IEC TS 62351-100-1

Edition 1.0 2018-11

TECHNICAL SPECIFICATION

colour inside

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

IEC TS 62351-100-1:2018-11(en)

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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.

IEC TS 62351-100-1

Edition 1.0 2018-11

TECHNICAL SPECIFICATION

colour inside

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

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.

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 6870-5-104-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*l

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

3.1.6
Message Authentication Code
MAC
calculated value used by a receiving station to authenticate and check the integrity of an information

3.1.7
monitor direction
direction of transmission from a controlled station to a controlling station

3.1.8
normal procedure tests
set of test cases to verify that the device fulfils the requirements of the standard in the expected (normal) conditions

3.1.9
Protocol Implementation Conformance Statement
PICS
summary of the referencing standard capabilities of the system to be tested

3.1.10
Protocol Implementation Document
PID
document which describes complete functionalities and system specific information

Note 1 to entry: The PID consists of the PICS and the PIXIT.

3.1.11
Protocol Implementation eXtra Information for Testing
PIXIT

document containing system specific information regarding the capabilities of the system to be tested and specifying which items are optional

3.1.12
resiliency tests
set of test cases to verify that the device fulfils the requirements of the standard in reacting to the unexpected (error) conditions

3.1.13
test equipment
all tools and instruments which simulate and verify the communication traffic, input or outputs of the system under test

3.1.14
test initiator
party initiating a conformance test of a device that is executed by a test facility

3.1.15
test facility
supplier-independent organization which is able to provide appropriate test equipment and trained staff for conformance testing

3.1.16
user number
USR
numeric value that unambiguously identifying a user in the protocol

3.2 Abbreviated terms

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

ASDU	Application service data unit
CASDU	Common address of ASDU
COT	Cause of transmission
DUT	Device under test
IOA	Information object address
IP	Inter-networking protocol
MAC	Message authentication code
PICS	Protocol implementation conformance statement
PID	Protocol implementation document (=PICS + PIXIT)
PIXIT	Protocol implementation extra information for testing
SAS	Substation automation system
SCADA	Supervisory control and data acquisition
TCP	Transport control protocol
USR	User number

4 General

4.1 Normatives covered by this technical specification

This document defines the conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7 and the security extensions for IEC 60870-5-101 and IEC 60870-5-104 base protocols.

Test cases for IEC 60870-5-101 and IEC 60870-5-104 base protocols are not in the scope of this document since they are already defined respectively in IEC TS 60870-5-601 and IEC TS 60870-5-604.

4.2 Conformance testing structure

4.2.1 General

The security extension defined in IEC TS 62351-5 and IEC TS 60870-5-7 introduces new procedures and new ASDU types to be exchanged at application level, each procedure has its own set of messages exchanged during execution.

The conformance test cases are divided into five clauses:

- Clause 5: Verification of configuration parameters. This clause contains the configuration parameters affecting the message contents and/or the protocol behaviour.
- Clause 6: Verification of communication. The goal of this clause is to verify that DUT is able to implement the security extension messages as described in IEC TS 60870-5-7.
- Clause 7: Verification of procedures. The goal of this clause is to verify that DUT is able to execute the security extension procedures as described in IEC TS 62351-5.
- Clause 8: Test result chart. This clause contains the results of the test cases listed in Clauses 6 and 7 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables (see Tables 4 to 56). They are numbered; their numbering syntax is: Subclause number (where the Table is located) + test case number.

In the column ‘reference’ each test case has a direct reference to IEC TS 62351-5 or IEC TS 60870-5-7 where the clause under test is defined.

Test cases are mandatory depending on the description in the column ‘Required’. The following situations are possible:

M = Mandatory test case. The test is referencing a clause that is mandatory in IEC TS 62351-5 or IEC TS 60870-5-7.

PICS x, x = Mandatory test case if the functionality is enabled in the PICS (by marking the applicable check box), with a reference to the section number of the PICS (x.x).

4.2.2 Conformance testing of security extension procedures

The security extension procedures can be summarized as follows:

- User management
- Update key maintenance
- Session key maintenance
- Challenge/Reply authentication
- Aggressive Mode authentication

In general, these procedures are executed in sequence as shown in Figure 1.

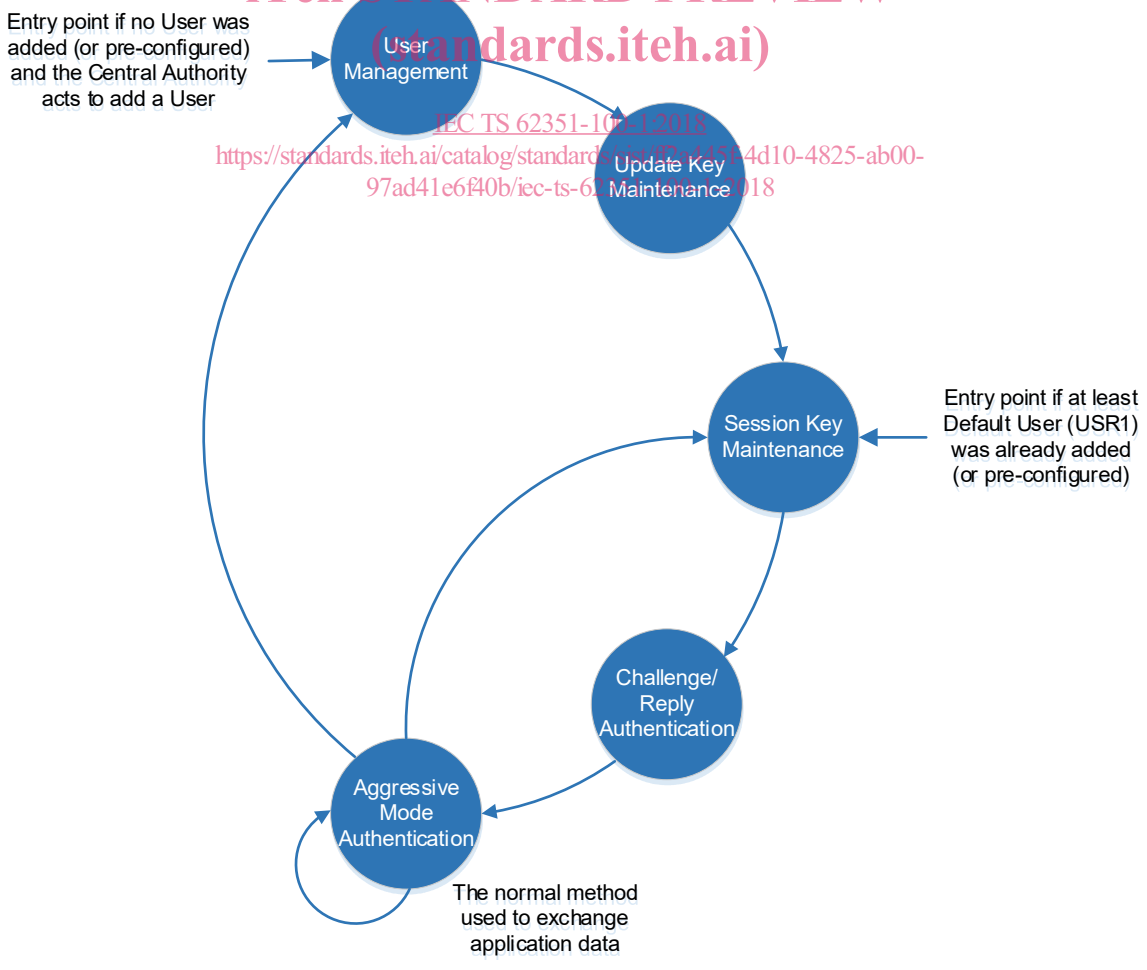

Figure 1 – IEC TS 62351-5 Security extension procedures