IEC TS 62351-100-6

Edition 1.0 2022-08

TECHNICAL SPECIFICATION

colour inside

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

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

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.

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.

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*