# IEC/TS 60870-5-7

Edition 1.0 2013-07

# 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

PRICE CODE X

ICS 33.200

ISBN 978-2-8322-0919-6

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

® Registered trademark of the International Electrotechnical Commission

# CONTENTS

FOREWORD ..... 5
1 Scope ..... 7
2 Normative references ..... 7
3 Terms, definitions and abbreviations ..... 8
3.1 Terms and definitions ..... 8
3.2 Abbreviated terms ..... 9
4 Selected options ..... 9
4.1 Overview of clause ..... 9
4.2 MAC algorithms ..... 9
4.3 Encryption algorithms ..... 9
4.4 Maximum error count ..... 9
4.5 Use of aggressive mode ..... 9
5 Operations considered critical ..... 9
6 Addressing information ..... 10
7 Implementation of messages ..... 10
7.1 Overview of clause ..... 10
7.2 Data definitions ..... 10
7.2.1 Causes of transmission ..... 10
7.2.2 Type identifiers ..... 10
7.2.3 Security statistics ..... 11
7.2.4 Variable length data ..... 11
7.2.5 Information object address ..... 12
7.2.6 Transmitting extended ASDUs using segmentation ..... 12
7.3 Application Service Data Units ..... 16
7.3.1 TYPE IDENT 81: S_CH_NA_1 Authentication challenge ..... 16
7.3.2 TYPE IDENT 82: S_RP_NA_1 Authentication Reply ..... 17
7.3.3 TYPE IDENT 83: S_AR_NA_1 Aggressive mode authentication request ..... 18
7.3.4 TYPE IDENT 84: S_KR_NA_1 Session key status request ..... 19
7.3.5 TYPE IDENT 85: S_KS_NA_1 Session key status ..... 20
7.3.6 TYPE IDENT 86: S_KC_NA_1 Session key change ..... 21
7.3.7 TYPE IDENT 87: S_ER_NA_1 Authentication error ..... 22
7.3.8 TYPE IDENT 88: S_UC_NA_1 User certificate ..... 23
7.3.9 TYPE IDENT 90: S_US_NA_1 User status change ..... 24
7.3.10 TYPE IDENT 91: S_UQ_NA_1 Update key change request ..... 25
7.3.11 TYPE IDENT 92: S_UR_NA_1 Update key change reply ..... 26
7.3.12 TYPE IDENT 93: S_UK_NA_1 Update key change – symmetric ..... 27
7.3.13 TYPE IDENT 94: S_UA_NA_1 Update key change – asymmetric ..... 28
7.3.14 TYPE IDENT 95: S_UC_NA_1 Update key change confirmation ..... 29
7.3.15 TYPE IDENT 41: S_IT_TC_1 Integrated totals containing time-tagged security statistics ..... 30
8 Implementation of procedures ..... 31
8.1 Overview of clause ..... 31
8.2 Initialization of aggressive mode ..... 31
8.3 Refreshing challenge data ..... 34
8.4 Co-existence with non-secure implementations ..... 34

9 Implementation of IEC/TS 62351-3 using IEC 60870-5-104 ..... 34
9.1 Overview of clause ..... 34
9.2 Deprecation of non-encrypting cipher suites ..... 34
9.3 Mandatory cipher suite ..... 34
9.4 Recommended cipher suites ..... 34
9.5 Negotiation of versions ..... 35
9.6 Cipher renegotiation ..... 35
9.7 Message authentication code ..... 35
9.8 Certificate support ..... 35
9.8.1 Overview of clause ..... 35
9.8.2 Multiple Certificate Authorities (CAs) ..... 36
9.8.3 Certificate size ..... 36
9.8.4 Certificate exchange ..... 36
9.8.5 Certificate comparison ..... 36
9.9 Co-existence with non-secure protocol traffic ..... 37
9.10 Use with redundant channels ..... 37
10 Protocol Implementation Conformance Statement ..... 38
10.1 Overview of clause ..... 38
10.2 Required algorithms ..... 38
10.3 MAC algorithms ..... 38
10.4 Key wrap algorithms ..... 38
10.5 Use of error messages ..... 38
10.6 Update key change methods ..... 38
10.7 User status change ..... 39
10.8 Configurable parameters ..... 39
10.9 Configurable statistic thresholds and statistic information object addresses ..... 40
10.10 Critical functions ..... 40
Bibliography ..... 44

Figure 1 – ASDU segmentation control ..... 12
Figure 2 – Segmenting extended ASDUs ..... 12
Figure 3 – Illustration of ASDU segment reception state machine ..... 15
Figure 4 – ASDU: S_CH_NA_1 Authentication challenge ..... 16
Figure 5 – ASDU: S_RP_NA_1 Authentication Reply ..... 17
Figure 6 – ASDU: S_AR_NA_1 Aggressive Mode Authentication Request ..... 18
Figure 7 – ASDU: S_KR_NA_1 Session key status request ..... 19
Figure 8 – ASDU: S_KS_NA_1 Session key status ..... 20
Figure 9 – ASDU: S_KC_NA_1 Session key change ..... 21
Figure 10 – ASDU: S_ER_NA_1 Authentication error ..... 22
Figure 11 – ASDU: S_UC_NA_1 User certificate ..... 23
Figure 12 – ASDU: S_US_NA_1 User status change ..... 24
Figure 13 – ASDU: S_UQ_NA_1 Update key change request ..... 25
Figure 14 – ASDU: S_UR_NA_1 Update key change reply ..... 26
Figure 15 – ASDU: S_UK_NA_1 Update key change – symmetric ..... 27
Figure 16 – ASDU: S_UA_NA_1 Update key change – asymmetric ..... 28
Figure 17 – ASDU: S_UC_NA_1 Update key change confirmation ..... 29

Figure 18 – ASDU: S_IT_TC_1 Integrated totals containing time-tagged security statistics ..... 30
Figure 19 – Example of successful initialization of challenge data ..... 33

Table 1 – Additional cause of transmission ..... 10
Table 2 – Additional type identifiers ..... 10
Table 3 – Maximum lengths of variable length data ..... 11
Table 4 – ASDU segment reception state machine ..... 14
Table 5 – Recommended cipher suite combinations ..... 35

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*