



# IEEE Standard for Secure SCADA Communications Protocol (SSCP)

IEEE Power and Energy Society

Developed by the  
Power System Communications and Cybersecurity Committee

IEEE Std 1711.2™-2019

# IEEE Standard for Secure SCADA Communications Protocol (SSCP)

Developed by the

**Power System Communications and Cybersecurity Committee**  
of the  
**IEEE Power and Energy Society**

Approved 7 November 2019

**IEEE SA Standards Board**

**Abstract:** A cryptographic protocol to provide integrity with optional confidentiality for cyber security of substation serial links is defined in this standard. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol. The elevated concern of cyber security throughout the power industry has created a need to protect communications to and from substations. This standard defines a cryptographic protocol known as Secure SCADA Communications Protocol (SSCP) that protects the integrity and, optionally, the confidentiality of asynchronous serial communications typically used by control system equipment. SSCP is primarily intended to protect serial SCADA communications, but can be applied to other serial communications, such as the maintenance ports of intelligent electronic devices. SSCP is independent of the underlying communications link and protocol (e.g., Modbus, DNP3, IEC 60870-5), and is appropriate for serial communications over leased lines, dial-up lines, multi-drop links, radio, power line carrier, fiber optic, etc. SSCP is suitable for implementation in new equipment or for deployment in bump-in-the-wire devices retrofitting protection to existing systems.

**Keywords:** communications protocol, confidentiality, cryptography, data acquisitions, IEEE 1711.2™, integrity, SCADA, secure communications, SSCP, supervisory control

---

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

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 21 January 2020. 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 978-1-5044-6313-3      STD23982  
Print: ISBN 978-1-5044-6314-0      STDPD23982

*IEEE prohibits discrimination, harassment, and bullying.  
For more information, visit <https://www.ieee.org/about/corporate/governance/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.*

## **Important Notices and Disclaimers Concerning IEEE Standards Documents**

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/ipr/disclaimers.html>.

### **Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents**

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, 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.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own 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.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

## **Translations**

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

## **Official statements**

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of 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 of IEEE.

## **Comments on standards**

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

## **Laws and regulations**

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document 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**

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted 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 these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

## Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, 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.

## Updating of IEEE Standards documents

Users of IEEE Standards documents 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.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, 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 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 IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

## Errata

Errata, if any, for IEEE standards can be accessed via <https://standards.ieee.org/standard/index.html>. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore: <https://ieeexplore.ieee.org/browse/standards/collection/ieee/>. Users are encouraged to periodically check for errata.

## Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. 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 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.

## Participants

At the time this IEEE standard was completed, the SSCP S4 Working Group had the following membership:

**Scott Mix, *Chair***  
**Mark Hadley, *Vice Chair***

Farel Becker	James Formea	Marc Lacroix
Ed Cenzone	Craig Goranson	Theo Laughner
Rich Corrigan	Chris Huntley	Rick Liposchak
Mike Dood	Dylan Jenkins	Dan Nordell
Thomas Edgar	Steve Kunsman	Craig Preuss

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman	Werner Hoelzl	Bansi Patel
Ali Al Awazi	Gary Hoffman	Pathik Patel
Johann Amsenga	Dennis Holstein	Dev Paul
Philip Beaumont	Noriyuki Ikeuchi	Bogdan Popescu
Derek Brown	Dmitry Ishchenko	Lakshman Raut
Gustavo Brunello	Atsushi Ito	Charles Rogers
Demetrio Bucaneg Jr.	Richard Jackson	Daniel Sabin
Stephen Bush	Raj Jain	Bartien Sayogo
Paul Cardinal	Anthony Johnson	Thomas Schossig
Ratan Das	Innocent Kamwa	Stephen Schwarm
Mike Dood	Piotr Karocki	Robert Seitz
Richard Doyle	Peter Kelly	Veselin Skendzic
Kevin Easley	Stuart Kerry	Thomas Starai
Thomas Edgar	Tanuj Khandelwal	Marcus Steel
Jiyuan Fan	Yongbum Kim	Scott Sternfeld
Ronald Farquharson	Jim Kulchisky	Walter Struppler
James Formea	Steve Kunsman	Gary Stuebing
Dan Friedman	Ronald Landheer-	David Tepen
Jean-Sebastien Gagnon	Cieslak	Michael Thesing
Gregory Gillooly	Robert Landman	Mark-Rene Uchida
Jalal Gohari	Scott Mix	James Van De Ligt
Keith Gray	William Munn	Srinivasa Vemuru
Randall Groves	R. Murphy	John Vergis
Mark Hadley	Arthur Neubauer	Jane Verner
Victoria Hailey	Michael Newman	Jian Yu
Randy Hamilton	Nick S. A. Nikjoo	Oren Yuen
Marco Hernandez		Janusz Zalewski

When the IEEE SA Standards Board approved this standard on 7 November 2019, it had the following membership:

**Gary Hoffman, *Chair***  
**Ted Burse, *Vice Chair***  
**Jean-Philippe Faure, *Past Chair***  
**Konstantinos Karachalios, *Secretary***

Masayuki Ariyoshi	Christel Hunter	David J. Law
Stephen D. Dukes	Joseph L. Koepfinger*	Joseph Levy
J. Travis Griffith	Thomas Koshy	Howard Li
Guido Hiertz	John D. Kulick	Xiaohui Liu

Kevin Lu  
Daleep Mohla  
Andrew Myles  
Annette D. Reilly

Dorothy Stanley  
Sha Wei  
Phil Wennblom

Philip Winston  
Howard Wolfman  
Feng Wu  
Jingyi Zhou

\*Member Emeritus

## Introduction

This introduction is not part of IEEE Std 1711.2–2019, IEEE Standard for Secure SCADA Communications Protocol (SSCP).

Pacific Northwest National Laboratory (PNNL) developed the Secure SCADA Communications Protocol, abbreviated SSCP, over the course of several years beginning in 2004. The original funding source was the National Center for Advanced Secure Systems Research program of the Office of Naval Research. Subsequent funding from the National SCADA Test Bed Program (now referred to as Cybersecurity for Energy Delivery Systems) at the Department of Energy allowed PNNL to mature the technology. Through the Hallmark project, Schweitzer Engineering Laboratories developed multiple products containing the SSCP.

PNNL staff formed an advisory board of industry experts to help ensure the SSCP design met expectations. Per the advisory board, the two primary design requirements were to provide message integrity and to help ensure the original message was not modified. By focusing on these goals, the PNNL team created a protocol that helped ensure the message has not been modified in transit, and also supported the operational need to monitor communication in support of availability. The SSCP also differs from other IEEE 1711 protocols in two significant ways. First, the SSCP does not contain a time requirement. This design choice supports those devices that may not include a clock. Second, for security purposes, the SSCP does not support broadcast communication.

This document provides a unified description of the protocol to facilitate consistent and interoperable implementations.

## Contents

1. Overview .....	10
1.1 Scope .....	10
1.2 Conventions .....	10
1.3 Word usage .....	10
2. Normative references .....	11
3. Definitions, acronyms, and abbreviations .....	12
3.1 Definitions .....	12
3.2 Acronyms and abbreviations .....	13
4. SSCP frame structures .....	13
4.1 Frame headers .....	13
4.2 Session establish request frame .....	15
4.3 Authentication challenge frame .....	15
4.4 Authentication response frame .....	15
4.5 Key exchange frame .....	16
4.6 Data frames .....	22
4.7 Close frame .....	26
5. State information .....	26
5.1 State definitions .....	26
5.2 Messages .....	26
6. SSCP frame validation .....	31
6.1 Cryptographic key material .....	31
6.2 Addressing .....	32
6.3 Field validation .....	32
6.4 Sequence numbering .....	32
6.5 Hashed Message Authentication Code (HMAC) .....	33
6.6 Authentication response RCV .....	33
6.7 Cryptographic algorithm .....	33
6.8 Key exchange timeout .....	33
6.9 Status reporting interval .....	34
Annex A (informative) Bibliography .....	35

# IEEE Standard for Secure SCADA Communications Protocol (SSCP)

## 1. Overview

This document provides a unified description of the protocol to facilitate consistent and interoperable implementations of the Secure SCADA Communications Protocol, abbreviated SSCP. The IEEE 1711.2 working group evaluated the original SSCP specification, replacing deprecated cryptographic algorithms and improving the security of the session negotiation process.

### 1.1 Scope

This standard defines the Secure SCADA Communications Protocol (SSCP), a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links communications without broadcast message support and without any time requirements. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol.

### 1.2 Conventions

“0x” indicates a hexadecimal value, and all other values not specified to be hexadecimal are decimal (base-10). For example, the hexadecimal number 0x41 is equal to the decimal value 65.

Items written in SMALL CAPS refer to the octets corresponding to a field in a physical message. For example, SYNC TOKEN refers to the first two octets of a message, containing the synchronization octets 0x16 and 0x75.

All fields are network ordered (big Endian) in design and shall be transmitted in this order. The most significant octets of a multi-octet field shall be delivered first.

### 1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (shall equals is required to).<sup>1,2</sup>

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (should equals is recommended that).

---

<sup>1</sup>The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

<sup>2</sup>The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.