

TECHNICAL SPECIFICATION



Power systems management and associated information exchange – Data and communication security
Part 100-6: Cybersecurity conformance testing for IEC 61850-8-1 and IEC 61850-9-2

[IEC TS 62351-100-6:2022](https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022)

<https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022>



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2022 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 Secretariat
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 corrigendum or an amendment might have been published.

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 It also gives information on projects, replaced and withdrawn publications.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

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 Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

[IEC TS 62351-100-6:2022](https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-e107413a560c/iec-ts-62351-100-6-2022)

<https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-e107413a560c/iec-ts-62351-100-6-2022>



TECHNICAL SPECIFICATION



Power systems management and associated information exchange – Data and communication security
Part 100-6: Cybersecurity conformance testing for IEC 61850-8-1 and IEC 61850-9-2

[IEC TS 62351-100-6:2022](https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022)

<https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022>

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-3976-6

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

CONTENTS

| | |
|---|----|
| FOREWORD..... | 3 |
| 1 Scope..... | 7 |
| 2 Normative references | 7 |
| 3 Terms and definitions | 8 |
| 4 General | 8 |
| 4.1 General guidelines..... | 8 |
| 4.2 Test methodology | 8 |
| 4.2.1 General | 8 |
| 4.2.2 Normal procedure tests and resiliency tests..... | 9 |
| 4.3 Conformance testing requirements..... | 9 |
| 4.3.1 Testing within the context of an application..... | 9 |
| 4.3.2 Requirements for the device under test..... | 9 |
| 4.3.3 Requirements for the test facility | 10 |
| 4.3.4 Test validation | 11 |
| 4.4 PICS..... | 11 |
| 4.5 PIXIT | 11 |
| 4.6 Tests cases for subscriber-type DUT | 14 |
| 4.7 Tests cases for publisher-type DUT | 14 |
| 5 Conformity Testing for 62351-6..... | 14 |
| 5.1 PICS for 62351-6 security profile | 14 |
| 5.2 GOOSE Security Conformity Testing..... | 15 |
| 5.2.1 General | 15 |
| 5.2.2 Test Procedures | 17 |
| 5.3 SV Security Conformity Testing..... | 22 |
| 5.3.1 General | 22 |
| 5.3.2 Test Procedures | 23 |
| 6 SCL extension requirements testing | 29 |
| Bibliography..... | 32 |
| Table 1 – PIXIT for Base Profile..... | 11 |
| Table 2 – PIXIT for GOOSE security extension and replay testing | 12 |
| Table 3 – PIXIT for SV security extension and replay testing | 13 |
| Table 4 – 62351-6 Subscriber Compliancy..... | 14 |
| Table 5 – 62351-6 Publisher Compliancy | 14 |
| Table 6 – Conformance table | 15 |
| Table 7 – GOOSE State Transition Tests Matrix | 16 |
| Table 8 – L2-GOOSE and R-GOOSE Security profiles | 16 |
| Table 9 – Verification of GOOSE subscriber security extension | 17 |
| Table 10 – Verification of GOOSE publisher security extension | 19 |
| Table 11 – Verification of GOOSE Replay Requirements | 20 |
| Table 12 – SV State Transition Tests Matrix | 23 |
| Table 13 – L2-SV and R-SV Security profiles..... | 24 |
| Table 14 – Verification of SV Subscriber Security Extension | 25 |
| Table 15 – Verification of SV publisher security extension | 27 |
| Table 16 – Verification of SV subscriber Replay Requirements | 28 |
| Table 17 – Verification of SCL extensions..... | 30 |

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION
EXCHANGE – DATA AND COMMUNICATION SECURITY –****Part 100-6: Cybersecurity conformance
testing for IEC 61850-8-1 and IEC 61850-9-2**

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.

IEC TS 62351-100-6 has been prepared by IEC technical committee 57: Power systems management and associated information exchange. It is a Technical Specification.

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

| | |
|-------------|------------------|
| Draft | Report on voting |
| 57/2438/DTS | 57/2484/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/standardsdev/publications.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communication 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 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.

IMPORTANT – The "colour inside" logo on the cover page of this document 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.

(standards.iteh.ai)

IEC TS 62351-100-6:2022

<https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022>

INTRODUCTION

The International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent. IEC takes no position concerning the evidence, validity, and scope of this patent right.

The holder of this patent right has assured IEC that s/he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with IEC. Information may be obtained from the patent database available at <http://patents.iec.ch>.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights other than those in the patent database. IEC shall not be held responsible for identifying any or all such patent rights.

The quality system of a device producer forms the basis of reliable testing in development and production activities. Many internal tests during the development of a device result in a unit level test performed at least by the provider and – if required by applicable standards – by an independent test authority. In the context of this document, the term type test is restricted to the functional behavior of the device.

Conformance testing does not replace project-specific system related tests such as the FAT (Factory acceptance Test) and SAT (Site Acceptance Test). The FAT and SAT are based on specific customer requirements for a dedicated substation automation system and are done by the system integrator and normally witnessed by the customer. These tests increase the confidence level that all potential problems in the system have been identified and solved. These tests establish that the delivered substation automation system is performing as specified. The conformance testing reduces the risks of failure during the FAT and SAT.

The purpose of this part of IEC 62351 is to cover all possible situations taking into consideration the normal operating test cases and also the failure test cases to demonstrate the capability of the DUT (Device Under Test) to operate with other devices in the specified way according to the IEC 62351-6.

Through this part of IEC 62351, a test facility can prove the IEC TS 62351-100-6:2022 (E), which is a technical specification, is part of the IEC 62351 suite of standards, which describes test cases for interoperability conformance testing of data and communication security for Substation Automation Systems [SAS] and telecontrol systems which implement IEC TS 62351-6. The tests described in this part do not evaluate the security of the implementation. Thus, citing conformance to this part does not imply that any particular security level has been achieved by the corresponding product, or by the system in which it is used.

The goal of this part of IEC 62351 is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. It is expected that using this specification during testing will minimize the risk of non-interoperability. Additional testing and assurance measures will be required to verify that a particular implementation of IEC TC 62351-6 has correctly implemented all the security functions and that they can be assured to be present in all delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify common available procedures and definitions for conformance and/or interoperability testing of IEC 62351-6, the IEC 61850-8-1, IEC 61850-9-2 and also their recommendations over IEC 62351-3 for profiles including TCP/IP and IEC 62351 4 for profiles including MMS. These are the security extensions for IEC 61850 and derivatives to enable unambiguous and standardized evaluation of IEC TS 62351-6 and its companion standards protocol implementations.

The detailed test cases per companion standard, containing among others mandatory and optional mandatory test cases per Secure Communication Application Function, secure ASDU (Application Service Data Unit) and transmission procedures, will become available as technical specifications (TS). Other functionality may need additional test cases, but this is outside the scope of this part of IEC 62351. This document is such a technical specification for the mentioned companion standard.

This document deals mainly with data and communication security conformance testing; therefore, other requirements, such as safety or EMC (Electromagnetic compatibility) 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. SMV at the DUT communication subsystem (or a part of it) conforms to IEC 62351-6.

The tests cases described in this specification do not guarantee full cybersecurity conformance testing. It should be complemented with other test suites.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[IEC TS 62351-100-6:2022](https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022)

<https://standards.iteh.ai/catalog/standards/sist/c27c05ad-b8af-4d33-b76e-ef074f3a5b0c/iec-ts-62351-100-6-2022>

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

Part 100-6: Cybersecurity conformance testing for IEC 61850-8-1 and IEC 61850-9-2

1 Scope

IEC TS 62351-100-6, which is a technical specification, is part of the IEC 62351 suite of standards, which describes test cases for interoperability conformance testing of data and communication security for Substation Automation Systems [SAS] and telecontrol systems which implement IEC TS 62351-6. The tests described in this part do not evaluate the security of the implementation. Thus, citing conformance to this part does not imply that any particular security level has been achieved by the corresponding product, or by the system in which it is used.

The goal of this part of IEC 62351 is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. It is expected that using this specification during testing will minimize the risk of non-interoperability. Additional testing and assurance measures will be required to verify that a particular implementation of IEC TC 62351-6 has correctly implemented all the security functions and that they can be assured to be present in all delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify common available procedures and definitions for conformance and/or interoperability testing of IEC 62351-6, the IEC 61850-8-1, IEC 61850-9-2 and also their recommendations over IEC 62351-3 for profiles including TCP/IP and IEC 62351-4 for profiles including MMS. These are the security extensions for IEC 61850 and derivatives to enable unambiguous and standardized evaluation of IEC TS 62351-6 and its companion standards protocol implementations.

The detailed test cases per companion standard, containing among others mandatory and optional mandatory test cases per Secure Communication Application Function, secure ASDU (Application Service Data Unit) and transmission procedures, will become available as technical specifications (TS). Other functionality may need additional test cases, but this is outside the scope of this part of IEC 62351. This document is such a technical specification for the mentioned companion standard.

This document deals mainly with data and communication security conformance testing; therefore, other requirements, such as safety or EMC (Electromagnetic compatibility) 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.

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

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

IEC 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

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

3 Terms and definitions

No terms and definitions are listed in this document.

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>

4 General

4.1 General guidelines

The test environment shall be as close as possible to the final environment. To perform the test, a specially designed testing device is used to test the DUT. Since the IED (Intelligent Electronic Device) can be tested in publisher or subscriber mode, there exist two versions of testing devices.

To realize the tests described in this document, a test equipment (TEQ) shall support the capability of analysis all the IEC 62351-6 requirements and be able to generate invalid messages to test the robustness of the DUT. The DUT shall provide means of reporting/displaying internal status (see 4.3.4) to provide to the test engineer enough information in order to validate the state machine status and the results of the tests.

The test facility will likely use a single publisher/subscriber simulator, but there is no restriction on using one publisher/subscriber which only supports certain communication services and using another to do the rest i.e. as long as the server(s)/client(s) simulators can cover the input requirements to the test case/DUT. Such test environment adaptations shall be documented in the test report.

A certificate authority is also required for the tests.

4.2 Test methodology

4.2.1 General

The tests are realized in a non-intrusive mode. The DUT has the same software and parameters as the production system. To realize the conformity testing, IED functions, at application level, are used to generate GOOSE or SV (Sampled Values) messages. When an operation fails, the DUT shall have the capability to provide an output to the tester to verify failing tests. The output may be through at least one of the following: DUT logs and security events (e.g. IEC 62351-14), internal data representation (e.g. if LGOS is supported, the data change in the application) and network management MIBs (e.g. IEC 62351-7). The tests are grouped in tables for each type of tests. In these tables, the test procedures have numeric references. If the test case needs more than one step, it will be enumerated as 1a), 1b), etc. If the test comprises different variants, it will be enumerated as 1-1, 1-2, etc. The test cases in this document should be referred as follows: "Table 1-1a)".

The detailed test procedures are not part of this document and are left to the test labs. Test labs claiming the ability to perform conformance testing to these parts shall be accredited for quality and technical competency by an internationally recognized organization.

4.2.2 Normal procedure tests and resiliency tests

IEC 62351-6 specifies how each IED (client and server) shall execute the procedures in normal conditions (expected behavior) and how it shall behave when unexpected or fault events occur during their execution (negative behaviors).

Normal procedure tests and resiliency tests shall be performed at least once for one of the mandatory cipher suites required by the standard referencing IEC 62351-6.

4.3 Conformance testing requirements

4.3.1 Testing within the context of an application

The test cases listed in this document shall be executed within the context of an application. The DUT claiming conformance to IEC 62351-6 shall execute an application protocol defined in a standard requiring conformance to the IEC 62351-6.

4.3.2 Requirements for the device under test

Prior to the present conformity testing, the DUT should have successfully performed the conformity testing for the base protocol which may include IEC61850 MMS and/or GOOSE and/or SV. It is expected that the DUT submitted for these tests has the same firmware version as the one used in the base protocol testing.

Before the beginning of the testing, the PIDs (Protocol Implementation Documents) that includes all the required parameters, settings and options for a particular protocol implemented in the IED is required. The required PIDs documents include the PICS (Protocol Implementation Conformance Statement) and PIXIT (Protocol Implementation eXtra Information for Testing) that will be provided and referenced by the test lab during the tests.

The entity submitting the device for testing shall provide the following:

- a) The DUT ready for testing;
- b) PICS (Protocol Implementation Conformance Statement);
- c) PIXIT (Protocol Implementation eXtra Information for Testing);
- d) Instruction manuals detailing the installation and operation of the device or assistance for operating the DUT during the test.

A device is ready for testing when the following are satisfied:

- a) The DUT is able to operate as a subscriber and/or publisher according to what has been stated in the PICS.
- b) The DUT shall be configured with a similar configuration submitted for a Client/Server Conformance Test. The supported security features declared in the PICS shall all be configured to allow all applicable test cases to be executed.
- c) The digital and/or analogue data that is in the configuration shall be verifiable in human readable way e.g., by an MMS client read of the data model, via the DUT HMI, LEDs, SNMP MIB Datapoint etc. as described in the DUT base protocol PIXIT. This verification can also include Syslog events according to IEC 62351-14 if supported.
- d) The DUT has successfully passed the initial PIDs verification to ensure all supported features have been presented and detailed. This verification is expected to be in advance of the any test case commencement.

61850 DUT shall also include:

- e) IED capability description in SCL (Substation Configuration Language) format (ICD)
- f) CID (Configured IED Description) and/or SCD (Substation Configuration Description) and/or IID (Instantiated IED description) file in SCL format as supported. The configuration within the configured SCL file shall also match the supported features stated in the PIDs.

4.3.3 Requirements for the test facility

The following requirements shall be satisfied by the test facility:

- The documentation provided with the DUT shall be inspected for correctness and completeness.
- The software and hardware versions of the DUT shall be verified.
- Conformance testing shall be customized for the DUT based on the capabilities identified in the base profile and Security PIDs. Upon this customization, the test facility shall communicate what the tailored test plan will cover.
- The test cases listed in Table 4 and Table 5 shall be performed with no errors detected during testing.
- The test cases should be performed in the order listed and the steps in each test case shall be followed, which means that the DUT is able to function as described in the specific test case.
- For each test case, the test results need to be marked in the appropriate column of the test result chart. Each test case can either pass the test (Passed), fail the test (Failed), not applicable (N.A.), when the configuration value is not supported by the device, or the test case was not performed (Empty). Ideally, there should be no empty box when testing is complete.
- Release a conformance test report of the DUT to the test requester.

The tests can be verified automatically by a testing software or verified manually by review of the test history log after execution provided that the test history log can clearly state which test case is run. If a complete test procedure log is not able to provide a separation with clearly stated test case references, it is expected that a log is inspected after each individual test case. The simulator is preferably flexible in adding or changing test cases in order to be adaptable to changes in the protocol standard and the PID provided with the DUT. In all cases, the test shall be reproducible over time by test engineers in the test facility.

All prerequisites of the tests including PID version numbers, DUT software version, Test Simulator version etc. should be captured in the Test Report and maintained in the event where test engineers need to reproduce the same test e.g., a retest due to failure.

In operational use, the device may show communication and/or behavior errors which forces the supplier to reproduce the complete conformance test (for example for verification afterwards) or for reproducing only the tests that were shown to have errors. It is expected that the DUT and Software version supplied to the test facility is not a Beta version and ready for market.

The test focuses only on the protocol elements and functions as described in the PIDs; the test does not include the application logic and the operation of the tested system.

For client testing, a homologated server shall be used. This server shall have the capability of sending conformant and erroneous message.

For server testing, a homologated client shall be used. This client shall have the capability of sending conformant and erroneous message.

Conformity testing shall be performed again on major software revision changes.