

TECHNICAL SPECIFICATION



**Power systems management and associated information exchange – Data and communications security –
Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2018 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions 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 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.

TECHNICAL SPECIFICATION



**Power systems management and associated information exchange – Data and communications security –
Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-6182-8

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

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviated terms	10
3.1 Terms and definitions.....	10
3.2 Abbreviated terms.....	12
4 General	12
4.1 Normatives covered by this technical specification.....	12
4.2 Conformance testing structure	12
4.2.1 General	12
4.2.2 Conformance testing of security extension procedures	13
4.2.3 Conformance testing addressed per station type	14
4.2.4 Normal procedure tests and resiliency tests.....	14
4.3 Conformance testing requirements.....	14
4.3.1 Testing base protocols with security extension.	14
4.3.2 Testing of profiles including TCP/IP	14
4.3.3 Requirements for the device under test	14
4.3.4 Requirements for the test facility	15
4.3.5 Test logging.....	15
5 Verification of configuration parameters.....	16
5.1 General.....	16
5.2 System definition	16
5.3 Application security extension.....	18
6 Verification of Communication	21
6.1 General.....	21
6.2 ASDU segmentation control	21
6.3 Verification of ASDUs	23
6.3.1 User management ASDUs	23
6.3.2 Update key maintenance ASDUs	26
6.3.3 Session key maintenance ASDUs	32
6.3.4 Challenge/reply and aggressive mode authentication ASDUs	35
6.3.5 Security statistics ASDU	39
7 Verification of procedures.....	39
7.1 General.....	39
7.2 User management.....	40
7.2.1 General	40
7.2.2 Controlling station.....	41
7.2.3 Controlled station	43
7.3 Update key maintenance - Symmetric	48
7.3.1 General	48
7.3.2 Controlling station.....	48
7.3.3 Controlled station	52
7.4 Update key maintenance - Asymmetric	54
7.4.1 General	54
7.4.2 Controlling station.....	55

7.4.3	Controlled station	59
7.5	Session key maintenance	61
7.5.1	General	61
7.5.2	Controlling station.....	62
7.5.3	Controlled station	67
7.6	Challenge/reply authentication	69
7.6.1	General	69
7.6.2	Controlling station.....	70
7.6.3	Controlled station	76
7.7	Aggressive mode authentication	80
7.7.1	General	80
7.7.2	Controlling station.....	81
7.7.3	Controlled station	84
8	Tests results chart.....	87
8.1	Verification of configuration parameters	87
8.2	Verification of communication	88
8.2.1	ASDUs segmentation control.....	88
8.2.2	User management ASDUs	89
8.2.3	Update key maintenance ASDUs	90
8.2.4	Session key maintenance ASDUs	92
8.2.5	Challenge/reply and aggressive mode authentication ASDUs	93
8.2.6	Security statistics ASDU	94
8.3	Verification of procedures	95
8.3.1	User management	95
8.3.2	Update key maintenance - Symmetric.....	98
8.3.3	Update key maintenance - Asymmetric.....	100
8.3.4	Session key maintenance	102
8.3.5	Challenge/reply authentication.....	105
8.3.6	Aggressive mode authentication	109
Figure 1	– IEC TS 62351-5 Security extension procedures	13
Table 1	– Configuration parameters: System definition	17
Table 2	– Configuration parameters: Application security extension.....	19
Table 3	– ASDU segmentation control.....	22
Table 4	– User management ASDUs.....	23
Table 5	– Update key maintenance ASDUs.....	26
Table 6	– Session key maintenance ASDUs.....	32
Table 7	– Challenge/reply and aggressive mode authentication ASDUs	35
Table 8	– Security statistics ASDU.....	39
Table 9	– User management: Controlling station normal procedure tests	41
Table 10	– User management: Controlling station resiliency tests	42
Table 11	– User management: Controlled station normal procedure tests	43
Table 12	– User management: Controlled station resiliency tests.....	44
Table 13	– Update key maintenance - Symmetric: Controlling station triggering conditions	48

Table 14 – Update key maintenance - Symmetric: Controlling station normal procedure tests	49
Table 15 – Update key maintenance - Symmetric: Controlling station resiliency tests	50
Table 16 – Update key maintenance - Symmetric: Controlled station normal procedure tests	52
Table 17 – Update key maintenance - Symmetric: Controlled station resiliency tests	53
Table 18 – Update key maintenance - Asymmetric: Controlling station triggering conditions	55
Table 19 – Update key maintenance - Asymmetric: Controlling station normal procedure tests	56
Table 20 – Update key maintenance - Asymmetric: Controlling station resiliency tests	57
Table 21 – Update key maintenance - Asymmetric: Controlled station normal procedure tests	59
Table 22 – Update key maintenance - Asymmetric: Controlled station resiliency tests	60
Table 23 – Session key maintenance: Controlling station triggering conditions	62
Table 24 – Session key maintenance: Controlling station normal procedure tests	63
Table 25 – Session key maintenance: Controlling station resiliency tests	64
Table 26 – Session key maintenance: Controlled station invalidating session key	67
Table 27 – Session key maintenance: Controlled station normal procedure tests	68
Table 28 – Session key maintenance: Controlled station resiliency tests	69
Table 29 – Challenge/reply authentication: Controlling station triggering conditions	70
Table 30 – Challenge/reply authentication: Controlling station normal procedure tests	71
Table 31 – Challenge/reply authentication: Controlling station resiliency tests	72
Table 32 – Challenge/reply authentication: Controlled station normal procedure tests	76
Table 33 – Challenge/reply authentication: Controlled station resiliency tests	77
Table 34 – Aggressive mode authentication: Controlling station normal procedure tests	81
Table 35 – Aggressive mode authentication: Controlling station resiliency tests	82
Table 36 – Aggressive mode authentication: Controlled station normal procedure tests	84
Table 37 – Aggressive Mode Authentication: Controlled station resiliency tests	85
Table 38 – Test results chart: Configuration parameters	87
Table 39 – Test results chart: ASDU segmentation control	88
Table 40 – Test results chart: User managements ASDUs	89
Table 41 – Test results chart: Update key maintenance ASDUs	90
Table 42 – Test results chart: Session key maintenance ASDUs	92
Table 43 – Test results chart: Challenge/reply and aggressive mode authentication ASDUs	93
Table 44 – Test results chart: Security statistics ASDU	94
Table 45 – Test results chart: User management procedure – Controlling station	95
Table 46 – Test results chart: User management procedure – Controlled Station	96
Table 47 – Test results chart: Update key maintenance – Symmetric – Controlling station	98
Table 48 – Test results chart: Update key maintenance – Symmetric – Controlled station	99
Table 49 – Test results chart: Update key maintenance – Asymmetric – Controlling station	100

Table 50 – Test results chart: Update key maintenance – Asymmetric – Controlled station	101
Table 51 – Test results chart: Session key maintenance – Controlling station	102
Table 52 – Test results chart: Session key maintenance – Controlled station	104
Table 53 – Test results chart: Challenge/reply authentication – Controlling station	105
Table 54 – Test results chart: Challenge/reply authentication – Controlled station	107
Table 55 – Test results chart: Aggressive mode authentication – Controlling station	109
Table 56 – Test results chart: Aggressive mode authentication – Controlled station	110

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION
EXCHANGE – DATA AND COMMUNICATIONS SECURITY –****Part 100-1: Conformance test cases for IEC TS 62351-5
and IEC TS 60870-5-7**

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 TS 62351-100-1, 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
57/1980/DTS	57/2016/RVDTS

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

A list of all parts in 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.

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.

INTRODUCTION

This technical specification describes test cases for conformance testing of telecontrol equipment or systems using the IEC TS 62351-5 security extension and its application in IEC TS 60870-5-7 for IEC 60870-5-101 and IEC 60870-5-104 communication protocols.

This document is a preview generated by EVS

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

Part 100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7

1 Scope

This part of IEC 62351, which is a technical specification, describes test cases of data and communication security for telecontrol equipment, substation automation systems (SAS) and telecontrol systems, including front-end functions of SCADA.

The goal of this document is to enable interoperability by providing a standard method of testing protocol implementations to verify that a device fulfils the requirement of the standard. Note that conformity to the standard does not guarantee interoperability between devices using different implementations. It is expected that using this specification during testing will minimize the risk of non-interoperability. A basic condition for this interoperability is a passed conformance test of both devices.

The scope of this document is to specify commonly available procedures and definitions for conformance and/or interoperability testing of IEC TS 62351-5 and IEC TS 60870-5-7. The conformance test cases defined herein are focused to verify the conformant integration of the underlying authentication, as specified in IEC TS 62351-5 and IEC TS 60870-5-7, to protect IEC 60870-5-101 and IEC 60870-5-104-based communications.

This document deals with data and communication security conformance testing; therefore, other requirements, such as safety or EMC, are not covered. These requirements are covered by other standards (if applicable) and the proof of compliance for these topics is done according to these standards.

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.¹

IEC 60870-5-6:2006, *Telecontrol equipment and systems – Part 5-6: Guidelines for conformance testing for the IEC 60870-5 companion standards*

IEC TS 60870-5-7:2013, *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)*

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

¹ The base standard always takes precedence. In case of ambiguity between this document and the base standards (IEC TS 62351-5 and IEC TS 60870-5-7), this part of IEC 62351 needs to be clarified or amended.

When testing, negative behaviour is not described in the base standard. The behaviour described in this document prevails and should be observed. The conformance statement produced after testing indicates any lack of conformance to either the test plan or the base standard.

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 60870-5-601:2015, *Telecontrol equipment and systems – Part 5-601: Transmission protocols – Conformance test cases for the IEC 60870-5-101 companion standard*

IEC TS 60870-5-604:2016, *Telecontrol equipment and systems – Part 5-604: Conformance test cases for the IEC 60870-5-104 companion standard*

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

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 62351-9:2017, *Power systems management and associated information exchange – Data and communications security – Part 9: Cyber security key management for power system equipment*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following 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 Terms and definitions

3.1.1

Application Service Data Unit

ASDU

application layer message submitted to lower layers for transmission

3.1.2

control direction

direction of transmission from the controlling station to a controlled station

3.1.3

controlled station

station which is monitored, or commanded and monitored by a master (controlling) station

Note 1 to entry: This is commonly called an “outstation” or “slave” or “server” in some specifications.

3.1.4

controlling station

station which performs the telecontrol of outstations (controlled station)

Note 1 to entry: This is commonly called a “master” or “master station” or “client” in some specifications.

3.1.5

interoperability

ability of two or more telecontrol devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation