IEC 62351-6

Edition 1.0   2020-10

INTERNATIONAL STANDARD

**Power systems management and associated information exchange –
Data and communication security –
Part 6: Security for IEC 61850**

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 62351-6

INTERNATIONAL STANDARD

colour inside

Power systems management and associated information exchange –
Data and communication security –
Part 6: Security for IEC 61850

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

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.**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

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*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*[1]

RFC 8052, *Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security Services*

NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation Galois/Counter Mode (GCM and GMAC)*

3   Terms, definitions and abbreviated terms

3.1   Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and IEC 61850-2 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/

- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
electronic security perimeter
logical border surrounding a network interconnecting critical cyber assets

3.1.2
client
functional unit that establishes an association and issues requests and receives services from a server.

3.1.3
server
functional unit that receives an association from a Client and provides services requested by the Client

3.2   Abbreviated terms

ACSE	Association Control Service Element
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit
ASN.1	Abstract Syntax Notation One
ESP	Electronic Security Perimeter
GDOI	Group Domain of Interpretation
GMAC	Galois Message Authentication Code
GOOSE	Generic Object Oriented Substation Event
GSE	Generic Substation Events
HMAC	Hashed Message Authentication Code
ICT	IED Configuration Tool
IED	Intelligent Electronic Device
KFA	Key Delivery Assurance
KDC	Key Distribution Centre

---

[1] Restricted to SNTP profile only.

MAC   Message Authentication Code

SMV   Sampled Measured Values

SCL   Substation Configuration Language

SV   Sampled Value

4 Security issues addressed by this document

4.1 Operational issues affecting choice of security options

For applications using Layer 2 IEC 61850-8-1 GOOSE and Layer 2 IEC 61850-9-2 Sampled Value and requiring 3 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, the communication path selection process (e.g. the fact that Layer 2 GOOSE and SV are supposed to be restricted to a logical substation LAN) shall be used to provide confidentiality for information exchanges. However, this document does define a mechanism for allowing confidentiality for applications where the 3 ms delivery criterion is not a concern.

NOTE The actual performance characteristics of an implementation claiming conformance to this technical specification is outside the scope of this document.

With the exception of confidentiality, this document sets forth a mechanism that allows co-existence of secure and non-secure PDUs.

4.2 Security threats countered

See IEC TS 62351-1 for a discussion of security threats and attack methods.

If encryption is not employed, then the specific threats countered in this clause include:

- unauthorized modification (tampering) of information through message level authentication of the messages.

If encryption is employed, then the specific threats countered in this clause include:

- unauthorized access to information through message level authentication and encryption of the messages;

- unauthorized modification (tampering) or theft of information through message level authentication and encryption of the messages.

- information disclosure is countered.

4.3 Attack methods countered

The following security attack methods are intended to be countered through the appropriate implementation of the specifications/recommendations found within this document:

- man-in-the-middle: this threat will be countered through the use of a Message Authentication Code mechanism specified within this document;

- tamper detection/message integrity: These threats will be countered through the algorithm used to create the authentication mechanism as specified within this document;

- replay: this threat will be countered through the use of specialized processing state machines specified within IEC 62351-4 and this document.

5 Correlation of IEC 61850 parts and IEC 62351 parts

5.1 General

There are four levels of interaction between the parts of the IEC 62351 series and parts of the IEC 61850 series. This part is concerned with the:

- Communication profile security regarding:
  - IEC 61850-8-1 Application Profile for Client/Server communications.
  - IEC 61850-8-2 Application Profile for Client/Server communications.
  - IEC 61850-8-1 Layer 2 T-Profile for GOOSE/GSE
  - IEC 61850-8-1 Layer 2 T-Profile for Multicast Sampled Values
  - IEC 61850-8-1 Layer 3 Routable GOOSE and Sampled Values
- Configuration extensions required for configuration of the Application and Transport communication profiles of concern. These extensions would impact IEC 61850-6.
- Object definitions, regarding security and identification, that are exposed at run-time as part of the IEC 61850-8-1 and IEC 61850-8-2 object mappings.
- The binding of Originator ID values to authenticated peers for Client/Server services.

The scope of this document provides security specifications for use within an Electronic Security Perimeter (ESP) and between ESPs.

5.2   IEC 61850-8-1 Profile for Client/Server communications

5.2.1   General

IEC 61850 implementations claiming conformance to this specification and declaring support for the IEC 61850-8-1 profile utilizing TCP/IP and ISO 9506 (MMS) shall implement Clauses 5 and 6 of IEC 62351-4:2020.

IEC 61850-8-1 specifies the use of MMS within a substation. However, the scope of this specification provides security specifications for use within the substation and external to the substation (e.g. Control Centre to Substation).
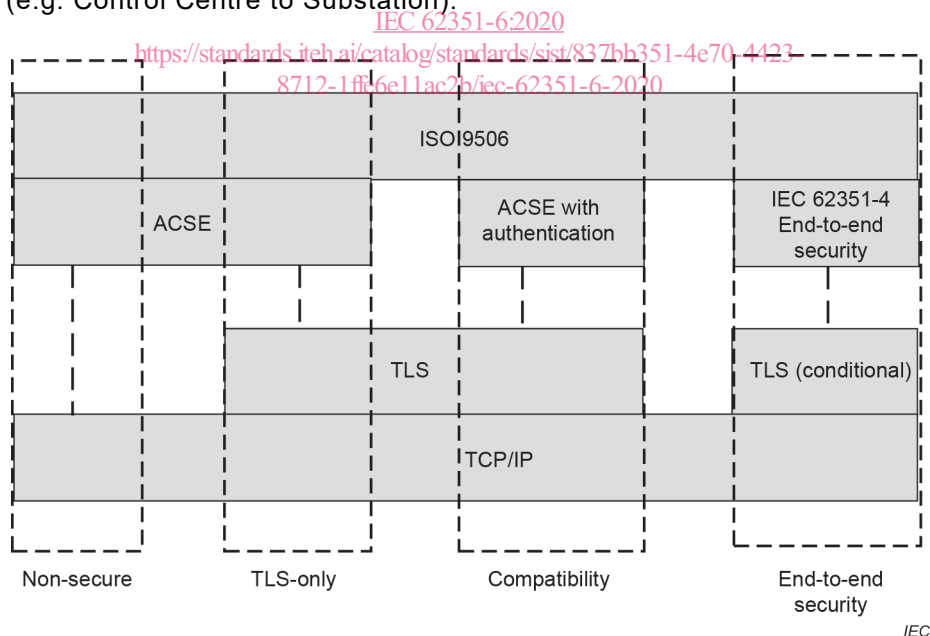
Figure 1 – MMS Security Profiles

Figure 1 shows the security profiles for IEC 61850 Client/Server associations based upon ISO/IEC 9506:

- Non-Secure: Implementations claiming conformance to this clause and Client/Server capability shall support the ability to be configured without securing connections per IEC 62351-4.