

IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

IEEE Power & Energy Society

Sponsored by the
Substations Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1711™-2010

15 February 2011

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

*"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.



Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24, 2026 at 23:34:53 UTC from IEEE Xplore. Restrictions apply.

Full document details: [IEEE 1711-2010](#)

IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

Sponsor

Substations Committee
of the
IEEE Power & Energy Society

Approved 9 November 2010

IEEE-SA Standards Board

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

Abstract: A cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of serial links is defined in this trial use standard. Specific applications or hardware implementations are not addressed, and the standard is independent of the underlying communications protocol.

Keywords: cyber security, encryption, IEEE 1711, integrity, serial link

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.
Published 15 February 2011. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-6501-1 STD96084
Print: ISBN 978-0-7381-6502-8 STDPD96084

IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

*"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS.**”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

*“Withdrawn” standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Introduction

This introduction is not part of IEEE Std 1711-2010, IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

This trial use standard defines a cryptographic protocol called Serial SCADA Protection Protocol (SSPP) to provide integrity, and optionally confidentiality, for cyber security of substation serial links. It focuses exclusively on “formatting bits on the wire” to provide cryptographic assurance of cyber security properties. It does not address specific applications or hardware implementations and is largely independent of the underlying communications channel and application or SCADA protocol. The requirements of this standard are in addition to any requirements contained in standards for individual devices in which this protocol is implemented.

SSPP operates by encapsulating each SCADA or application message in a cryptographic envelope that adds minimal overhead to the message. This encapsulation is performed in a manner that is largely independent of the underlying communications protocol. While SSPP was originally designed to protect serial SCADA communications, its domain of application is not limited to SCADA. SSPP can also be used to protect other types of serial communications, such as data concentrator links, load management links, dial-in revenue meter reading, dial-in maintenance connections, etc.

SSPP is designed for systems or applications in the following circumstances:

- Traffic is message-oriented, with messages consisting of contiguous sequences of 7-bit or 8-bit characters, in lengths ranging from a few characters to a few hundred characters.
- The communications channel may be either half-duplex or full-duplex.
- Messages are never reordered by the communications channel.
- Messages are never fragmented by the communications channel.
- The communications topology is point-to-point, point-to-multipoint, or broadcast.
- For point-to-multipoint topologies, messages include an identifying address of the receiver in the header of the message.
- Transmission speeds may be slow enough that cryptographic protocol overhead in the form of too many additional header, trailer, or framing characters may significantly impact message latency and roundtrip message delivery times.
- Message integrity is critical to reliable system operation, and system operation may be adversely impacted if messages are modified, forged, spliced, reordered, or replayed.
- The system or application is able to tolerate lost messages.

SSPP assures message integrity by detecting modified, forged, spliced, reordered, or replayed messages and discarding them. Applications such as SCADA systems are designed to accommodate accidental communications errors and, through timeouts, detects and retries lost or damaged messages. Such applications thereby recover from messages discarded by SSPP in the same way as they recover from messages lost or damaged by communications errors. Applications such as dial-in remote maintenance involve a live operator who can reissue commands whose action or response is discarded by SSPP.

SSPP is designed to support point-to-point links, point-to-multi-point (or multi-drop) links, and broadcast links. For multi-drop links and broadcast links, SSPP supports mixed-mode operation, where some of the stations use SSPP to achieve protected communications, and other stations communicate in the clear. Mixed-mode operation allows for phased or incremental deployment of devices providing SSPP protection so that all stations on a multi-drop or broadcast link do not have to be upgraded simultaneously. SSPP protection can be deployed at the master station first, then incrementally added to slave stations as needed.

information. All amendments or corrigenda associated with this standard have also been withdrawn.

SSPP may be implemented in standalone security devices, integrated in communications modems, or embedded in applications or systems. When implemented in standalone bump-in-the-wire security devices, SSPP may be used to retrofit protection of legacy serial systems with little or no modification of existing systems and equipment. Figure a illustrates a typical deployment of SSPP implemented with a multi-channel Ethernet-to-Serial SSPP gateway in the control center and SSPP bump-in-the-wire (BITW) devices in the substations.

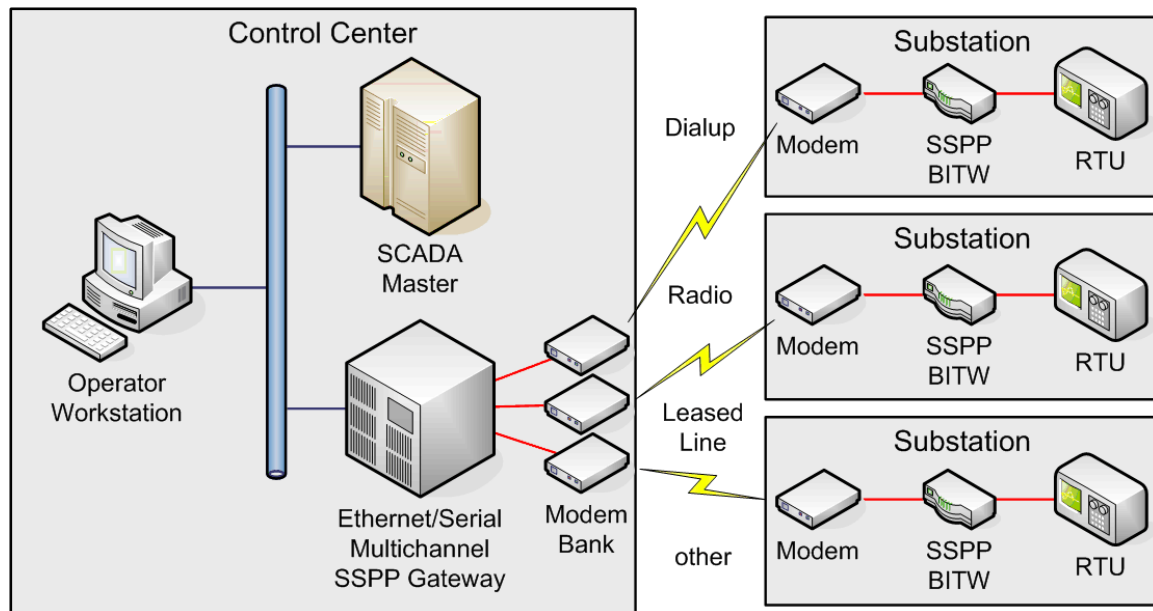


Figure a—Retrofit bump-in-the-wire SSPP deployment

Key management for the long-term cryptographic keys used by SSPP is specifically not addressed in this standard. Key management is a complex issue, and including key management would significantly increase the size and complexity of the standard. But more significantly, key management for SSPP keys is not markedly different from key management for other cryptographic systems. Including a specific mechanism for key management in SSPP could preclude integration with existing commercial key management systems and inhibit adoption of SSPP in products. It is expected that key management systems for SSPP keys follow good security practices, and the quality, flexibility, and usability of such systems should be evaluated by prospective purchasers of SSPP implementations.

Goals

This standard has several goals.

Designing cryptographic algorithms and protocols that operate correctly and are free of undiscovered flaws is difficult at best. There is general agreement in the cryptography community that openly published and time-tested cryptographic algorithms and protocols are less likely to contain security flaws than secretly developed ones because their publication enables scrutiny by the entire community. Historically, proprietary and secret protocols have frequently been found to contain flaws when their designs become public. However, well-known and time-tested protocols such as TLS and SSH that are designed for high-speed IP networks add too much overhead when used on slow serial communications links. There are no suitable cryptographic protocols for protecting the integrity of asynchronous serial communications of a SCADA-like nature. By defining such a protocol that can be used with a wide variety of systems and

Withdrawn standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

application protocols, this standard aims to help manufacturers build secure systems, products, and applications, and avoid the pitfalls of proprietary and secret cryptographic designs.

By utilizing a common framework, different implementations of this protocol built by different vendors may be able to interoperate. Adherence to this standard is by no means a guarantee of interoperability, but this standard does provide a significant step toward interoperable implementations. Interoperability can foster competition and lead to more and better choices for end users. Interoperability can also simplify merging diverse operational infrastructures, such as can occur when two utilities merge. Finally, interoperability can provide opportunities for alternative support or migration from one vendor's equipment to another.

Systems operators may use this specification in procurement requirements to gain some assurance that products are well-designed and secure. Without a specification of this nature, most utilities do not have the expertise to evaluate cryptographic designs.

Security and control systems manufacturers will build products only if they perceive a viable market. This standard has the potential to create a market for serial communications protection products.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this trial-use standard may require use of subject matter covered by patent rights. By publication of this trial-use standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this trial-use standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Trial use

Publication of this trial-use standard for comment and criticism has been approved by the Institute of Electrical and Electronics Engineers. Trial-use standards are effective for 24 months from the date of publication. Comments for revision will be accepted for 18 months after publication. Suggestions for revision should be directed to the Secretary, IEEE-SA Standards Board, 445 Hoes Lane, Piscataway, NJ 08854, and should be received no later than 15 August 2012. It is expected that following the 24-month period, this trial-use standard, revised as necessary, shall be submitted to the IEEE-SA Standards Board for approval as a full-use standard.

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

Participants

At the time this trial-use standard was submitted to the IEEE-SA Standards Board for approval, the Cryptographic Protocol for Cyber Security of Substation Serial Links Working Group had the following membership:

David Whitehead, *Chair*
Andrew Wright, *Vice Chair*

Mason Clark
Mike Dood
Dennis Holstein

Marc Lacroix
Craig Preuss
Sam Sciacca

Lee Smith
John Tengdin
Tim Tibbals

The following members of the individual balloting committee voted on this trial-use standard. Balloters may have voted for approval, disapproval, or abstention.

William J. Ackerman
Terrence Burns
Arvind K. Chaudhary
Stephen Conrad
Ratan Das
Gary Donner
Michael Dood
Randall Dotson
Neal Dowling
Sourav Dutta
Gary Engmann
Kenneth Fodero
Frank Gerleve
Grant Gilchrist
Ron Greenthaler
Randall Groves
Adolfo Gutierrez
David Harris
John Hawkins
Gary Heuston
Dennis Holstein

C. Huntley
R. Jackson
Piotr Karocki
Yuri Khersonsky
J. Koepfinger
Jim Kulchisky
Marc Lacroix
Chung-Yiu Lam
John McDonald
Jerry Murphy
R. Murphy
Bruce Muschlitz
Michael S. Newman
Nick S. A. Nikjoo
Satoshi Obara
Chris Osterloh
Craig Preuss
Jose Puthenkulam
Michael Roberts
Charles Rogers
Anne-Marie Sahazizian

Miriam Sanders
Steven Sano
Bartien Sayogo
Samuel Sciacca
Hamidreza Sharifnia
Devki Sharma
Gil Shultz
Mark Simon
James Smith
Gary Stoedter
Walter Struppler
Michael Swearingen
William Taylor
John Tengdin
David Tepen
Joe Uchiyama
Eric Udren
John Vergis
Ilia Voloh
David Whitehead
Andrew Wright

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

When the IEEE-SA Standards Board approved this trial-use standard on 9 November 2010, it had the following membership:

Robert M. Grow, *Chair*
Richard H. Hulett, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Karen Bartleson
Victor Berman
Ted Burse
Clint Chaplin
Andy Drozd
Alexander Gelman
Jim Hughes

Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Hung Ling
Oleg Logvinov
Ted Olsen

Ronald C. Petersen
Thomas Prevost
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Julie Alessi
IEEE Standards Program Manager, Document Development

Soo H. Kim
IEEE Standards Program Manager, Technical Program Development

"Withdrawn" standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

Withdrawn Standard*

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
2. Normative references.....	2
3. Definitions, acronyms, and abbreviations	2
3.1 Definitions	2
3.2 Acronyms and abbreviations	3
4. Substation Serial Protection Protocol (SSPP).....	4
4.1 Protocol overview	4
4.2 SSPP organizational layers	6
4.3 Octet order in SSPP messages	6
4.4 Session layer.....	6
4.5 Transport layer.....	17
4.6 Link layer.....	18
4.7 Cipher suites	23
4.8 SSPP management messages	28
Annex A (informative) Background.....	30
A.1 Overview	30
Annex B (informative) Implementation considerations	31
B.1 Link layer mixed-mode operation.....	31
B.2 Hardware handshaking.....	31
B.3 Dialup modem interaction.....	33
B.4 Timing consideration for shared connections	34
B.5 Design consideration for cipher suites	35
B.6 Side channel design considerations.....	35
B.7 Session clock considerations.....	35
B.8 Broadcast sessions	35
Annex C (informative) Bibliography.....	37

*“Withdrawn” standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

IMPORTANT NOTICE: *This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This trial use standard defines a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links. It does not address specific applications or hardware implementations, and is independent of the underlying communications protocol.

1.2 Purpose

The elevated concern of cyber security throughout the power industry has created a need to protect communications to and from substations. This trial use standard defines a cryptographic protocol known as Substation Serial Protection Protocol (SSPP) that can protect the integrity and optional confidentiality of asynchronous serial communications typically used by substation equipment. SSPP is primarily intended to protect serial SCADA communications, but can be applied to other serial communications – such as the maintenance ports of IEDs. SSPP is largely independent of the underlying communications link and protocol (e.g. Modbus, DNP3), and is appropriate for serial communications over leased lines, dial-up lines, multi-drop links radio, power line carrier, fiber optic, etc. SSPP is suitable for implementation in new equipment or for deployment in bump-in-the-wire devices retrofitting protection to existing systems.

*“Withdrawn” standards are standards that are no longer useful or contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., each is to be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

FIPS PUB 180-3: Secure Hash Standard, National Institute of Standards and Technology.¹

FIPS PUB 197: Advanced Encryption Standard, National Institute of Standards and Technology.

FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC) Standard, National Institute of Standards and Technology.

NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology.²

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this trial-use standard, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be consulted for terms not defined in this clause.³

character: A 7-bit or 8-bit value transmitted on a serial communications channel.

cipher suite: A set of cryptographic algorithms, keys, and parameters identified by a cipher suite number.

ciphertext: Message data that is encrypted.

cleartext: Message data that is not encrypted.

confidentiality: Refers to the secrecy of a message.

integrity: Refers to the validity of a message.

mixed mode: In a multi-drop topology, some messages are allowed to be delivered in cleartext without SSPP protection, while other messages are protected using SSPP.

octet: An 8-bit value.

Position Embedding (PE) mode: A cryptographic mode designed by members of the AGA 12 committee specifically for low latency integrity protection in bump-in-the-wire deployments. It is used by one of the cipher suites.

NOTE—See Os vik, D., Shamir, A., and Tromer, E. [B4] for the rationale behind the design of this mode. Note that PE mode as used here includes an additional output whitening step over the description in [B4].⁴

¹ FIPS publications are available by mail from the National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312 (<http://www.ntis.org/>).

² <http://www.nist.gov/index.html>

³ *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>, or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.

sequence number: An unsigned number carried in the header of all messages. Sequence numbers are used to prevent replay attacks.

session: A (usually) bidirectional virtual communications channel established between two SSPP peers. There may be more than one session established between the same two peers.

session identifier: A value between 1 and 255 used to distinguish different types of bidirectional traffic flows between two SSPP peers.

Substation Serial Protection Protocol (SSPP) address: A 16-bit number that identifies a particular SSPP peer. Every SSPP peer on a shared communications link shall have a unique SSPP address. The address 0xFFFF is a reserved broadcast address. The address 0x0000 is considered invalid.

Substation Serial Protection Protocol (SSPP) peer (or simply **peer**): A device or application implementing SSPP.

whitening: A process of XORing some key material into the input or output of a block cipher.

3.2 Acronyms and abbreviations

AES	Advanced Encryption System
BITW	Bump In The Wire
CRC	Cyclic Redundancy Check
HMAC	Keyed-Hash Message Authentication Code
IED	Intelligent Electronic Device
SCADA	Supervisory Control and Data Acquisition
SSPP	Substation Serial Protection Protocol

⁴ The numbers in brackets correspond to those in the bibliography in Annex C. contain significant obsolete or erroneous information. All amendments or corrigenda associated with this standard have also been withdrawn.