IEC/TS 60870-5-7

Edition 1.0   2013-07

TECHNICAL SPECIFICATION

colour inside

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)

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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

IEC/TS 60870-5-7

TECHNICAL SPECIFICATION

colour
inside

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

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) 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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

• the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or

• the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 60870-5-7, which is a technical specification, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
57/1308/DTS	57/1339/RVC

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

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

In this publication the following print types are used:

Clause 10: Direct quotations from IEC/TS 62351-3:2007: in italic 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 publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International Standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

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.

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 describes messages and data formats for implementing IEC/TS 62351-5 for secure authentication as an extension to IEC 60870-5-101 and IEC 60870-5-104.

The purpose of this base standard 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. It provides methods to authenticate not only the device which originated the APDU but also the individual human user if that capability is supported by the rest of the telecontrol system.

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

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

The scope of this specification 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 should implement IEC 61850 using the security measures from in IEC/TS 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 specification and may be addressed by other IEC/TS 62351 specifications in the future.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 62351-3:2007, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC/TS 62351-5:2013, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

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

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE   Terms 3.1.1 to 3.1. 7 are included here because they are specific to the IEC 60870-5 standards and may be useful for reading this specification as an independent document. Terms 3.1.8 to 3.1.9 are included here because they are specific to IEC/TS 62351-5.

3.1.1
Application Protocol Data Unit
complete application layer message transmitted by a station

3.1.2
Application Service Data Unit
application layer message submitted to lower layers for transmission

3.1.3
Controlling Station
device or application that initiates most of the communications and issues commands

Note 1 to entry: Commonly called a "master" in some protocol specifications.

3.1.4
Controlled Station
remote device that transmits data gathered in the field to the controlling station

Note 1 to entry: Commonly called the "outstation" or "slave" in some protocols.

3.1.5
Control Direction
data transmitted by the controlling station to the controlled station(s)

3.1.6
Message Authentication Code
calculated value used by a receiving station to authenticate and check the integrity of an Application Protocol Data Unit

3.1.7
Monitoring Direction
data transmitted by the controlled station to the controlling stations

3.1.8
Challenger
station that issues authentication challenges. May be either a controlled or controlling station.

3.1.9
Responder
station that responds or reacts to authentication challenges. May be either a controlled or controlling station.

3.2   Abbreviated terms

Refer to IEC/TS 62351-2 for a list of applicable abbreviated terms. Terms 3.2.1 to 3.2.3 are included here because they are specifically used in the affected protocols and used in the discussion of this authentication mechanism.

**3.2.1
ASDU**
Application Service Data Unit

**3.2.2
APDU**
Application Protocol Data Unit

**3.2.3
MAC**
Message Authentication Code

4   Selected options

4.1   Overview of clause

This clause describes which of the options specified in IEC/TS 62351-5 shall be implemented in IEC 60870-5-101 and IEC 60870-5-104.

4.2   MAC algorithms

IEC 60870-5 stations shall implement all the mandatory MAC algorithms listed in IEC/TS 62351-5, and may implement any of the optional MAC algorithms listed there.

4.3   Encryption algorithms

IEC 60870-5 stations shall implement all the mandatory encryption algorithms listed in IEC/TS 62351-5, and may implement any of the optional encryption algorithms listed there.

4.4   Maximum error count

IEC 60870-5 stations may implement a maximum error count in the range specified in IEC/TS 62351-5.

4.5   Use of aggressive mode

IEC 60870-5 stations shall implement IEC/TS 62351-5 aggressive mode. Aggressive mode shall be the normal method of authentication for stations implementing this specification. However, IEC 60870-5 stations shall also permit it to be configured as disabled. A station with aggressive mode disabled shall not transmit any S_AR_NA_1 Aggressive Mode Request ASDUs and shall reply to any such ASDUs with S_ER_NA_1 Authentication Error ASDUs, subject to the limitations on Error messages described in IEC/TS 62351-5.

Regardless of whether aggressive mode is disabled, IEC 60870-5 stations shall initialize the challenge data in both directions when establishing communications, as described in 8.2.

5   Operations considered critical

IEC 60870-5-101 and IEC 60870-5-104 ASDUs identified as "M" (for "Mandatory") in the "M/O" ("Mandatory or Optional") column in 10.10 shall be considered critical operations. Stations complying with this standard shall require the sender to authenticate those ASDUs. Any station may optionally require authentication of any other ASDUs.

Devices complying with this standard shall provide information along with the Interoperability Tables identifying which ASDUs the device/station considers critical, requiring authentication. Refer to 10.10. If an ASDU is identified as critical, the ACT or DEACT cause of transmission is shall be considered mandatory critical, but not ACTCON or ACT_TERM.

IEC/TS 62351-5 states that any device may arbitrarily decide that an ASDU is critical and can therefore initiate a challenge for any reason. However, IEC 60870-5 shall not enforce this rule. ASDUs that are considered critical at any time by an IEC 60870-5 station shall always be considered critical by that station unless the station is reconfigured.

Any ASDUs capable of changing security configuration parameters, now or in the future, shall be considered critical.

6 Addressing information

Each IEC 60870-5-101 station shall include in its MAC calculations the destination station address from the IEC 60870-5 data link layer in the "Addressing Information" portion of the calculation. The octets of the address when included in the calculation shall be as transmitted.

7 Implementation of messages

7.1 Overview of clause

This clause describes how the secure authentication messages described in IEC/TS 62351-5 are implemented in IEC 60870-5-101 and IEC 60870-5-104.

7.2 Data definitions

7.2.1 Causes of transmission

Stations implementing secure authentication shall use the causes of transmission listed in Table 1 in addition to those described in 7.2.3 of IEC 60870-5-101:2003.

Table 1 – Additional cause of transmission

Cause := UI6[1..6]<14..16>
<14>   := authentication
<15>   := maintenance of authentication session key
<16>   := maintenance of user role and update key

7.2.2 Type identifiers

Stations implementing secure authentication shall use the Type Identifications listed in Table 2 in addition to those described in 7.2.1 of IEC 60870-5-101:2003 and Clause 6 of IEC 60870-5-104:2006. This range of Type Identifications was previously allocated for system information in the monitor direction. The ASDUs identified by these types may be transmitted in either the control or monitor direction.

Table 2 – Additional type identifiers

TYPE IDENTIFICATION	:=	UI8[1..8]<81..87>	
<41>	:=	integrated totals containing time tagged security statistics	S_IT_TC_1
<81>	:=	authentication challenge	S_CH_NA_1
<82>	:=	authentication reply	S_RP_NA_1
<83>	:=	aggressive mode authentication request	S_AR_NA_1
<84>	:=	session key status request	S_KR_NA_1