a particular SCADA message cannot be modified or forged without detection. Inter-message integrity refers to ensuring that messages are not reordered or replayed.

E.3.1 Intra-message integrity

A proven cryptographic mechanism used to validate the integrity of a message is a MAC. A MAC is a short signature of both the contents of the message and the value of a key, with the property that any change in the message or key, no matter how slight, will result with very high probability in a different signature. To use a MAC, the sender and receiver must share a secret MAC key. The sender appends to the message the MAC of the message computed with this key. The receiver computes a MAC of the received message with the same key and compares the computed value with that received with the message. If the two match, the receiver concludes the message’s integrity has been preserved. Since any change in the message should result in different MAC, an adversary cannot modify the transmitted MAC to match modifications to the message

[30] Stuart G. Stubblebine and Virgil D. Gligor, “On Message Integrity in Cryptographic Protocols,” published in the Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy, pp. 85-104, 1992.

without knowing the key.

Using a MAC to check integrity requires the receiver of a message to buffer the entire message (an operation called “full holdback”) until both the message and transmitted MAC have been received, a MAC of the received message has been computed, and that computed MAC has been compared against the received MAC. When the comparison is completed successfully, only then can the receiver be assured of the integrity of the received message.

In the context of a “bump-in-the-wire” retrofit CM, using a MAC to protect a SCADA message would require the CM receiving the protected message to buffer the entire message and verify its MAC before forwarding the underlying SCADA message to the receiving SCADA unit. Buffering the message would introduce additional latency that depends on the length of the message, since it would take as long to forward the message over the CM-to-SCADA communication link as it did to receive it over the CM-to-CM communication link. Since this could double the communication latency between the two SCADA units, using a MAC on every SCADA message with “full holdback” may introduce unacceptable delays in many SCADA deployments.

For repetitive messages (such as the status request), the same MAC value would be computed, enabling an eavesdropper to identify encrypted messages carrying the same data. The selection of the input to the MAC should include data that changes for each message so that a different MAC value is produced.

E.3.2 Inter-message integrity

An adversary who is unable to modify or forge individual messages might still be able to reorder messages, replay old messages, or destroy specific messages. Given a solution to intra-message integrity with low latency, inter-message integrity is assured.

Unlike on the Internet, where a packet can travel multiple paths, a SCADA message usually travels over one specific communication link. An adversary able to write messages to this communication link can effectively deny use of this link by damaging every message sent on the link. Fortunately, most SCADA masters will detect the fact that commands and responses are not getting through and alert an operator, who can initiate actions to try to track down the attack. Therefore, the focus is on attacks that attempt to reorder or replay the occasional message, which would be difficult for most SCADA software to distinguish from the occasional problems introduced by communication channel noise. Any implementation should include methods to prevent message replay.

Two aspects of the SCADA environment conspire to make the problem of preventing replay and reordering of messages difficult. One is the requirement for timely delivery of SCADA responses to polls. The second is the potential for collisions on the communication link. The next two sections discuss these issues.

E.4 Accommodating various SCADA poll and retry strategies

Existing SCADA protocols already include mechanisms for handling messages lost or damaged in transit by line noise. Some SCADA systems may timeout and retry sending the message. Some systems may simply move on to the next remote unit in the polling cycle, rather than retry. Some SCADA systems may use positive and/or negative acknowledgements in conjunction with timeouts. A TCP-like protocol to carry SCADA messages that uses windowing, retry, and timeouts could ensure reliable, ordered

delivery between cryptographic modules, but delays introduced by the process may interfere with the SCADA system's error-handling mechanism and lead to SCADA responses being delivered out of synchronization with polls. A protocol for protecting SCADA communications should take into account the time-sensitive nature of SCADA messages and the various manners in which SCADA systems poll and retry.

E.5 Avoiding communication channel collisions

Half-duplex serial and multidrop serial lines generally do not provide a method to ensure that two senders do not transmit at the same time. Furthermore, senders whose messages collide may not receive any notification of this collision. Many SCADA networks avoid collisions by having remote units send messages in response only to polls from a single master. The protocol used by cryptographic modules should be careful to avoid increasing significantly the chance of a collision in the communication channel.

E.6 Supporting mixed-mode deployments

In a multidrop SCADA network in which there are multiple remote field units sharing a channel, some of the remote units may not be sufficiently important to merit the business decision for a cryptographic module. Alternatively, during a phased installation, the modules for some remote units may not yet be deployed. In a mixed-mode deployment, SCADA messages destined for remote units not protected by cryptographic modules will be transmitted in their native SCADA form. Thus, native SCADA messages and encrypted messages will not interfere with each other. A security protocol for protecting SCADA communication should accommodate such mixed-mode deployments. Furthermore, the fact that some messages are available in cleartext form should not reduce the security assurances provided for encrypted messages.

E.7 Supporting broadcast messages

Most SCADA systems include some form of broadcast capability. Integrity for broadcast messages may be less or more important than for unicast messaging. For instance, integrity may be considered less important for a "set the time" message, but more important for an "emergency shutdown" message. However, broadcast communication can be awkward to achieve in a setting where messages are encrypted. Since all remote field units must be able to decrypt a broadcast message sent from a SCADA master, they all must have access to the decryption key. The selection of a key management protocol that supports broadcasting or multicasting becomes extremely important.

A solution to protecting the integrity of broadcast messages should take into account the SCADA system's mechanism for ensuring delivery of a broadcast message. Many SCADA systems simply repeat the broadcast message several times, which may be acceptable for small systems with only a few devices.

A solution to protecting the integrity of broadcast messages also should consider mixed-mode deployments in which some of the SCADA remote units are not protected by a cryptographic module and must receive the broadcast in cleartext (native SCADA) form. If a broadcast message in a mixed-mode deployment is transmitted twice, once in plaintext form and once in ciphertext form, the cryptographic protocol should take into account that the adversary has precise knowledge of the plaintext.

E.8 Incorporating key management

Key management is a set of processes and mechanisms that support generation and establishment of keys and the maintenance of keying relationships, including replacing old keys with new keys when necessary. Key management for cryptographic modules can be as simple as manual entry of the same symmetric key into the configuration interfaces of two or more modules, or as complex as PKI or as sophisticated as a system that provides for discovery of peering relationships and provides the centralized management of role-based authentication and authorization requirements. Above all, a key management system for cryptographic modules should result in a system that is simple to operate by the user community so as not to complicate significantly the operations and maintenance tasks required of operators and field technicians. More sophisticated key management methods can simplify and centralize the processes required for key management, but some of these more sophisticated methods require high bandwidth and/or a high degree of connectivity between modules. As noted earlier, SCADA communication links often provide only low bandwidth. Furthermore, in many environments in which SCADA systems are used, there are many independent SCADA communication lines. Cryptographic modules on separate communication lines will be unable to exchange key management information without an additional communications channel.

Key management for cryptographic modules is a subject of sufficient importance and scope that it will be the subject of a future AGA 12, Part 1 recommendation.

Appendix F Cyber security practice fundamentals (normative)

When discussing security with organizations responsible for operations, there is a belief that process control systems such as SCADA and DCS are different than IT managed systems and, as such, have special needs or requirements. From a technological and environmental viewpoint (hardware, software, protocols, communication media, temperature, humidity, etc.), there is some truth in this belief. However, from a security viewpoint, in particular when data derived from process control systems eventually affect business systems managed by corporate IT, the need for a consistent corporate-wide security strategy is paramount, and the processes to determine security needs in these two types of systems are identical.

Appendix F of AGA 12, Part 1 builds upon the recommended cyber security practices outlined in Section 3, by describing in more detail many of the steps that should be undertaken. Subjects addressed include organizing a cyber security team, developing cyber security policies, assessing the current state of cyber security, analyzing the findings to define priorities and required resources, knowing when goals have been reached, and implementing ongoing processes to maintain these goals.

F.1 Recommendations for staffing an InfoSec team

Once senior management has decided that it needs to address cyber security issues, the first step is to form an InfoSec team. The InfoSec team should consist of not only technicians and engineers from IT and operations, but also stakeholders from all segments of the company that are covered by the scope of the security project or that would be harmed by the compromise of the data.

Technicians and engineers tend to understand the hardware and software components of an enterprise or field communications network. Support personnel understand the operations and daily management of the enterprise and field operations network. Users and operators understand the business processes the networks and systems support and the relevance of the information or data that they generate, process, store and share. Management understands the costs and business impacts when processes change. And corporate council understands the regulatory and legal issues that require compliance and have enforcement implications. Each of these stakeholders has a different view of the cyber security project and should be required to join the InfoSec team so that their unique perspectives can be taken into account.

A member of senior management should head the InfoSec team because it is inevitable that information security enhancement will involve some expense, disrupt business processes for a period of time as assessments are being conducted, and potentially lead to future changes in business processes. Because of his or her position, a senior manager can approach department heads and request assistance to support the InfoSec team’s efforts, present findings and recommendations to other members of senior management, and enforce policies.

Finally, the InfoSec team should be chosen carefully since these employees or contractors will delve into many sensitive business areas of the company, such as access control methodologies, cryptography management, and databases of confidential information. The findings of the InfoSec team also will become sensitive because they will document security flaws and vulnerabilities within customer, partner and supplier contracts and agreements.

AGA 12 recommends that all members of the InfoSec team each sign an ethics and confidentiality agreement before joining the team, stating their agreement to protect the confidentiality of all of their findings, not use their newly acquired knowledge in a malicious or unapproved manner, and keep the findings private.

F.2 Awareness of cyber security assurance

Either during or soon after the formation of the InfoSec team, someone will raise the questions, “Where do we begin?” and “What needs to be addressed?” For team members and organizations that have never taken a top-down look at a business, these can be troubling questions. In the 1990s, the U.S. government asked the same questions about its own cyber systems. It concluded that it needed a consistent cyber security philosophy and methodology across every department and agency and, as a result, began the task of documenting the best practices, standards, and training required to accomplish its goal. NIST and NSA became the lead organizations creating these standards and documentation, some of which are available to the public on the following web sites.

- http://csrc.nist.gov/publications [12]
- www.nsa.gov/isso [13]
- www.iatf.net [14]
- www.nstissc.gov [15]

NIST and NSA concluded that cyber security can be divided into three general categories and then further subdivided into 18 specific classes (see Table F- 1). Appendix F addresses three of the NIST-defined security classes: InfoSec Documentation, System Assurance and Auditing. This does not mean that the AGA 12 Task Group felt the other classes were not important. Instead, the Task Group felt two classes (InfoSec Documentation and System Assurance) are the foundation upon which all of the others are built, and the third (Auditing) is the key to retaining an effective security posture. As such, they are important enough to warrant further detail in this appendix.

AGA 12 recommends that readers review Table F- 1 and its related documentation, developed by NIST [12] and the NSA [13] to understand better how to achieve an effective security posture.

Table F- 1 Cyber security categories and classes

Category	Class	Description
Management	InfoSec Documentation	The InfoSec documentation includes cyber security policies, guidelines, regulatory requirements, standard operating procedures, and user documentation.
Management	InfoSec Roles and Responsibilities	This management plan includes definitions of and responsibilities for information owners, organizations, and users.

Category	Class	Description
Management	Contingency Planning	The contingency plan identifies single points of failure, backup and restoration plans and procedures, and man-made or natural events that may disrupt an organization's ability to conduct business.
Management	Configuration Management	This management plan establishes a Configuration Control Board; patch and update review, approval and acceptance process; and processes to document and backup current system configurations.
Technical	I&A	The I&A document is the most fundamental element of InfoSec; it defines the requirements for I&A for each security domain and information sensitivity level, including the use of multi-factor authentication and the use of cryptography for access to resources, such as facilities, systems, networks, software and data.
Technical	Account Management	The account management document defines the formal processes to request an account on a system or request access to data; includes processes for resource (information) owner's approval, direct-report supervisory approval, procedures to disable accounts when users are terminated, and procedures for reviewing and eliminating in-active accounts.
Technical	Session Control	The session control document defines the protective measures for workstation access, network access and remote access, such as inactivity timeouts, password or PIN blocking on unsuccessful log-on attempts or least-privilege account permissions.
Technical	Auditing	The auditing document defines the standard operating procedures for what to audit and when to audit; defines requirements for intrusion detection, audit data reduction tools, and audit log retention.
Technical	Malicious Code Protection	The malicious code protection document defines the procedures for how and what software may be loaded onto systems and networks, requirements for scanning tools, updates to scanning tools, employee training and awareness, violation enforcement, and recovery procedures.
Technical	Maintenance	The maintenance document defines the policies for personnel performing maintenance, including vendor personnel; control of diagnostic software and scan results; disposition of failed components; and remote access for support purposes.
Technical	Systems Assurance	The systems assurance document defines the need and procedures for certification and accreditation, security test and evaluation, and independent verification and validation.

Category	Class	Description
Technical	Networking and Connectivity	The networking and connectivity document defines the policies for “allow everything” or “allow nothing” cyber security philosophies; justification for local and remote access; defines need and operating procedures for intrusion detection, auditing, firewalls, link encryption or tunneling, wireless, and hiding internal network architecture.
Technical	Communications Security	The communications security document defines the requirements and procedures for accessing, transmitting and sharing sensitive information; includes document security, link encryption/tunneling, cryptographic algorithms and key strengths.
Operational	Media Control	The media control document defines the policies, procedures, and responsibilities for backup media handling, including on-site and off-site storage, transportation, re-use, sanitization and destruction.
Operational	Labeling	The labeling document defines the policy and procedures for marking sensitive information, including document, media, systems, and facilities.
Operational	Physical Environment	The physical environment document defines the requirements for physical security (secure facilities, guards, vaults, etc.) to augment cyber security.
Operational	Personnel Cyber Security	The personal cyber security document defines the policy and procedures for personnel hiring and termination, including background checks, security clearances, signed agreements, account management, and training and education.
Operational	Education Training and Awareness	The education training and awareness document defines the policy and procedures for initial and periodic review of security policies, standard operating procedures, and security trends and vulnerabilities.

F.3 Recommendations for writing cyber security policies

Cyber security policies are an organization’s written statement of how resources or assets, such as facilities, personnel, systems, and information, should be acquired, managed over their useful life and retired at end-of-life. Cyber security policies define practices and procedures to guarantee management’s security visions are met, and they grant the authority to departments and individuals to carry out those practices and procedures. AGA 12, Part 1 recommends that cyber security policies be developed by the InfoSec team and approved for implementation and clearly supported by the company’s senior management.

The goal of a cyber security policy is to mitigate risk to an acceptable level by defining what is important to an organization; by establishing procedures, practices, and responsibilities to manage resources in a consistent and prudent manner; and by

defining steps to limit corporate exposure when something goes wrong.

When a breakdown in the system occurs, cyber security policies define how to recover from an incident, how to determine if the incident was a malicious act, how to investigate and handle evidence related to the incident and, if it necessary, what disciplinary and/or legal actions should be taken. Cyber security policies are becoming increasingly important in business litigation. Organizations that have well-defined security policies and, more important, actively adhere to them, find it easier to defend themselves against negligence or wrongful-cause litigations, as well as to prosecute those that commit maliciously acts using or targeting those resources.

In order for a cyber security policy to be effective, the policy should be understood easily and followed by those individuals it affects. A cyber security policy should cover cyber security only and not address other types of security matters. Cyber security policies usually are written in an outline format. They start with general management-driven policy statements and drill-down to specific procedural details that are required to meet the goals of the policy. AGA 12, Part 1 recommends that policy statements be broad in scope and avoid technical terminology, and that associated procedure statements be technical and detailed in nature. Cyber security policies should be balanced; too much trust leads to too little cyber security, while too much cyber security leads to an inability to complete the mission at hand.

AGA 12 recommends that a cyber security policy contain, as a minimum, the following major sections.

- Overview: A single paragraph that describes the essence of the policy.
- Purpose: A single paragraph documenting why the senior management team feels the policy is required.
- Scope: A single paragraph defining the personnel, departments, business functions, processes, and resources that are affected by the policy.
- Policy: The actual security policy statement; it documents senior management's goals or priorities for the subject matter and empowers specific departments or individuals to implement and enforce the policy.
- Practices: A definition of the InfoSec team's strategies to implement the policy.
- Procedures: A description of the specific steps and details to implement the strategy in a particular instance.
- Enforcement: A description of actions that will be taken against individuals who intentionally or maliciously circumvent the policy.
- Checklists: A description of the procedural steps to implement, enforce, maintain, audit, and track the implementation and awareness of the policy.
- Definitions: A glossary, which defines terms used within the policy.
- History: A date-stamped list documenting all revisions to the policy.

Cyber security policies are living documents. They will change over time along with the culture and the needs of a company and with the introduction of new technologies. Some up-front thought should be given to how the cyber security policies will be made available to employees and how the document will be maintained to support the BCP, IRT, and AEP.

Some organizations find it best to print the documents, while others find it best to keep them available on the corporate intranet. For instance, if the BCP identified electrical

power loss as a concern, then the IRT that directs recovery efforts should have printed documents because the electronic version may not be accessible during a power outage. If the BCP mandates printed copies for some personnel, it is advisable that a central administrator send notices of changes to the affected individuals and require the return of the original documents as an audit to make sure the printed copies are up-to-date. Since policies will change over time, it is important that an AEP be associated with the cyber security policies to guarantee that employees review them on a periodic basis.

The goal of a security policy is to lower risk to an acceptable level by defining what is important to an organization; by establishing procedures, practices and responsibilities to manage resources in a consistent and prudent manner; and by defining steps to limit corporate exposure when something goes wrong. But, most important, cyber security policies are effective only if they are followed strictly on a daily basis.

F.4 Recommendations for performing assessment and analysis

Investing in cyber security creates costs in the forms of staff time, short-term inconvenience to your business, and procurement of hardware, software, and services. When implementing security, it is all too easy to invest money and efforts at the wrong place or at the incorrect level. In order to rationally allocate resources, assessment and analysis should be performed to identify the current state of cyber security; determine areas in which it is deficient, prioritize each deficiency, and determine if potential corrective actions are sufficient, effective, and economically sound.

Since the September 11, 2001, terrorist attacks on the United States, a number of industry organizations and governmental agencies have called for utilities to perform vulnerability assessments of their SCADA communication systems. From a cyber security viewpoint, when reading the recommendations for the assessment, most of these documents describe perimeter testing only, such as the assessments conducted during a traditional PTA. AGA 12, Part 1 recommends that further analysis be performed to assess impacts on internal systems, networks, and data stores.

AGA 12 recommends a methodology for securing a cyber system, which is described below. The methodology is built upon a concept called DiD. To implement DiD, AGA 12, Part 1 recommends that three practices be implemented: TLA, SAA and SCA.

DiD is a practice of placing multiple barriers between an attacker (a threat agent) and the prize or secrets within the inner-sanctum of the cyber system. Each barrier protects the cyber system in a particular manner, and each barrier augments the cyber security of the barrier before it. Each barrier defines a cyber security domain for which every system, application, network, packet of data, and operator needs to possess the proper cyber security characteristics and operate at the appropriate cyber security level. As data (and people) transition between security domains, AGA 12, Part 1 recommends that each piece of data or person is evaluated to determine the following.

- What it is, where it came from, and where it is going?
- That it is authorized to transit the barrier and proceed to its destination.
- That data are validated to ensure their integrity.
- That, when appropriate, data require encryption to keep them confidential from adversaries.
- That when appropriate, data require non-repudiation so one of the parties cannot claim at a later time it was not involved in the transaction.

- That, when appropriate, real-time tracking is implemented effectively for accounting purposes.
- That post-processing tracking is implemented effectively for audit purposes.

F.4.1 Three-layer analysis

Cyber systems in use by many utilities today are designed and implemented to support a number of underlying business practices. Many times the business practices require sharing data between systems of differing makes or vintages, and interconnection to remote facilities or outside business partners. The bottom line is, these systems and architectures are complex, and implementing cyber security properly and without affecting the underlying business practice will be accomplished only with great care.

Just as cyber security policies are developed via a top-down approach, AGA 12, Part 1 recommends that cyber security for a complex cyber system be designed and implemented the same way — by starting with the cyber security needs of the entire cyber system, and then drilling down to the needs of the individual systems, applications, data, transactions, and users.

TLA is a practice of identifying the cyber security needs of a complex cyber system by defining areas of common security requirements, called “security domains” and by focusing on business practices and the flow of data between various networks, systems and applications.

F.4.1.1 First steps

TLA begins by evaluating the physical infrastructure of the cyber system, essentially a detailed “as-built” map of the system. TLA identifies each perimeter entry point, edge system or device, internal system or device, and communication path. Next, TLA looks at what types of data flow over each communication path. TLA identifies each protocol employed on a communication segment (such as PPP, TCP/IP, HTTP, DNP, Modbus) and lists their capabilities and vulnerabilities. Finally, TLA looks at the relationship between software and data. Specifically, what is system software and what is application software, where data are generated, where data are stored, how data are packaged and formatted, how data flow between systems and devices, and where data are generated, processed and used.

F.4.1.2 Post-TLA evaluation

After TLA has been completed, a picture begins to emerge that describes each security domain including its systems, software, applications, and data. Also described are the cyber security boundary that surrounds each security domain and what data are allowed to move through it.

Post-TLA evaluation should identify and characterize the vulnerabilities and threats to the cyber system — where attacks may come from, who may perform an attack, and what an attack may target.

F.4.2 Cyber security architecture analysis

AGA 12, Part 1 recommends the use of SAA, which is a proactive or an offensive approach to cyber security.

SAA begins by examining each cyber security domain, focusing on its resources (systems, applications, communications medium, protocols, users, and data-at-rest),

comparing them with the organizations' security policies to determine the appropriate security requirements that should be applied to the domain. Within any cyber security domain, all resources should be treated equally. If resources have different security requirements, such as levels of sensitivity, integrity, or access control, recommendations should be made to move one or more of the resources to a more appropriate domain. Likewise, if it is determined the security domain is not being protected properly, corrective measures, such as tightening access control methodologies or adding cryptography, should be implemented.

Finally, SAA evaluates the interaction between cyber security domains, which results in identifying the security requirements for the data-in-transit, transaction processing, and communication protocols. If it is determined the data-in-transit or transactions are not being protected properly, accounted for, and audited, then the use of cryptography for authentication, authorization, confidentiality, integrity or non-repudiation should be implemented.

Likewise, the protocols in use may not be appropriate to cross a cyber security boundary, such as those that are broadcast-based and do not direct their traffic to a specific end-point device. If so, changing protocols, encapsulating the protocol, or adding an application firewall is recommended.

F.4.3 Successive compromise analysis

SCA is an investigative or auditing approach to cyber security. SCA is described most easily as surgical penetration testing. After TLA and SAA are complete, a definitive list of potential vulnerabilities within a security domain, a security boundary, and inter-domain transactions are known.

Using SCA techniques, AGA 12, Part 1 recommends applying SCA techniques and using the knowledge gained to target the vulnerabilities to determine if protective measures are configured correctly and provide the required level of security.

F.4.4 Risk analysis

In order to allocate resources in a rational manner, AGA 12, Part 1 recommends that an analysis be performed to identify security needs by priority and to determine if the proposed corrective actions are economically sound. Risk analysis is the process of bringing together the assessment and analysis findings and the corrective action recommendations into a format that senior management can use to determine if solutions are appropriate.

Risk analysis typically is performed in two steps — a quantitative analysis and a qualitative analysis. A quantitative analysis answers the question of appropriateness by evaluating costs, while a qualitative analysis answers the question of appropriateness by evaluating company priorities.

F.4.4.1 Quantitative analysis

A quantitative analysis focuses on costs related to risks verses costs related to corrective actions. AGA 12, Part 1 recommends that this approach be used to estimate anticipated costs, similar to looking for a return on investment. If the cost of corrective action is similar to or higher than the cost related to risk, then the corrective action should be reconsidered. However, if the cost of corrective action is significantly lower than the cost related to risk and meets the goals and standards set forth in approved cyber security policies, then a realistic corrective action opportunity has been identified.

Quantitative analysis does have one drawback. The numbers used to calculate costs typically are incomplete, often based on guesses or underlying assumptions and, therefore, inaccurate. For this reason, AGA 12, Part 1 recommends that a quantitative analysis be performed to determine if a proposed corrective action is feasible economically and warrants further consideration.

F.4.4.2 Qualitative analysis

A qualitative analysis focuses on company priorities. It should be used to determine where management feels it is most at risk. Risk priorities should consider internal decisions as well as constraints introduced from outside sources, such as regulators, industry associations, or stockholders. For this reason, AGA 12, Part 1 recommends that qualitative analysis be performed to determine if a proposed corrective action is feasible economically and warrants further consideration.

F.4.4.3 The final step of risk analysis

The final step of the risk analysis is to review the quantitative and the qualitative analyses to determine the highest priority corrective actions, based on which potential solution provides the highest economic return. If a particular corrective action is near the top of both analyses, it is a good sign that it is a serious candidate for consideration.

F.5 Auditing

Cyber security is an ongoing effort. Just when everything seems to be under control, a new vulnerability is discovered, a new worm or virus is launched, a new system patch or update is made available by a vendor, a new requirement is mandated by management or a regulator agency, or someone within the organization adds a new feature to the cyber system without consulting the InfoSec team. For this reason, AGA 12, Part 1 recommends that audits be performed to determine if the protective measures are installed correctly and are effective. AGA 12, Part 1 recommends three types of audits that should become part of the cyber security portfolio — a preliminary action audit, a post-implementation audit, and a recursive audit.

F.5.1 Preliminary action auditing

TLA, SAA, and SCA as described in Sections F.4.1, F.4.2, and F.4.3, respectively, will take time and require employees or contractors with extensive experience to conduct them. As a result, it may be a number of months from the time these processes begin to the actual implementation of the analysis-derived protective measures. AGA12, Part 1 recommends performing a PAA as a good first step to securing a cyber system. The PAA will identify common-sense protective measures that every organization should implement, including proper settings on firewalls, passwords that are not shared by multiple individuals, and passwords that are not guessable. The DOE “21 Steps to Security” [18], the American Petroleum Institute’s document “API 1164” [19], the ISA-TR99 documents [20] [21], and the NERC 1200 series [22] are examples.

F.5.2 Post-implementation auditing

After implementing a corrective action, whether it was recommend by a preliminary action audit or derived from an extensive analysis of your cyber system, AGA 12, Part 1 recommends that a post-implementation audit be performed to determine if the counter measure was installed and configured correctly, and mitigates the risk to an acceptable

level. If the counter measure was chosen, implemented, or configured incorrectly, it is possible that it may not mitigate a risk to an acceptable level or, in some cases, actually may introduce an entirely new set of vulnerabilities, threats and risks. If the post-implementation audit reveals that the risks are not mitigated to an acceptable level, AGA 12, Part 1 recommends that an action item be generated to instruct the InfoSec team to investigate the situation and develop a new plan of action to correct the deficiency.

F.5.3 Recursive auditing

Over time systems change because new features are added or components are upgraded or replaced and, unfortunately, new vulnerabilities probably will be discovered on a daily basis. The efforts made to secure the cyber system as little as a year before may not be adequate today.

For this reason, AGA 12, Part 1 recommends that a recursive audit (also known as “red team penetration testing”) be conducted periodically or when needed. The recursive audit should be designed to review all cyber systems for changes and to evaluate whether changes made or new threats identified have degraded the protection desired. Like the post-implementation audit, the recursive audit will show the InfoSec team the appropriate steps to take if a new risk has been identified or a previous risk is no longer mitigated to an acceptable level.

Appendix G Classes of attacks against SCADA systems (informative)

The AGA 12 series focuses attention on “Cryptographic Protection of SCADA Communications.” AGA 12, Part 1 and all subsequent documents in the series recommend practices to mitigate cyber attack against SCADA communication, with some extensions to protect SCADA data at rest — who can access the information, what they can do with the information, and control over the duration of the access privilege. AGA 12, Part 1 does not use the strict definition of SCADA; rather, AGA 12, Part 1 includes all supervisory control and data acquisition functions related to operation, maintenance, and engineering associated with gas, electricity, water, wastewater, and pipeline transmission and distribution systems.

Appendix G address two subjects: classes of attacks and security models that are addressed in the AGA 12 series, and the classes of attacks that are not addressed in the AGA 12 series.

G.1 Technical references

[1] Doraswamy, Naganand and Harkins, Dan (1999) “IPSec – The New Security Standard for the Internet, Intranets, and Virtual Private Networks,” Prentice Hall PTR.

[2] Kay, Trevor (2003) “Mike Meyers’ Certification Passport – Security+,” McGraw-Hill/Osborne.

[3] Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) “Handbook of Applied Cryptography,” CRC Press.

[4] Northcutt, Stephen (1999) “Network Intrusion Detection: An Analyst’s Handbook,” New Riders Publishing.

[5] Rescorla, Eric (2001) “SSL and TLS – Designing and Building Secure Systems,” Addison-Wesley.

[6] Theriault, Marlene and Heney, William (1998) “Oracle Security,” O’Reilly & Associates, Inc.

G.2 Classes of attacks and security models addressed in the AGA 12 series

The purpose of Section G.2 is to describe more clearly the classes of attacks and security models considered in the normative parts of the AGA 12 series and to characterize when encryption is and is not effective. Furthermore, when encryption is not an effective solution, suggested alternatives are described.

Menezes [3] in the “Handbook of Applied Cryptography” describes the classes of attacks and security models that were adopted with some modification for the AGA 12 series.

G.2.1 Communication participants and channels

The following terminology describes the communication participants.

- An entity or party is someone or something that sends, receives, or manipulates information.

- A sender is an entity in a two-party communication that is the legitimate transmitter of information.
- A receiver is an entity in a two-party communication that is the intended legitimate recipient of information.
- An adversary is an entity in a two-party communication that is neither the sender nor receiver and that tries to defeat the information security service being provided between the sender and receiver. Various other names are synonymous with adversary, such as enemy, attacker, opponent, tapper, hacker, eavesdropper, intruder, and interloper. An adversary often will attempt to play the role of either the legitimate sender or the legitimate receiver.

The following terminology describes the communication channels.

- A channel is a means of conveying information from one entity to another.
- A physically secure channel or secure channel is one that is not physically accessible by the adversary.
- An unsecured channel is one from which parties other than those for which the information is intended can reorder, modify, delete, insert, or read.
- A secured channel is one from which an adversary does not have the ability to reorder, modify, delete, insert, or read.

One should note above the subtle difference between a physically secure channel and a secured channel — a secured channel may be secured by physical or cryptographic techniques.

- An information security service is a method to provide some specific aspect of security. For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.
- Breaking an information security service (which often involves more than simple encryption) implies defeating the objective of the intended service.
- A passive adversary is an adversary that is capable only of reading information from an unsecured channel.
- An active adversary is an adversary that also may transmit, alter, or delete information on an unsecured channel.
- A passive attack is one in which the adversary only monitors the communication channel. A passive attacker only threatens the confidentiality of data. Passive threats include release of information and traffic analysis.
- An active attack is one in which the adversary attempts to delete, add, or in some other way alter the transmission on the channel. An active attacker threatens data integrity and authentication as well as confidentiality. Active threats include masquerade, replay, modification of message content, and denial of service.

G.2.2 Attacks on encryption schemes

The objective of the following attacks is to systematically recover plaintext from ciphertext, or even more drastically, to deduce the encryption key.

- A ciphertext-only attack is one in which the adversary tries to deduce the encryption key or plaintext by only observing the ciphertext. Any encryption scheme vulnerable to this type of attack is considered completely insecure. The AGA 12 series is designed to mitigate this threat.

- A known-plaintext attack is one in which the adversary has a quantity of plaintext and then is given the corresponding ciphertext. The AGA 12 series is designed to mitigate this threat.
- A chosen-plaintext attack is one in which the adversary chooses plaintext and then is given the corresponding ciphertext. Subsequently, the adversary uses any information deduced to recover plaintext corresponding to previously unseen ciphertext. The AGA 12 series is designed to mitigate this threat.
- An adaptive-chosen plaintext attack is a chosen-plaintext attack wherein the choice of plaintext may depend on the ciphertext received from previous requests. The AGA 12 series is designed to mitigate this threat.
- A chosen-ciphertext attack is one in which the adversary selects the ciphertext and then is given the corresponding plaintext. One way an adversary mounts such an attack is by gaining access to the equipment used for decryption (but not the decryption key, which may be embedded securely in the equipment). The objective is to be able, without access to such equipment, to deduce the plaintext from (different) ciphertext. The AGA 12 series is designed to mitigate this threat.
- An adaptive chosen-ciphertext attack is a chosen-ciphertext attack in which the choice of ciphertext may depend on the plaintext received from previous requests. The AGA 12 series is designed to mitigate this threat.

Most of these attacks also apply to digital signature schemes and message authentication codes. In this case, the attacker's objective is to forge messages, which is described in Section G.2.3.

G.2.3 Types of attack on signature schemes

The goal of an adversary is to forge signatures; that is, produce signatures that will be accepted as those of some other entity. The following provides the set of criteria used in the AGA 12 series to break a signature scheme.

- Total break: An adversary is able either to compute the private key information of the signer or to find an efficient signing algorithm functionally equivalent to the valid signing algorithm.
- Selective forgery: An adversary is able to create a valid signature for a particular message or class of messages chosen *a priori*. Creating the message does not directly involve the legitimate signer.
- Existential forgery: An adversary is able to forge a signature for at least one message. The adversary has little or no control over the message whose signature is obtained, and the legitimate signer may be involved in the deception.

There are two basic attacks against public-key digital signatures that were considered in the design of the AGA 12 series.

G.2.3.1 Key-only attacks

In these attacks against public key cryptographic algorithms, an adversary knows only the signer's public key.

G.2.3.2 Message attacks

Here an adversary is able to examine signatures corresponding either to known or

chosen messages. Message attacks can be divided further into three classes.

- Known-message attack: An adversary has signatures for a set of messages that are known to the adversary but not chosen by the adversary.
- Chosen-message attack: An adversary obtains valid signatures from a chosen list of messages before attempting to break the signature scheme. This attack is nonadaptive in the sense that messages are chosen before any signatures are seen. Chosen-message attacks against signature schemes are analogous to chosen-ciphertext attacks against public-key encryption schemes.
- Adaptive chosen-message attack: An adversary is allowed to use the signer as an oracle; the adversary may request signatures of messages that depend on the signer's public key and on previously obtained signatures or messages.

In principle, an adaptive chosen-message attack is the most difficult type of attack to prevent. It is conceivable that given enough messages and corresponding signatures, an adversary could deduce a pattern and then forge a signature of its choice. While an adaptive chosen-message attack may not be feasible to mount in practice, the AGA 12 series includes a well-designed signature scheme that is designed to protect against the possibility.

The level of security required in a digital signature scheme may vary according to the application. For example, in situations in which an adversary is capable of mounting a key-only attack only, it may suffice to design the scheme to prevent the adversary from being successful at selective forgery. In situations in which the adversary is capable of a message attack, it may be necessary to guard against the possibility of existential forgery. The AGA 12 series includes options for both situations.

When a hash function, ***h***, is used in a digital signature scheme (as is the case in the AGA 12 series), ***h*** should be a fixed part of the signature process so an adversary is unable to take a valid signature, replace ***h*** with a weak hash function, and then mount a selective forgery attack.

G.2.4 Protocols and mechanisms

A cryptographic protocol (protocol) is a distributed algorithm defined by a sequence of steps precisely specifying the actions required of two or more entities to achieve a specific security objective.

As opposed to protocol, a "mechanism" is a more general term encompassing protocols, algorithms (specifying steps followed by a single entity), and noncryptographic techniques (e.g., hardware protection and procedural controls) to achieve specific security objectives.

Encryption schemes, digital signatures, hash functions, and random number generation are among the basic cryptographic tools used in the AGA 12 series to build a protocol.

A protocol failure or mechanism failure occurs when a mechanism fails to meet the goals for which it is intended, in a manner whereby an adversary gains advantage not by breaking directly an underlying primitive such as an encryption algorithm, but by manipulating the protocol or mechanism itself. The AGA 12 series is designed to mitigate this risk.

G.2.5 Attacks on protocol

The following is a partial list of attacks that might be mounted on various protocols. Until

a protocol is proved to provide the service intended, the list of possible attacks can never be said to be complete. For this reason, AGA 12, Part 1 includes a comprehensive recommendation in Section 3 and Appendix F to review, test, and evaluate continually the implemented security policies.

- Known-key attack: An adversary obtains some keys used previously and then uses this information to determine new keys. The AGA 12 series is designed to mitigate this threat.
- Replay: An adversary records a communication session and replays either all or parts of the session at some later point in time. The AGA 12 series is designed to mitigate this threat.
- Impersonation: An adversary assumes the identity of one of the legitimate parties in a network. The AGA 12 series is designed to mitigate this threat.
- Dictionary: This is usually an attack against passwords. 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 with the stored value. An adversary can take a list of probable passwords, hash all entries in this list, and then compare this with the list of true encrypted passwords with the hope of finding matches. The AGA 12 series is designed to mitigate this threat.
- Forward search: This attack is similar in spirit to the dictionary attack and is used to decrypt messages. The AGA 12 series is designed to mitigate this threat.
- Interleaving attack: This usually involves some form of impersonation in an authentication protocol. The AGA 12 series is designed to mitigate this threat.

G.2.6 Models for evaluating security

The AGA 12 Task Group has evaluated the cryptographic primitives and protocols using several different models. The most practical security metrics are computational, provable, and ad hoc methodologies. Quantitative analysis has been performed using a CRM in combination with laboratory tests using proof-of-concept cryptographic hardware. Shortly after publication of AGA 12, Part 1, cryptographic schemes will be field-tested using the SCADA systems of several gas, electric, and water utilities.

In this manner, the confidence level in the amount of security provided by a primitive or a protocol base on computational or ad hoc security increases with time and investigation of the scheme. However, time is not enough if few people have given the method careful analysis.

G.2.6.1 Unconditional security

The most stringent measure is an information-theoretic measure — whether or not a system has unconditional security. An adversary is assumed to have unlimited computational resources, and the question is whether or not there is enough information available to defeat the system. Unconditional security for encryption systems is called “perfect secrecy.” For perfect secrecy, the uncertainty in the plaintext, after observing the ciphertext, must equal the *a priori* uncertainty about the plaintext — observation of the ciphertext provides no information whatsoever to an adversary. Based on CRM and laboratory tests, AGA 12, Part 1 implementations meet this requirement.

G.2.6.2 Complexity-theoretic security

An appropriate model of computation is defined and adversaries are modeled as having polynomial computational power. Then a proof of security relative to the model is constructed. An objective is to design a cryptographic method based on the weakest assumptions possible in anticipation of a powerful adversary. Asymptotic analysis and usually also worst-case analysis are used and so care should be exercised to determine when proofs have practical significance. In contrast, polynomial attacks that are feasible under the model might, in practice, still be computationally infeasible.

Security analysis of this type, although not of practical value in all cases, nonetheless, may pave the way to better overall understanding of security. Complexity-theoretic analysis is invaluable for formulating fundamental principles and confirming intuition.

The AGA 12 Task Group did not perform complexity-theoretic analysis, but it encourages other expert groups to perform this analysis and publish their findings.

G.2.6.3 Provable security

A cryptographic method is said to be provably secure if the difficulty of defeating it can be shown to be as difficult essentially as solving a well-known and supposedly difficult (typical number-theoretic) problem, such as integer factorization or the computation of discrete algorithms. Thus, “provable” here means provable subject to assumptions.

This approach is considered by some to be the best existing practical analysis technique. Both CRM and laboratory testing have shown that AGA 12, Part 1 implementations provide provable security.

G.2.6.4 Computational security

This is a measure of the amount of computational effort required, by the best currently known methods, to defeat a system; it is assumed here that the system has been well-studied to determine which attacks are relevant. A proposed technique is said to be computationally secure if the perceived level of computation required to defeat it (using the best attack known) exceeds, by a comfortable margin, the computational resources of the hypothesized adversary. Computational security sometimes also is called “practical security.”

The AGA 12 Task Group worked with several utility operators and consultants to determine which attacks are relevant and relied on algorithms approved by NIST and NSA to meet the criteria for computational security.

G.2.6.5 Ad hoc security

This approach consists of a variety of convincing arguments that every successful attack requires a resource level (e.g., time and space) greater than the fixed resources of a perceived adversary. Cryptographic primitives and protocols that survive such analysis are said to have heuristic security, with “security” here typically being in the computational sense.

Basic cryptographic tools and protocols usually are designed to counter standard attacks such as those described in Sections G.2.2 and G.2.5. While ad hoc security perhaps the most commonly used approach (especially for protocols), it is, in some ways, the least satisfying. Claims of security generally remain questionable and unforeseen attacks remain a threat. Be this as it may, the AGA 12 Task Group did use an ad hoc security model to evaluate and support the recommendations in the AGA 12 series. And because

of the concerns expressed above, other experts are invited to use more formal methods to evaluate the recommendations in the AGA 12 series and report their findings.

G.2.7 Attacks against SCADA databases and related repositories

The subject of attacks against SCADA databases and related repositories is treated in part in the AGA 12 series. AGA 12, Part 1 provides recommendations for access control and use of data in these databases and repositories. AGA 12, Part 1 does not address the physical security of the databases and repositories. The same user policies and practices, which require backup and redundancy to protect high-value data, apply with or without the recommendations of AGA 12, Part 1.

Oracle and Sybase are two commonly used SCADA database management systems. The AGA 12 Task Group used with modification the Oracle Security model [6].

G.2.7.1 Threats

Adversaries have different motives for attacking SCADA databases and related repositories. Some of these motives are to gain a competitive edge, to seek revenge or to retaliate in response to how they have been harmed, simply to prove that a "protected" system can be penetrated, or curiosity. Regardless of the motive, the adversary can do significant harm.

G.2.7.2 Security model

The layers of security that can be implemented consist of the following.

- Controlling access to the database tables through roles, grants, triggers, and procedures. The AGA 12 series does address the requirements to implement secure access control and secure use of the data.
- Controlling access to a table through views, triggers, and procedures. The AGA 12 series does address the requirements to implement secure access control and secure use of the data.
- Ensuring recoverability of data. The AGA 12 series does not address the requirements to recover data, but does recommend requirements to ensure secure access control and secure use of the data for the recovery process.
- Enabling more complex forms of security, such as data encryption, digital signatures, and single sign-on. The AGA 12 series does address the requirements for the more complex forms of security.
- Supporting web site structures and database access. The AGA 12 series does not address the requirements for supporting web site structures and database access per se, but the cryptographic system solution recommended in the AGA 12 series certainly applies to this domain.

G.3 Classes of attacks not addressed in the AGA 12 series

The purpose of Section G.3 is to describe more clearly the classes of attacks on SCADA communication not addressed the AGA 12 series on cryptographic protection and to provide an explanation of why they were not considered and to offer some guidelines or suggestions on procedures and implementation to mitigate these attacks.

G.3.1 Physical attacks on SCADA

Physical attacks on SCADA communication, databases, and related repositories are not addressed in the AGA 12 series. SCADA systems, even without consideration of cyber security, should be designed to mitigate physical attacks against the communication system or, for that matter, to mitigate any disruption (e.g., environmental disruption) in communication services deemed necessary for delivery of critical mission data.

The most common approach, where needed, is to design backup systems and redundant communications into the architecture. AGA 12, Part 1 recognizes the need to consider these requirements and constraints for designing the cyber protection solution. For example, AGA 12, Part 1 requires support for mixed-mode operation in which some communications are protected against cyber attack and others are not. And, of course, the mixed-mode requirement can be applied to the operation of backup systems and redundant communication channels. The AGA 12 series also allows a SCADA system to switch from one communication system to another without disrupting cryptographic protection.

G.3.2 Layers of security not addressed

Requirements for the layers of security not addressed by the AGA 12 series consist of the following.

- Protect the operating system files.
- Protect the application code that interacts with the database.
- Control connections to the database.

G.3.3 Interdependencies on other networks

Interdependencies of one network (e.g., a gas system) on another network (e.g., an electricity grid or a communication network) are a very broad and complex problem. The complete treatment of this set of questions is beyond the scope of the AGA 12 series. The reader is referred to work done by the DOE Sandia National Laboratories, which is responsible for addressing issues of interdependency among multiple critical national infrastructures.

Despite the previous comments, there are several obvious practices that SCADA operators can follow that provide protection against interdependency problems. Good practice requires addressing interdependency problems through both policy and technology.

G.3.4 Denial of service caused by cyber attack

A DoS attack is characterized by an explicit attempt by attackers to prevent legitimate users of a system the capability from using that system. Examples include:

- Attempts to “flood” a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to disrupt service to a specific system or person.

Not all service outages, even those that result from malicious activity, are necessarily DoS attacks. Other types of attacks may include DoS as a component, but DoS may be part of a larger attack.

DoS attacks essentially can disable SCADA computer components or SCADA communication networks. Depending on the operational procedures and dependency on mission critical data, this can affect seriously the continuity of business and the reliable delivery of service.

DoS caused by cyber attack is not addressed in the AGA 12 series because cryptographic solutions cannot mitigate this attack. For example, an adversary can create scenarios to flood leased-line communication channels, dial-up communication channels, or networks based on IP. Flooding will deny access because the channel always is busy, or it could result in overflowing the communication buffers.

As discussed in Section G.3.1, providing a backup communication system can mitigate the effects of a DoS attack by allowing the SCADA system to switch to an alternate communication network if the primary network experiences a DoS attack.

G.3.4.1 Leased-line or dial-up communication service

Providing backup systems and redundant communications with hot switch-over are the most effective methods to mitigate DoS attacks against leased-line or dial-up communication services.

G.3.4.2 IP-based communication service

As described by Rescorla [5], the simplest attack that an adversary can mount on a separate port negotiation is simply to make it appear that the server isn't listening on the appropriate port at all. This is trivial to do for any adversary that can inject packets into the network. The adversary simply waits for the sender (in this case the client) to send the TCP SYN to open the connection and then forges a reset flag-TCP header (RST)[31] packet in response. The client is not able to detect that the RST packet came from the adversary rather than from the legitimate server, so the TCP stack returns an error to the client code.

Under normal circumstances, this would be a simple DoS attack and of minimal concern. However, the client's (or user's) behavior can make it something far worse. If the user follows the directions literally and activates the standard server link (not the secure server link), an adversary easily can cause the user to change to this insecure mode by simulating an error when the user tries the secure link. The situation can be made even worse if the client automatically falls back to the insecure modes. In either case, the adversary has achieved much more than a DoS attack. It's an active confidentiality and integrity attack.

Naturally, this isn't the only way that an adversary can make it appear that a connection cannot be created.

G.3.4.3 Countermeasures for IP-based communication service attacks

Noncryptographic solutions can be installed to mitigate partially these DoS attacks. IP-based systems can be constructed with partial defenses against DoS attacks. These defenses do not defeat all DoS attacks, but merely increase the cost and complexity to launch them. For example, adaptive IP routing schemes can be installed in routers, and

---

[31] TCP/IP connections are controlled through a series of packets that are received by the two computers involved in the connection. Connections are reset with a packet called an "RST." RST packets contain a sequence number that must be valid according to certain rules in the standard.

detection systems can be used to block IP flooding (sometimes called a “ping attack”).

These solutions are well beyond the scope of the AGA 12 series, but are clearly of concern to the end user.

G.3.5 Risk of terminal emulation attached directly to SCADA components

The AGA 12 series addresses all requirements to protect against terminal emulation that is connected by communications to any SCADA component. The AGA 12 series also provides secure access control of terminals connected directly to SCADA components.

However, if the adversary has the proper access and use permissions and is attached directly to a SCADA component, the adversary is now “behind the cryptographic system firewall.” For this situation, the AGA 12 series does not address the requirements for protection. The only protection against this type of an attack is to protect the SCADA component from physical access.

Appendix H Cryptographic system test plan (normative)

H.1 Introduction

The purpose, scope, objectives, intended use, and maintenance of this test plan are described.

H.1.1 Purpose

The purpose of CSTP is to define the test and evaluation requirements to measure performance characteristics introduced by integrating CM for SCADA communication security and to evaluate design compliance to the CM functional requirements specified in the AGA 12 series. The recommendations also may apply to certain DCS.

H.1.2 Scope

The scope of CSTP includes test and evaluation plans for all configurations of CMs designed to meet the requirements specified in the AGA 12 series.

H.1.3 Test and evaluation objectives

The primary test and evaluation objectives follow.

1. Measure and evaluate the performance characteristics introduced by integrating CMs into communication paths.

2. Measure and evaluate the CM application features/functions required to implement various levels of SCADA communication protection.

3. Perform regression tests and reliability tests to evaluate performance and to evaluate potential bottlenecks introduced by CMs.

4. Evaluate the interoperability of CMs provided by different manufacturers or different versions of CMs provided by the same manufacturer.

H.1.4 Intended use for CSTP

Primary and other uses of this test plan are described.

H.1.4.1 Primary use

The primary use of CSTP is to support development and configuration of facilities and of detailed procedures that will be used to perform the tests. Detailed test procedures for each facility (manufacturer, independent test and evaluation, certification, user) and test configuration will include a compliance table of the requirements specified in this test plan.

H.1.4.2 Other uses

An intended use of this test plan is to provide input to industry subcommittees about the most common test and evaluation requirements for configurations and capabilities of existing field computers and SCADA systems used in the gas, water/wastewater, pipeline, and electricity industries. Users and manufacturers will use these test and

evaluation guidelines to help them determine whether encryption can be embedded in their field systems.

The test plan also may be used to help establish independent test and evaluation procedures for platform products to evaluate encryption implementations in existing systems.

H.1.5 Maintenance of this document

The AGA 12 series will evolve to include lessons learned from tests and evaluations, as well as user experience with deployed cryptographic solutions. Commensurate with changes in the AGA 12 series, this test plan will be updated.

H.2 Technical references

[1] IEEE 1588-2000, “Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.”

[2] IEEE 1613™-2003, “IEEE Standard Environmental Requirements for Communications Networking Devices in Electric Power Substations.”

[3] IEEE 1646™-2004, “IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.”

[4] IEEE C37.115™-2003, “IEEE Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System.”

[5] American National Standard for Financial Services X9.52-1998, “Triple Data Encryption Algorithm Modes of Operation.” American Bankers Association, Washington, D.C., July 29, 1998.

[6] FIPS PUB 46-3, “Data Encryption Standard (DES).” DoC/NIST, October 25, 1999.

[7] FIPS PUB 81, “DES Modes of Operation.”" U.S. DoC/NIST, December 1980.

[8] FIPS PUB 180-2 with Change Notice, “Secure Hash Standard (SHS).” U.S. DoC/NIST, February 25, 2004.

[9] FIPS PUB 186-2, “Digital Signature Standard (DSS).”" U.S. DoC/NIST, January 27, 2000.

[10] FIPS PUB 197, “Advanced Encryption Standard (AES).” U.S. DoC/NIST, November 26, 2001.

[11] FIPS PUB 198, “The Keyed-Hash Message Authentication Code (HMAC).” U.S. DoC/NIST, March 6, 2002.

[12] NIST Special Publication 800-38A, “Recommendation for Block Cipher Modes of Operation — Methods and Techniques,” 2001 Edition.

[13] Gould Modicon Modbus Protocol Reference Guide — PI-MBUS-300 Rev A, November 1983.

[14] Modicon Modbus Protocol Reference Guide — PI-MBUS-300 Rev. J, June 1996.

H.3 Test requirements and evaluation criteria

Test requirements and evaluation criteria are defined for functional tests, performance tests and operability tests.

H.3.1 Functional and performance requirements

Functional and performance requirements are described to evaluate compliance with the CM design requirements, to describe CM application/functional testing, synchronization testing, and requirements to measure performance characteristics.

H.3.1.1 Evaluation of compliance with CM design requirements

As a minimum, a CM manufacturer shall perform KATs and MCTs. KATs are designed for ECB mode implementation. MCTs are designed for ECB and CBC mode implementations[32].

- Encryption tests shall include the serial input of plaintext, serial output of ciphertext, and validation and independent verification of the encryption using some accepted source, such as a trusted third-party program or NIST test vectors [5] [6] [7] [8] [9] [10] [11] [12].
- Decryption tests shall include the serial input of ciphertext, serial output of plaintext, and validation and independent verification of the decryption using some accepted source, such as a trusted third-party program or NIST test vectors [5] [6] [7] [8] [9] [10] [11] [12].

Supplying known plaintext to the plaintext interface of the DUT and comparing the output ciphertext with known ciphertext shall be used to evaluate the encryption function.

Supplying known ciphertext to the ciphertext interface of the DUT and comparing the output plaintext to known plaintext shall be used to evaluate the decryption function.

Validation of encryption and decryption requires that the cryptographic protocol be understood well.

H.3.1.2 Application feature/functional testing

Features of CM applications and underlying communication protocol that may be affected by network load, traffic patterns (e.g., polling sequence), or data volume should be included in functional testing. The testing process should install on the server applicable background messages and specific test scripts to exercise CM functions under test.

H.3.1.2.1 Test measurements

The objective of the tests is to verify that the operation of the CM feature under test was completed successfully. Before starting each test, there should be a defined procedure for accomplishing test verification. When a single CM performs an operation, it should be easy to determine that it was completed successfully by verifying the presence of output. When two or more CMs operate over a communication network, data volume and timing issues often make verification more difficult and may require automated data reduction and analysis.

---

[32] Test values are described in the file rijndael-vals.zip, which is available from http://csrc.nist.gov/encryption/aes/rijndael/rijndael-vals.zip.

In addition to checking that a specific CM function occurred, it also is important to validate that other functions — specifically, the process used to create the message load on the CM — also functioned properly.

H.3.1.2.2 Test configurations

All test configurations are emulated. The test configuration should include communication speed between the application processor (RTU, field device, or SCADA master) and at least two CMs that represent the target field installation. A target field installation may have the capability to send messages from the application processor to the CM at a higher speed than the communication speed between CMs.

In a network configuration, a sufficient number of application processors should be included to create a heavy load on the receiving CM.

H.3.1.2.3 Load model

Functional testing requires that the test be conducted with a heavy credible loading[33] against the CMs. Test scripts that exercise the CM feature-under-test and its converse operation (encryption versus decryption) are needed. The functional test scripts typically are run for a single iteration only, and it may be easier or required to start all test scripts concurrently. In this case, the functional test scripts should run long enough to ensure that the CM is heavily loaded when the actual test occurs. This can be accomplished by having a delay in the start of the functional test script or by performing “dummy” commands for the first few seconds while the background test scripts create a heavy credible CM load.

H.3.1.3 Synchronization testing

Synchronization testing is described in terms of clock synchronization test, CM jitter test, and CM protocol synchronization test.

H.3.1.3.1 Clock synchronization test

A clock synchronization test should be performed initially without CMs. The test should be repeated with CMs in place and the differences measured.

One approach is to use the SCADA system write and read clock commands to measure clock synchronization. If more precision is required, then a global positioning system time signal generally is used. Another approach is to use IEEE 1588 to synchronize clocks over a local area network [1].

H.3.1.3.2 CM jitter test

When multiple field devices share common data, reliable data served to a SCADA master is critical to its application integrity and system operation. The test should measure the elapsed time beginning with the entry of the last bit of the SCADA message into the sending CM to the exit of the last bit of the SCADA message from the receiving CM. This test should be repeated with and without the CMs and the standard deviation compared.

---

[33] This will include at least a test of operation under continuous polling. For multidrop applications, a sufficient number of remote units should be included in the test to evaluate scaling (incremental effect on bandwidth and robustness).

H.3.1.3.3 CM protocol synchronization test

If the CM permits recognition and/or negotiation between CMs to allow the addition of one or more new or alternate CMs to an established pair, the time to bring the new or alternate CM on line should be measured.

H.3.1.3.4 Requirements to measure performance characteristics

Timing measurements, block length probing, throughput testing, throughput measurements, performance test configurations, and load model are described to measure performance characteristics.

H.3.1.3.4.1 Timing measurements

Any timing reported by the CM firmware or software shall be checked independently for reasonableness. There are four events of interest that occur:

T_0 is the time at which the first bit of a message enters the encrypting CM.

T_1 is the time at which the last bit of a message enters the encrypting CM.

T_2 is the time at which the first bit of a message exits the decrypting CM.

T_3 is the time at which the last bit of a message exits the decrypting CM.

T_r is the theoretical time to transmit the message at the test data rate with no interruption.

The overall CM latency introduced by a pair of CMs shall be defined as

$$\text{CM Latency} = T_3 - T_0 - T_r$$

Jitter shall be defined as the standard deviation of at least 100 samples of a particular latency test.

Since measured latency and jitter, as defined in Appendix H, depend on the use of flow control applied to the messages entering the encrypting CM, the calculated latency shall be reported with and without flow control enabled. If both hardware and software flow control options are present, the latency and jitter measurements for each configuration shall be reported. Flow control shall not be actively applied to the output of the decrypting module when measuring latency and jitter. The baseline measurement of latency and jitter shall use a hardwire connection between the ciphertext ports of the encrypting and decrypting CMs.

H.3.1.3.4.2 Block length probing

CMs using block algorithms distribute encapsulated data (hereafter referred to as “payload”) into blocks. The amount of payload that will fit into a block is equal to the block size minus the CM overhead for that block. The CM overhead may vary depending on the location of the block within a message. Typically, four cases characterize the cryptographic system.

- A single-block message.
- The first block of a multi-block message.
- The last block of a multi-block message.
- The middle block(s) of a message spanning three or more blocks.

For messages spanning from one to a few blocks, performance of the cryptographic system is strongly dependent on how the payload fits within the block structure. For example, if the cryptographic system can fit a maximum payload of 12 bytes into a

single-block message, a payload of 12 bytes can be transmitted in approximately half the time required for a payload of 13 bytes. It is important that the testing entity recognize these block boundaries to assess their impact on testing and/or operation with the cryptographic system. A method for identifying the block boundaries is outlined below. This method assumes a block length of 16 bytes. It can be modified for other block lengths.

Send a sequence of messages with monotonically increasing length, from 1 byte to 48 bytes. For each message, record the total time from the exit of the first bit from the data source until the arrival of the last bit at the data sink. Calculate the delta for each step change in the message length. The step change should be virtually identical within a block boundary. When the message length crosses a block boundary, the step change will increase dramatically. Subsequent step changes should be virtually identical until the next block boundary is reached. Block boundaries should occur as the payload size approaches multiples of the block size. The boundaries should be identified for messages spanning one, two, and three blocks. This information can be extrapolated to longer messages by adding middle blocks as required.

H.3.1.3.4.3 Effect of message content on latency

For a given message length, comparing the average and standard deviation of various data patterns should reveal any variation due to message content.

Calculate latency averages and standard deviations for each data pattern and message length. Test patterns can be used in place of actual native protocol messages. Following are example test patterns with bytes containing:

- All zeros.
- All 1's.
- Alternating 1's and zeros with bit zero equal to 1.
- Alternating 1's and zeros with bit zero equal to 0.
- Ascending binary count.
- Descending binary count.
- Random values.

H.3.1.3.4.4 Throughput testing

Throughput testing is used to measure the maximum sustainable rate of SCADA MPH. A large number of transaction requests will stress the CM's ability to buffer the incoming messages, encrypt the message, and buffer the encrypted message to be sent to the receiving CM.

The ciphertext header and encrypted message together are longer than the plaintext. Therefore, continuous sustained throughput is not expected. The CM should be able to buffer messages up to the desired operational rate.

H.3.1.3.4.5 Throughput measurements

Throughput in payload bits per second is expected to be dependent on message length, due to block padding and other overhead. Since it is desirable to treat the CM as a black box, ideally the throughput would be measured for every realistic message length. Measurements should be made at expected data rates to be used. If throughput testing cannot be automated and the size of the largest block is known, it should be sufficient to

measure throughput for messages up to three blocks long, with extrapolations based on the throughput of the middle block (since the first and last blocks may have special overheads). The delta time between a two-block and a three-block message (because the two-block message has first and last blocks) should be measured. Units for reporting throughput should be bits per second and messages per second. Alternatively, reporting the inverse of the throughput (seconds per message) makes it easier to compute polling intervals and also coincides with the definition of “latency” used here.

H.3.1.3.4.6 Performance test configurations

All test configurations are emulated. The same configuration should be used for response time and throughput. If field devices are distributed across different segments and interconnecting paths include slow speed links that could affect performance, these are included in the test configuration to measure their impact on throughput. If errors are detected during the test, they have to be investigated. If a problem is found, the tests shall be rerun to get relevant response-time measurements.

H.3.1.3.4.6.1 Baseline configuration

The baseline test configuration should not include CMs or any loading other than that introduced from application processors. This configuration establishes the maximum MPH over the communication path.

H.3.1.3.4.6.2 Baseline with CMs

Test configurations that include CMs will be used to measure the realized MPH over the same communication path.

H.3.1.3.4.6.3 Baseline with CMs and other loads

Test configurations that include CMs and other loading will be used to measure the realized MPH over the same communication path.

H.3.1.3.4.6.4 Degradation

Degradation shall be reported as the 1- (realized MPH divided by the maximum MPH).

H.3.1.3.4.7 Load model

Load models can be created to measure CM throughput. All CM transactions (poll request and response) should be handled from cached data. This can be done by reading the same record over and over across all application processors in the test. This allows maximum transaction load to be achieved with minimal hardware.

H.3.1.3.5 Evaluation of the effect of noise on CM performance

CMs should be tested to determine the effect of message corruption on performance.

1. On the bench, replace the null modem connecting the CMs with a device that digitally modifies the serial data passing through it. This device simulates errors resulting from communication channel noise that the modem could not ignore or correct.

2. Under appropriate traffic conditions, determine how message delivery is affected (additional latency, or no delivery altogether) by manipulation of message bits. The tests could include the introduction of a single bit error per message, multiple bit errors per message, and the introduction of an extra byte.

If the message was not delivered during step 2, determine if there is a dead period

during which messages are ignored or buffered for later transmission. The dead period should be measured by sending an additional message that is delayed a variable amount of time after the corrupted is sent.

H.3.1.3.6 Susceptibility to adverse conditions

If appropriate, the CM should be tested to determine its ability to withstand (and, perhaps, even function despite) specific environmental conditions, such as transients, discharges, RF radiation, or extremes of humidity or temperature. IEEE 1613™ describes some such tests [2].

H.3.2 Operability tests

Operability tests should be designed to perform regression testing and reliability testing, and to provide the capability to identify and isolate bottleneck problems. CM hardware and software are designed to minimize the impact on operational systems and operating procedures. IEEE 1646™ describes the delivery time performance requirements for electric power substations [3]. IEEE 1646 is used as a guide to evaluate potential degradation in operating performance and procedures introduced by the CMs.

H.3.2.1 Regression testing

Regression testing is not one test, but a series of tests that measure critical aspects of the CM under test. For each new release of CM software and hardware, regression testing ensures that the upgrade will function properly prior to deployment. A regression test plan identifies which new basic test objectives should be run against each new CM product release.

CM regression testing can verify that a hardware or software upgrade does not impact performance, reliability, or functionality of the cryptographic system. Regression testing does not measure new features or capabilities. Such tests fall under functional testing discussed in Section H.3.1.2.

Use test data from past regression test as a baseline for the current regression test. If current data do not exist, first run a test against the current cryptographic system before testing the upgrade. Without a baseline against which to compare the CM upgrade, it cannot be determined that the cryptographic system has been improved or regressed.

H.3.2.2 Reliability testing

Reliability testing forces the CM or the cryptographic system under test to handle in a compressed time the activity it normally would experience over weeks, months, or years in operation. The testing may use accelerated loading techniques to apply and maintain high load on the CM for prolonged periods of time (30 hours or more). Reliability testing attempts to accelerate failure of the CM or the cryptographic system caused by the following.

- Cumulative errors: These are the result of repeating an operation multiple times in a fashion that results in an error.
- Timing errors: These errors are caused by two time-dependent operations that occur out of sequence or without proper delay.
- Statistical errors: It is virtually impossible to test and verify every possible path through the CM's code. However, statistically, over time, every path will be traversed, either because of an error condition or a seldom-invoked sequence

of events. Reliability testing increases the probability that a statistical error will occur.

Cryptographic system reliability testing measures how well CMs maintain operation under various loads and feature configurations.

H.3.2.2.1 Test measurements

Reliability testing provides the following three key measurements.

Operational reliability: Cryptographic system operation under maximum sustained load.

Stressed reliability: Cryptographic system operation under peak load.

Reliable recovery: Time to re-establish normal cryptographic system operation after non-fatal faults (e.g., adverse environmental conditions or loss of power supply).

The first measurement, operational reliability, determines how reliable the cryptographic system is under a sustainable load in which virtually all received messages are forwarded correctly to the destination. The second measurement, stressed reliability, determines how stable the cryptographic system is under peak loads. Operational reliability requires the cryptographic system to be stable for a long time at medium to heavy loads. Under stressed reliability, cryptographic systems can almost always be forced to fail; it is the mode of failure and recovery (e.g., fail-safe) that are important. Typical results could show:

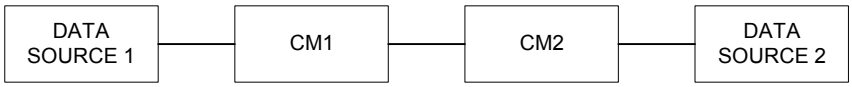
- The cryptographic system cannot maintain the sustained load for long periods.
- The cryptographic system can maintain sustained loads, but fails under peak loads.
- The cryptographic system can maintain both sustained and peak loads.
- The cryptographic system encounters noncritical or recoverable errors under one or both loads.
- The cryptographic system encounters fatal errors under sustained loads.

H.3.2.2.2 Test configurations

All test configurations are emulated. The test configurations should represent the most critical or typical operational communication configurations, including point-to-point, multidrop, and networked.

Testing should be divided into two configurations in which the line connecting the two CMs may be implemented as either a dedicated link or a shared link, such as Ethernet:

- Unidirectional testing consists of a continuous stream of messages applied to one CM. In the diagram below, DATA SOURCE is configured to send one message after another without intervening delay beyond the minimum inherent in the test system. DATA SINK is configured to collect statistics, but not to respond to the messages.
- Bidirectional testing consists of a continuous sequence of message pairs, with a message from DATA SOURCE 1 immediately followed by a message from DATA SOURCE 2, without intervening delay. The cycle is repeated when DATA SOURCE 1 sends its message again (or a different message) immediately after receiving the message from DATA SOURCE 2, again without intervening delay.



H.3.2.2.3 Load model

The reliability test load model can be developed from either the operational communication network baseline or from throughput test results.

H.3.2.2.3.1 Throughput load model

If one use uses the throughput load model, reliability-testing measures the cryptographic system relative to the sustained and maximum throughput based on throughput test results. It is a more conservative measurement than that used for the baseline load model and automatically factors in communication network traffic growth.

As throughput tests measure cryptographic system capacity, this test effectively measures “stress capacity.” Operational and peak loads are from the baseline load model results. Sustained and maximum throughput is from the throughput model results. The difference indicates the capacity of the cryptographic system to reliably handle additional load.

This is the preferred method of reliability testing. If the cryptographic system fails this test, it can be re-tested using the baseline load model to determine if it can handle existing communication network traffic. This testing provides a margin of comfort that the baseline modeling does not. Another advantage of using this model is that the load scripts can be reused from throughput testing.

H.3.2.2.3.2 Load modeling bursty traffic

During a reliability test, the loading should not be constant, but bursty, as is typical of most communication network transmissions. This can be done using the following two techniques.

- Create a load script that varies the number of messages forwarded from the source to the destination.
- Vary the MPH rate or number of load generators running concurrently.

Make sure that when using bursty traffic, the average MPH rate measured over a specified time increment is equal to the load model average and peak MPH rates for operational and stressed reliability, respectively.

H.3.2.2.3.3 Baseline load model

If one uses the baseline load model, reliability testing measures the reliability of the cryptographic system under test relative to the current operational system loading. It tells how the cryptographic system will work, if there are no changes in the operational communication network traffic or load. If throughput testing hasn’t been conducted on the cryptographic system, this is the best load model to use.

- DATA
- SOURCE
- CM1
- CM2
- DATA SINK

H.3.2.3 Bottleneck identification and problem isolation

The addition of cryptographic protection has the potential for creating a bottleneck in SCADA communications. To determine whether a bottleneck may exist, refer to the manufacturer's specification of the maximum sustained throughput for each component through which the data travel. It may be necessary to convert or interpret the specifications to derive a common measure (such as bits per second) for all of the components. If the full data stream passes through a CM and it has the lowest rated throughput, it represents a theoretical bottleneck.

In reality, a component is a bottleneck only if it impedes operation. A component may be capable of operating at a peak rate adequate to meet the requirements of the SCADA system, or the SCADA system may not exercise the full system throughput capability. For the cryptographic system, this can be determined by operating the SCADA system under worst-case conditions both with and without the cryptographic system and comparing the results.

In some cases, when the cryptographic system creates a bottleneck, the problem can be alleviated using configuration options. For example, the interface between a CM and its associated computer (the plaintext port) may be capable of operating at a substantially higher speed than the communication link (on the ciphertext port). This type of asymmetric operation can dramatically reduce delays associated with filling and emptying the CM buffers.

H.4 Interoperability testing

Interoperability testing requires a test configuration (point-to-point, series, series star, and multidrop — see Appendix C and Appendix D) with CMs from different vendors or different CM versions from the same vendor. Application feature/functional testing described in Section H.3.1.2 should be run with this configuration.

H.5 Special test setup requirements

Test setup to determine appropriate values for SCADA communication parameters affected by the addition of cryptographic protection is described in general, and in terms of unique requirements for specific native protocols.

H.5.1 Communication channel considerations

Communication channel parameters are described in terms of general considerations and key channel characteristics.

H.5.1.1 General considerations

To test the effects of CM security on communication channels, it may be necessary to adjust some of the channel timing parameters in the sender, receiver or both. SCADA channel parameters often are customized to suit the specific requirements of the channel. Changes could be required that affect time-out, channel turn-on, turn-off, turn around, and squelch times. Channel characteristics may be altered significantly by timing changes made to accommodate CM security. Changes should be recorded as part of the test documents.

H.5.1.2 Key channel characteristics

Some field devices respond to requests faster than others. Typical RTUs are ready to

begin a response within a few milliseconds. However, communication channel equipment may introduce additional delay. For example, it is common practice to key up a radio transmitter or wire line, wait for the receiver to open, and wait for the path to settle down before the response begins. This sometimes is referred to as the PT mark. The receiver, to synchronize to the serial channel, also uses the PT mark. PT marks often are set at 8 ms, but can be as long as 50 ms, maybe longer when an MAS repeater is used, for example, on a 900 MHz radio channel.

At the end of the message, there often is a need to hold the channel at mark for a short period of time so the receiver can decide the message has ended. This is sometimes referred to as the "post mark." Post marks typically have delays based on the time to send two bytes of data, some even longer.

Radios (MAS[34] and spread spectrum) need long PT marks and post marks. They also need time for the slave radio to go from transmit to receive and back again.

H.5.2 Modbus time-out parameter assignment

Modbus is a poll-response data communications protocol that defines "no response" as a valid response. Therefore, time-out is an issue relevant to Modbus [14] [15].

One master on a channel polls one or more remote devices on that channel. If the protocol requires a response to a particular poll, at most one remote will send the required response back to the master. If a remote detects a master poll that has been corrupted, the remote will not respond. Therefore, the master shall be configured to assume that an error has occurred if an expected response is not received within a predetermined time. This time will depend on a number of factors, including channel data rate, type of poll, and the processor speed of the remotes.

A single master time-out parameter often is set based on the longest response delay that the master will encounter on the channel. If this parameter is set too short, the master will stop listening too soon and some remote responses will be missed. If it is set too long, the master will be forced to wait longer than necessary every time noise corrupts a poll and reduces the channel scan rate. A simple trial-and-error approach can be used to find the smallest master time-out parameter that avoids missed remote responses on a channel.

During a bench test of maximum throughput in a noiseless environment, there should be a one-for-one poll-response relationship. Therefore, the master time-out parameter can simply be set to a large value for the duration of the test.

If a cryptographic system is inserted between the master and the remotes on a channel, the poll-response delay characteristics may change. Accordingly, a new master time-out parameter should be determined after insertion.

The time-out parameter used during a test should be documented as part of the test environment.

---

[34] These are usually 900 MHz radio, which are very common on electric power distribution feeder applications and water distribution systems. Some are being replaced with spread spectrum radios that do not require FCC licensing.

H.6 Test reports

Test reports are described to state clearly who has ownership of the test and evaluation results, and to describe the template for a standard report format.

H.6.1 Ownership of test results

Ownership is a matter to be negotiated between the manufacturer and the certifier.

H.6.2 Standard report format

Feature/functionality test results related to a specific test procedure will be reported as not supported, not applicable, pass, or fail with optional qualifying remarks.

Performance and operability test results related to a specific test procedure will be reported in terms of measured results, statistical significance measures, and optional qualifying remarks.

H.7 Test architecture and environment

Test architecture that identifies clearly the components classified as the DUT or SUT, and the components classified as the “test environment” shall be specified in the test procedures.

Test environment describes equipment, software, and documentation provided by the vendor and by the test facility. Engineering test platforms for test management and IED emulation needed to support the tests also will be described.

Form for Suggestion to Change

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

Send to: **Operating Section**
American Gas Association
400 North Capitol St., N.W., 4th Floor
Washington, DC 20001
U.S.A.
Fax: (202) 824-7082

Name:_____

Company:_____

Address:_____

Phone: _____ **Fax:**_____**E-mail:**_____

Please Indicate Organization Represented (if any):_____

1. Section/Paragraph :_____

2. Proposal Recommends: (check one): ☐ **new text** ☐ **revised text** ☐ **deleted text**

3. Proposal (include proposed new or revised wording, or identification of wording to be deleted; use separate sheet if needed): [Proposed text should be in legislative format; i.e., use underscore to denote wording to be inserted (inserted wording) and strike-through to denote wording to be deleted (~~deleted wording~~).]

4. Statement of Problem and Substantiation for Proposal (use separate sheet if needed): (State the problem that will be resolved by your recommendation; give the specific reason for your proposal including copies of tests, research papers, etc.)

5. ☐ **This proposal is original material.** (Note: Original material is considered to be the submitter's own idea based on or as a result of his/her own experience, thought or research and, to the best of his/her knowledge, is not copied from another source.)

☐ **This proposal is not original material; its source (if known) is as follows:** _____

_____

Type or print legibly. If supplementary material (photographs, diagrams, reports, etc.) is included, you may be required to submit sufficient copies for all members of reviewing committees or task forces.

I hereby grant the American Gas Association the non-exclusive, royalty-free rights, including non-exclusive, royalty-free rights in copyright, in this proposal and I understand that I acquire no rights in any publication of the American Gas Association in which this proposal in this or another similar or analogous form is used.

Date: _____ Signature (Required) _____

FOR OFFICE USE ONLY

Log # _____