IEC TS 62351-100-4

Edition 1.0 2023-11

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communication security – Part 100-4: Cybersecurity conformance testing for IEC 62351-4

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-8322-7903-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

Part 100-4: Cybersecurity conformance testing for 62351-4

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 62351-100-4 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
57/2505/DTS	57/2564/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.

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.

In this document the following print types are used:

- Abstract Syntax Notation One (ASN.1) and W3C XML Schema Definition (W3C XSD) notions are presented in **`bold Courier New`** typeface; and
- when ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in **`bold Courier New`** typeface.

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/publications.

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 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.

To validate the results of some tests, internal IED information should be made available (see 5.3.4). These requirements are beyond those specified in IEC 62351-4 and therefore the manufacturer/vendor shall describe in Table 2 how the IED can expose the required information.

Conformance testing does not replace project-specific system-related tests such as the POC (Proof Of Concept) FAT (Factory acceptance Test) and SAT (Site Acceptance Test). The POC, 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 POC, 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 the resiliency test cases to demonstrate the capability of the DUT to operate with other devices in the specified way according to IEC 62351-4:2018/AMD1:2020, and also according to the PID (Protocol Implementation Document). Testing of Application layer protocol (61860-8-1, 61850-8-2 or ICCP) features or performances is out of scope.

Through this part of IEC 62351, a test facility can prove that the DUT communication subsystem (or a part of it) conforms to IEC 62351-4:2018/AMD1:2020.

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

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

Part 100-4: Cybersecurity conformance testing for 62351-4

1 Scope

This part of IEC 62351, which is a technical specification, describes test procedures for interoperability conformance testing of data and communication security for power system automation and protection systems which implement MMS, IEC 61850-8-1 (MMS), IEC 61850-8-2 (XMPP) or any other protocol implementing IEC 62351-4:2018/AMD1:2020. The tests described in this document cover only E2E security testing and do not evaluate A-security[1] profile implementation. Thus, citing conformance to this document 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 document 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 document 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 62351-4:2018/AMD1:2020 has correctly implemented all the security functions and that they can be assured to be present in the delivered products. This topic is covered in other IEC standards, for example IEC 62443.

The scope of this document is to specify available common procedures and definitions for conformance and/or interoperability testing of IEC 62351-4:2018/AMD1:2020.

This document deals mainly with cyber 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.

T-profile testing is to be performed prior to E2E security profile testing. T-profile testing is described in IEC 62351-100-3 in the context of IEC 61850-8-1. T-profile testing for IEC 61850-8-2 is to be described in the corresponding IEC 61850-8-2 test specification.

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 62351-4:2018, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*
IEC 62351-4:2018/AMD1:2020

IEC 62351-3:2023, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

---

[1] A-profile is specified in IEC 62351-4:2020 for backward compatibility with IEC 62351-4:2007.

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