IEC TS 60870-5-7

Edition 2.0 2025-03

TECHNICAL SPECIFICATION

Telecontrol equipment and systems –
Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8327-0275-8

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TS 60870-5-7 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Specification.

This second edition cancels and replaces the first edition published in 2013. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) This edition has been completely revised with respect to the previous edition;

b) Alignment with updated versions of IEC 62351-3:2023 and IEC 62351-5:2023;

c) Definition of specific profiles for application layer and transport layer;

d) Introduction of Session Initiation Request to handle situations in which the called station reestablishes a connection;

e) Inclusion of multicast security for the unbalanced mode of IEC 60870-5-101 including key management;

f) Consideration of RBAC based on IEC 62351-8.

This Technical Specification is to be used in conjunction with IEC 62351-5:2023 and IEC 60870-5-104:2016.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
57/2740/DTS	57/2762/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

NOTE The following print types are used:

- Encoding in ASN.1: in `courier new type`.

A list of all the parts in the IEC 60870 series, published under the general title *Telecontrol equipment and systems*, 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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

TELECONTROL EQUIPMENT AND SYSTEMS –

Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)

1 Scope

This part of IEC 60870, which is a technical specification, describes messages and data formats for implementing IEC 62351-5:2023 for secure communication as an extension to IEC 60870-5-101 and IEC 60870-5-104.

The purpose of this document is to permit the receiver of any IEC 60870-5-101/-104 Application Protocol Data Unit (APDU) to verify that the APDU was transmitted by an authorized user and that the APDU was not modified in transit.

This document is also intended to be used, together with the definitions of IEC 62351-3:2023, in conjunction with the IEC 60870-5-104 companion standard.

The state machines, message sequences, and procedures for exchanging these messages are defined in IEC 62351-5:2023. This document describes only the message formats, selected options, critical operations, addressing considerations and other adaptations required to implement IEC 62351 in the IEC 60870-5-101 and IEC 60870-5-104 protocols.

NOTE The version handling is controlled by configuration and not dynamically changed, therefore unexpected / unknown messages are neglected and not processed.

In addition to the previous edition, this new edition of this document also addresses role-based access control, by utilizing the IEC 62351-8 RBAC approach and the already defined role to permission mapping from IEC 62351-5:2023.

The scope of this document does not include security for IEC 60870-5-102 or IEC 60870-5-103. IEC 60870-5-102 is in limited use only and will therefore not be addressed. Users of IEC 60870-5-103 desiring a secure solution need to implement IEC 61850 using the security measures from in IEC 62351 referenced in IEC 61850.

Management of keys, certificates or other cryptographic credentials within devices or on communication links other than IEC 60870-5-101/104 is out of the scope of this document and might be addressed by other IEC 62351 publications in the future.

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 60870-5-101:2003, *Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks*

IEC 60870-5-104:2006, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*

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

IEC 62351-3:2023, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC 62351-5:2023, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management*