BS EN IEC 62351-6:2020

BSI Standards Publication

Power systems management and associated information exchange — Data and communications security

Part 6: Security for IEC 61850

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

National foreword

This British Standard is the UK implementation of EN IEC 62351-6:2020. It is identical to IEC 62351-6:2020. It supersedes DD IEC/TS 62351-6:2007, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/57, Power systems management and associated information exchange.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 02198 1

ICS 33.200

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN IEC 62351-6

December 2020

ICS 33.200

English Version

Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850 (IEC 62351-6:2020)

Gestion des systèmes de puissance et échanges d'informations associés - Sécurité des communications et des données - Partie 6: Sécurité pour l'IEC 61850 (IEC 62351-6:2020)

Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 6: Sicherheit für IEC 61850 (IEC 62351-6:2020)

This European Standard was approved by CENELEC on 2020-11-24. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62351-6:2020 E

AVA Documents Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

European foreword

The text of document 57/2234/FDIS, future edition 1 of IEC 62351-6, prepared by IEC/TC 57 "Power systems management and associated information exchange" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62351-6:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-08-24
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-11-24

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62351-6:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 62351-3 NOTE Harmonized as EN 62351-3

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 61850-6	-	Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs	EN 61850-6	-
IEC 61850-7-3	-	Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes	EN 61850-7-3	-
IEC 61850-8-1	-	Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3	EN 61850-8-1	-
IEC 61850-8-2	-	Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)	EN IEC 61850-8-2	-
IEC 61850-9-2	-	Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3	EN 61850-9-2	-
IEC/TS 62351-1	-	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues	-	-

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

Publication	Year	Title	EN/HD	Year
IEC/TS 62351-2	-	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms	-	-
IEC 62351-4	2020	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives	-	-
IEC 62351-9	-	Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment	EN 62351-9	-
ISO/IEC 13239	-	Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures	-	-
ISO/IEC 9594-8 | Rec. ITU-T X.509	-	Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks	-	-
RFC 2104	-	HMAC: Keyed-Hashing for Message Authentication	-	-
RFC 5905[1]	-	Network Time Protocol Version 4: Protocol and Algorithms Specification	-	-
RFC 8052	-	Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services	-	-
NIST SP 800-38D	-	Recommendation for Block Cipher Modes of Operation - Galois/Counter Mode (GCM) and GMAC	-	-

[1] Restricted to SNTP profile only.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

CONTENTS

FOREWORD 4
1 Scope and object 6
1.1 Scope 6
1.2 Namespace name and version 6
1.3 Code Component distribution 7
2 Normative references 7
3 Terms, definitions and abbreviated terms 8
3.1 Terms and definitions 8
3.2 Abbreviated terms 8
4 Security issues addressed by this document 9
4.1 Operational issues affecting choice of security options 9
4.2 Security threats countered 9
4.3 Attack methods countered 9
5 Correlation of IEC 61850 parts and IEC 62351 parts 9
5.1 General 9
5.2 IEC 61850-8-1 Profile for Client/Server communications 10
5.2.1 General 10
5.2.2 Control centre to substation 11
5.2.3 Substation communications 11
5.3 IEC 61850 security for profiles using VLAN IDs 11
5.4 IEC 61850-8-2 for Client/Server communications 11
5.5 Using OriginatorID for Client/Server Services 11
6 Multicast Association Protocols 12
6.1 General 12
6.2 Replay Protection 12
6.2.1 GOOSE replay protection 12
6.2.2 Sampled Value replay protection 16
7 Security for SNTP 19
8 Layer 2 security for profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 Sampled Value 20
8.1 Overview of Ethertype (informative) 20
8.2 Extended PDU 20
8.2.1 General format of extended PDU 20
8.2.2 Format of extension octets 21
9 Substation configuration language extensions 25
9.1 Service capability 25
9.1.1 Access Point support security for GOOSE Publisher 25
9.1.2 Access Point support security for SV Publisher 25
9.1.3 Acces Point support security for GOOSE and SMV subscriber 25
9.1.4 Server Access Point support security for TPAA 26
9.1.5 Client Access Point support security for TPAA 26
9.2 Publish with security enabled 26
9.2.1 GOOSE 26
9.2.2 SMV 26
9.2.3 Key Policy and Management 27
9.3 Use of Simulation 27

AVA Documents
Document Sharing Hub
Full document details: BS EN IEC 62351-6:2020

10 Extension of LGOS and LSVS 27
11 Conformance 27
11.1 General conformance 27
11.2 Conformance for implementations claiming IEC 61850-8-1 ISO 9506 profile security 28
11.2.1 General 28
11.2.2 IEC 62351-4 TLS Conformity for ISO-9506 Client/Server Profile using ACSE Authentication 29
11.3 Conformance for implementations claiming VLAN profile security 29
11.4 Conformance for implementations claiming SNTP profile security 32
Bibliography 33

Figure 1 – MMS Security Profiles 10
Figure 2 – Replay Protection State Machine for GOOSE 13
Figure 3 – Replay Protection State Machine for SV 17
Figure 4 – General format of extended PDU 20
Figure 5 – Definition of Reserved 1 20
Figure 6 – Calculated MAC Domain 22
Figure 7 – AES-GCM application on the example of a L2 GOOSE/SV packet. 23

Table 1 – Scope of application to standards 6
Table 2 – Extract from IEC 61850-9-2 (Informative) 16
Table 3 – Extension of the LGOS class 27
Table 4 – Extension of the LSVS class 27
Table 5 – Conformance table 28
Table 6 – PICS for IEC 61850-8-1 ISO 9506 profile 28
Table 7 – PICS for TLS IEC 61850-8-1 Client/Server using ACSE Authentication 29
Table 8 – PICS for VLAN profiles 30
Table 9 – IEC 61850-8-1 L2 GOOSE Security 30
Table 10 – IEC 61850-9-2 L2 SMV Security 31
Table 11 – IEC 61850-8-1 Routable GOOSE 31
Table 12 – IEC 61850-9-2 Routable SMV 32
Table 13 – PICS for SNTP profiles 32

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATION SECURITY –

Part 6: Security for IEC 61850

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-6 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
57/2234/FDIS	57/2258/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

AVA Documents
Document Sharing Hub

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATION SECURITY –

Part 6: Security for IEC 61850

1 Scope and object

1.1 Scope

This part of IEC 62351 specifies messages, procedures, and algorithms for securing the operation of all protocols based on or derived from the IEC 61850 series. This document applies to at least those protocols listed in Table 1.

Table 1 – Scope of application to standards

Number	Name
IEC 61850-8-1	Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC 61850-8-2	Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)
IEC 61850-9-2	Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-6	Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in power utility automation systems related to IEDs

The initial audience for this document is intended to be the members of the working groups developing or making use of the protocols listed in Table 1. For the measures described in this specification to take effect, they must be accepted and referenced by the specifications for the protocols themselves. This document is written to enable that process.

The subsequent audience for this document is intended to be the developers of products that implement these protocols.

Portions of this document may also be of use to managers and executives in order to understand the purpose and requirements of the work.

1.2 Namespace name and version

This new clause is mandatory for any IEC 61850 namespace (as defined by part 7-1 of IEC 61850 Edition 2).

The parameters which identify this new release of this namespace are:

- Namespace version: 2020
- Namespace revision: A
- Namespace name: “IEC 62351-6:2020A”
- Namespace release: 1

The table below provides an overview of all published versions of this namespace.

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020

Edition	Publication date	Webstore	Namespace
Edition 1.0	2020-?	IEC 62351-6:2020	IEC 62351-6:2020

1.3 Code Component distribution

There is currently no code component scheduled for the code component downloading area.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-6, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-8-1, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-8-2, *Communication networks and systems for power utility automation – Part 8-2: Specific communication service mapping (SCSM) – Mapping to Extensible Messaging Presence Protocol (XMPP)*

IEC 61850-9-2, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

IEC 62351-4:2020, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

ISO/IEC 13239, *Information technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures*

ISO/IEC 9594-8 | Rec. ITU-T X.509: *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

Documents
Document Sharing Hub

Full document details: BS EN IEC 62351-6:2020