IEC TS 62351-100-3

Edition 1.0 2020-01

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communications security – Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

IEC TS 62351-100-3:2020-01(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 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 It also gives information on projects, replaced and withdrawn publications.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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries 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 TS 62351-100-3

Edition 1.0 2020-01

TECHNICAL SPECIFICATION

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-7644-0

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 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

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 62351-100-3, 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
57/2090/DTS	57/2130/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.

This document is to be read in conjunction with IEC 62351-3:2014, IEC 62351-3/AMD1:2018 and IEC 62351-3/AMD2:2020.

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.

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 integrating the IEC 62351-3 security extension for profiles including TCP/IP.

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

Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP

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 IEC 62351-3. Note that conformity to IEC 62351-3 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 the specification of common available procedures and definitions for conformance and/or interoperability testing to ensure conformity to IEC 62351-3. The conformance test cases defined here are focused to verify the conformant integration of the underlying authentication/encryption protocol (TLS), as specified in IEC 62351-3, to protect TCP/IP based communications.

This document is not intended to test the underlying authentication/encryption protocol required by IEC 62351-3 to be implemented over TCP/IP (TLS). The conformance testing of the authentication/encryption protocol over TCP/IP is outside the scope of this document.

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 TS 62351-2:2008, *Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms*

IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles*

[1] The base standard always takes precedence. In case of ambiguity between this technical specification and the base standards (IEC 62351-3), this part of IEC 62351 needs to be clarified or amended.

When testing, negative behavior is not described in the base standard, the behavior 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.

including TCP/IP
IEC 62351-3:2014/AMD1:2018, IEC 62351-3:2014/AMD2:2019

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
client
device receiving or requesting services or information from server devices

Note 1 to entry: In some specifications, a device is commonly called "controlling station" or "master" or "master station".

3.1.2
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

3.1.3
Message Authentication Code (MAC)
calculated value used by a receiving station to authenticate and check the integrity of an information

3.1.4
normal procedure tests
set of test cases to verify that the device fulfils the requirements of IEC 62351-3 in the expected (normal) conditions

3.1.5
Protocol Implementation Conformance Statement (PICS)
summary of the referencing standard capabilities of the system to be tested

3.1.6
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.

3.1.7
protocol Implementation eXtra Information for Testing (PIXIT)
system specific information contained in the PIXIT document regarding the capabilities of the system to be tested, which specifies which items are optional

3.1.8
resiliency tests
set of test cases to verify that the device fulfils the requirements of IEC 62351-3 in reacting to the unexpected (error) conditions

3.1.9
server
device that provides information or services to client devices

Note 1 to entry: In some specifications, a server is commonly called "controlled station" or "outstation" or "slave".

3.1.10
test equipment
all tools and instruments which simulate and verify the communication traffic, inputs and/or outputs of the system under test

3.1.11
test initiator
party initiating a conformance test of a device that is executed by a test facility

3.1.12
test facility
supplier-independent organization which is able to provide appropriate test equipment and trained staff for conformance testing

3.2 Abbreviated terms

Refer to IEC 62351-2 for a list of applicable abbreviated terms. The abbreviations listed below are included here because they are specific to IEC 62351-3 and they may be useful for reading this document as an independent document.

CRL	Certificate Revocation List
DUT	Device Under Test
IP	Inter-Networking Protocol
MAC	Message Authentication Code
OCSP	Online Certificate Status Protocol
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

4 General

4.1 Normatives covered by this document

This document defines the conformance test cases for the requirements defined in IEC 62351-3:2014, IEC 62351-3:2014/AMD1:2018, IEC 62351-3:2014/AMD2:2019 and the parts of the series requiring conformance to IEC 62351-3.

In addition to the test cases described in this document there are further test cases necessary for TLS base protocol RFC as well as test cases depending on the content provided in the certificates. An example may be the RBAC extension specified in IEC 62351-8 or certificate profiles defined in IEC 62351-9.

4.2 Conformance testing structure

4.2.1 General

IEC 62351-3 defines the requirements related to the authentication/encryption protocol, procedures and methods to be implemented at TCP/IP (transport) level.

The conformance test cases are divided into three clauses:

- Clause 5: Verification of configuration parameters. This clause contains the parameters specified by the standards referencing IEC 62351-3 (see IEC 62351-3:2014/AMD1:2018, Clause 7) and affecting the protocol behavior.
- Clause 6: Verification of IEC 62351-3 requirements. The goal of this clause is to verify that DUT is conformant to the requirements of the IEC 62351-3.
- Clause 7: Test result chart. This clause contains the results of the test cases listed in Clause 6 for each supported value of the configuration parameters listed in Clause 5.

The test cases are organized in tables. 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 62351-3 where the clause under test is defined. PICS or PIXIT could be found in the “Reference” column for some test cases whenever the execution of the test case shall take into account specific parameter values declared in the PICS or PIXIT of the DUT.

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 to a clause that is mandatory in IEC 62351-3.

PICS
or
PIXIT = Mandatory test case if the functionality is enabled in the PICS or PIXIT by marking the applicable check box or declaring the applicable value.

4.2.2 Conformance testing addressed per station type

The test cases in Clause 6 to verify the requirements defined in IEC 62351-3 are addressed per station type (client and server).

4.2.3 Normal procedure tests and resiliency tests

IEC 62351-3 specifies how each station (client and server) shall execute the procedures in normal conditions (expected behavior) and also how it shall behave when unexpected or fault events occur during their execution (negative behaviors). So, for each procedure in Clause 6 the test cases are also divided in two sections: the normal procedures test cases addressing the expected behaviors and the resiliency test cases addressing unexpected or fault events.

Normal Procedure tests and Resiliency tests shall be performed according to the parameters values supported by the DUT as defined in Clause 6, declared in the PICS and in the PIXIT of the DUT.

All the tests defined in this technical specification shall be executed for client stations and server stations unless otherwise specified in the test cases.

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 62351-3 shall execute an application protocol defined in a standard requiring conformance to IEC 62351-3.

4.3.2 Requirements for the device under test

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

a) The device ready for testing;

b) The Protocol Implementation Document (PID);

c) 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 requisites are satisfied:

d) The DUT is able to operate as a client or server station according to the PID (depending on the type of DUT).

e) The DUT must be fully configured according to the PID and shall be able to execute all the functionality of the protocol implementation as described in the PID.

f) The functionality described in the PID related to data points such as parameter loading, read procedure, command transmission, etc. is implemented with a representative sub-set of data points.

g) Verification of the data points shall be possible in a human readable way or format, and the verification of analogue and digital status changes is possible.

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. Also, 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 PID (=PICS+PIXIT). Upon this customization, the test facility shall communicate what the tailored test plan will cover.
- The test cases listed in Clauses 5 and 6 shall be performed with no errors detected during testing.
- The test cases in Clause 6 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 listed in Clauses 5 and 6 the test results need to be marked in the appropriate column of the test result chart in Clause 7. Each test case can either pass (Passed), or fail (Failed), or be not applicable (NA) when the configuration value is not supported by the device, or the test case cannot be performed (Empty). Ideally, there should be no empty boxes when the conformance testing is completed.
- Release a conformance test report of the DUT to the test initiator.

All test cases listed in Clause 7 should be verified automatically by a testing software or verified manually by review of the test history log after execution of the test procedures. 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.

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.

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

4.3.4 Test logging

During the execution of conformance testing the following information should be logged by the DUT in a readable format for test results analysis:

- communication events (first handshake, session renegotiation, session resumption);
- certificate check results (e.g. valid, expired, revoked, invalid key length, invalid signature);
- change cipher result (e.g. unsupported).
- The security events raised by the DUT (defined in IEC 62351-3) whenever a negative behavior occurs while performing resiliency tests.

If the specific test logging defined herein and IEC 62351-3 is not supported by the DUT, the DUT shall provide the means by which the tester can verify the proper execution of the test cases.

5 Verification of Configuration parameters

5.1 General

The scope of this clause is to verify the configuration of all the parameters that affect security extension procedures and protocol behavior so that the whole or part of conformance testing shall be executed (and the tests result chart in Clause 7 shall be filled accordingly) for each value of these parameters as indicated in 5.2. Basically, the DUT must be tested to verify that the whole functionality and behavior are correct according to the configuration(s) defined in Table 1.

5.2 Configuration parameters

Table 1 – Configuration Parameters

No.	Test	Definition	Reference	Required
5.2.1	Station Type	Client, Server	PICS	M
		All conformance tests listed in Clause 6 shall be performed for each station type supported.		
5.2.2	TCP IP Port to be used for secure communication	All conformance tests listed in Clause 6 shall be performed for the value of this parameter.	IEC 62351-3:2014, Clause 7 PICS	M
5.2.3	TLS Versions	TLS protocol versions supported.	IEC 62351-3:2014, 5.2 PICS, PIXIT	M
		All conformance tests listed in Clause 6 shall be performed for each value (mandatory and optional) supported in this parameter.		
5.2.4	TLS Cipher Suites	Set of cipher suites supported in TLS protocol.	IEC 62351-3:2014, Clause 7 PICS, PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		
5.2.5	Public Key Lengths	Public Key lengths supported in certificate signing and TLS session key exchange.	IEC 62351-3:2014, 5.6.4.6 IEC 62351-3:2014, 5.6.4.7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		

No.	Test	Definition	Reference	Required
5.2.6	Certificates Revocation Check methods	Methods to verify the Certificate Revocation Status (CRL/OCSP).	IEC 62351-3:2014, 5.6.4.4 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed for each value supported in this parameter.		
5.2.7	Certificate Revocation Check Interval	Configured interval for Certificate Revocation check. NOTE During conformance testing, to facilitate the execution of the test cases involving this parameter, this value can be decreased.	IEC 62351-3:2014, 5.6.4.4 IEC 62351-3:2014, Clause 7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		
5.2.8	TLS Session Renegotiation Interval	Configured interval for Session Renegotiation NOTE During conformance testing, to facilitate the execution of the test cases involving this parameter, this value can be decreased.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		
5.2.9	TLS Session Resumption Interval	Configured interval for Session Resumption Note: During conformance testing, to facilitate the execution of the test cases involved by this parameter, this value can be decreased.	IEC 62351-3:2014, 5.3 IEC 62351-3:2014, Clause 7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		
5.2.10	Number of CA supported	Recommended minimum number of Certification Authority supported	IEC 62351-3:2014, 5.6 IEC 62351-3:2014, Clause 7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed at least for the minimum mandatory value supported in this parameter.		
5.2.11	Maximum certificate size	Maximum public key certificate size supported	IEC 62351-3:2014, 5.6.2 IEC 62351-3:2014, Clause 7 PIXIT	M
		All conformance tests listed in Clause 6 shall be performed for the maximum mandatory value supported in this parameter		

6 Verification of IEC 62351-3 requirements

6.1 General

This clause defines the conformance test procedure to be performed to verify that the DUT correctly implements the requirements defined in the IEC 62351-3. To proceed with the execution of conformance tests listed in this clause, a valid PKI certificate for TLS shall be pre-installed on the DUT.

6.2 Normal procedure test cases

Table 2 describes the normal procedures test cases to verify the behavior of the DUT in normal (expected) conditions.

Table 2 – IEC 62351-3 requirements: Normal procedure tests

No.	Test	Reference	Required
6.2.1	The DUT (Client only) initiates the TCP/IP connection to the Server using remote station TCP/IP port specified for secure communication.	IEC 62351-3:2014, Clause 7 PICS	M
6.2.2	The DUT (Server only) accepts the TCP/IP connection on TCP/IP port specified for secure communication.	IEC 62351-3:2014, Clause 7 PICS	M
6.2.3	The DUT (Client only) performs the Initial TLS Handshake upon the connection is established and no previous TLS Session was established.	IEC 62351-3:2014, 5.4	M
6.2.4	The DUT (Server only) performs Session Renegotiation at the configured interval for Session Renegotiation, in an ongoing TLS Session by sending the HelloRequest to the client.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7 PICS	M
6.2.5	If the DUT (Client only) does not receive a TLS session renegotiation request (HelloRequest) from the Server at the expected interval, the DUT initiates the TLS session renegotiation by sending the ClientHello to the Server.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7 PICS	M
6.2.6	If CRL certificate check method is used, at least one TLS renegotiation is synchronized with (performed immediately after) the CRL update.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7 (see Note 1)	PIXIT
6.2.7	If OCSP certificate check method is supported, the TLS Session Renegotiation is performed at the Configured interval for Certificate Revocation check.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7	PICS

No.	Test	Reference	Required
6.2.8	The DUT supports at least minimum number of root CAs (has the corresponding number of root CA certificates installed locally).	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7 PICS	M
6.2.9	The DUT accepts any Remote Station certificate from one or more authorized CA locally configured, after successful validation.	IEC 62351-3:2014, 5.6.4.2 PICS	M
6.2.10	The DUT accepts one or more specific Remote Station certificate (locally configured) from one or more authorized CA (locally configured).	IEC 62351-3:2014, 5.6.4.3 PICS	M
6.2.11	During the initial handshake the DUT (Client only) provides the Trusted CA Indication in the ClientHello message.	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS
6.2.12	During the initial handshake, the DUT (Server only), in the Server Certificate message, provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS
6.2.13	During the initial handshake, the DUT performs Mutual Authentication with the Remote Station.	IEC 62351-3:2014, 5.6.3	M
6.2.14	During the initial handshake, the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is supported.	IEC 62351-3:2014, 5.5	M
6.2.15	During the initial handshake, the TLS Session Extension defined in RFC5746 is supported.	IEC 62351-3:2014, 5.4	M
6.2.16	During the initial handshake, the DUT accept remote certificates having size limited to the maximum certificate size supported.	IEC 62351-3:2014, 5.6.2 IEC 62351-3:2014, Clause 7	M
6.2.17	During the initial handshake, the process of accessing the CRL to check the status of the received certificate, does not cause the established TCP/IP connection or the initial handshake to be terminated, if the received certificate is valid.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT
6.2.18	During the initial handshake, the process of accessing the OCSP responder to check the status of the received certificate, does not cause the established TCP/IP connection or the initial handshake to be terminated, if the received certificate is valid.	IEC 62351-3:2014, 5.6.4.4	PICS
6.2.19	During the session renegotiation, the DUT (Client only) provides the Trusted CA Indication in the ClientHello message.	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS

No.	Test	Reference	Required
6.2.20	During the session renegotiation, the DUT (Server only), in the Server Certificate message, provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	IEC 62351-3:2014, 5.6.1	PICS
6.2.21	During the session renegotiation, the DUT performs Mutual Authentication with the Remote Station.	IEC 62351-3:2014, 5.6.3	M
6.2.22	During the session renegotiation, the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is supported.	IEC 62351-3:2014, 5.5	M
6.2.23	During the session renegotiation, the TLS Session Extension defined in RFC5746 is supported.	IEC 62351-3:2014, 5.4	M
6.2.24	During the session renegotiation, The DUT accept remote certificates having size limited to the maximum certificate size supported.	IEC 62351-3:2014 5.6.2 PIXIT	M
6.2.25	During the session renegotiation, the process of accessing the CRL to check the status of the received certificate, does not cause the established TCP/IP connection or the TLS session to be terminated, if the received certificate is valid.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT
6.2.26	During the session renegotiation, the process of accessing the OCSP responder to check the status of the received certificate, does not cause the established TCP/IP connection or the TLS session to be terminated, if the received certificate is valid.	IEC 62351-3:2014, 5.6.4.4	PICS
6.2.27	The DUT (Client only) is able to perform the TLS Session Resumption (initiated by sending the ClientHello message to the Server) upon the TCP/IP connection is re-established, if a previous TLS Session was dropped within the Configured interval for Session Renegotiation.	IEC 62351-3:2014, 5.3 IEC 62351-3:2014, Clause 7 PIXIT	M
6.2.28	The DUT (Client only) is able to perform the TLS Session Resumption (initiated by sending the ClientHello message to the Server) at the Configured interval for Session Resumption, in an ongoing TLS Session.	IEC 62351-3:2014, 5.3 IEC 62351-3:2014, Clause 7 PIXIT	M
6.2.29	The DUT (Server only) is able to perform the TLS Session Resumption (by sending the HelloRequest message to the Client) at the Configured interval for Session Resumption, in an ongoing TLS Session.	IEC 62351-3:2014, 5.3 IEC 62351-3:2014, Clause 7 PIXIT	M

6.3 Resiliency test cases

Table 3 describes the resiliency procedures test cases to verify the behavior of the DUT when unexpected or fault events occur.

Table 3 – IEC 62351-3 requirements: Resiliency tests

No.	Test	Action	Reference	Required
6.3.1	During the initial handshake, the Remote Station proposes TLS version 1.1 and this version is supported by the DUT.	The DUT shall perform the following actions: - Raise the security event “Warning: Insecure TLS version” - Maintain the TCP/IP connection and continue the TLS handshake procedure	IEC 62351-3:2014, 5.2 IEC 62351-3:2014, Clause 7 PICS	PICS
6.3.2	During the initial handshake, the Remote Station proposes TLS version 1.0 and this version is supported by the DUT.	The DUT shall perform the following actions: - Raise the security event “Warning: Insecure TLS version” - Maintain the TCP/IP connection and continue the TLS handshake procedure	IEC 62351-3:2014, 5.2 IEC 62351-3:2014, Clause 7 PICS	PICS
6.3.3	During the initial handshake, the Remote Station proposes TLS version prior to 1.2 and not supported by the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: Unsecure communication” - Close the TCP/IP connection.	IEC 62351-3:2014, 5.2 IEC 62351-3:2014, Clause 7 PICS	M
6.3.4	During the initial handshake, the DUT is not able to access to the CRL and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: CRL not accessible”. - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT
6.3.5	During the initial handshake, the CRL is not updated (validity time expired) and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: CRL expired”. - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT
6.3.6	During the initial handshake, The DUT is not able to access to the OCSP responder and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: OCSP responder not accessible”. - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 2)	PICS
6.3.7	During the initial handshake, The DUT is able to access to the OCSP responder but the OCSP response expired and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: OCSP response expired”. - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014 5.6.4.4	PICS

No.	Test	Action	Reference	Required
6.3.8	During the initial handshake, the Remote Station proposes none of the mandatory TLS cipher suites and none implemented in the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: No matching TLS cipher suites” - Close the TCP/IP connection	IEC 62351-3:2014, 5.1 IEC 62351-3:2014, Clause 7 PICS	M
6.3.9	During the initial handshake, the Remote Station does not provide the certificate.	The DUT shall perform the following actions: - Raise the security event “Alarm: certificate unavailable” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.3	M
6.3.10	During the initial handshake, the DUT receives a Remote Station’s certificate having size longer than the maximum certificate size supported.	The DUT shall perform the following actions: - Raise the security event “Alarm: TLS certificate size exceeded” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.2 IEC 62351-3:2014, Clause 7 PICS	M
6.3.11	During the initial handshake, the DUT receives a Remote Station’s certificate referring to a CA for which the certificate is not installed in the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: certificate validation: CA certificate not available” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.2	M
6.3.12	During the initial handshake, the DUT receives a Remote Station’s certificate referring to a CA for which the certificate is installed in the DUT, but the Remote Station’s individual certificate is not specifically configured in the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: certificate validation: trusted individual certificate not available” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.3 IEC 62351-3:2014, Clause 7	M
6.3.13	During the initial handshake, the DUT (Server only) is NOT able to provide a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	The DUT (Server only) shall perform the following actions: - Raise the security event “Alarm: CA certificate not found” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS
6.3.14	During the initial handshake, the DUT (Client only) receives a Remote Station’s certificate NOT belonging to any of the Certificate Chains selected in the Trusted CA Indication of the last ClientHello message transmitted.	The DUT (Client only) shall perform the following actions: - Raise the security event “Alarm: certificate unavailable” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS
6.3.15	During the initial handshake, the DUT receives an expired Remote Station’s certificate.	The DUT shall perform the following actions: - Raise the security event “Alarm: expired certificate” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.5	M
6.3.16	During the initial handshake, the DUT receives a revoked Remote Station’s certificate.	The DUT shall perform the following actions: - Raise the security event “Alarm: revoked certificate” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.4	M

No.	Test	Action	Reference	Required
6.3.17	During the initial handshake, the DUT receives a Remote Station's certificate with a public key length equal to the minimum for legacy mode and is supported by the DUT.	The DUT shall perform the following actions: - Raise the security event "Warning: minimum key length". - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014, 5.6.4.7 PICS	M
6.3.18	During the initial handshake, the DUT receives a Remote Station's certificate with a public key length shorter than the minimum supported.	The DUT shall perform the following actions: - Raise the security event "Alarm: Insufficient key length". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.7 PIXIT	M
6.3.19	During the initial handshake, the DUT receives a Remote Station's certificate specifying an unsupported certificate signature algorithm.	The DUT shall perform the following actions: - Raise the security event "Alarm: Algorithm not supported". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.6 PIXIT	M
6.3.20	During the initial handshake, the DUT receives a Remote Station's certificate with a not valid signature.	The DUT shall perform the following actions: - Raise the security event "Alarm: certificate validation: certificate signature could not be validated". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.6	M
6.3.21	During the session resumption, the Remote Station negotiates a TLS version different from the initial handshake.	The DUT shall perform the following actions: - Raise the security event "Alarm: TLS version change detected" - Close the TCP/IP connection	IEC 62351-3:2014, 5.2 IEC 62351-3:2014, Clause 7 PICS	M
6.3.22	Session renegotiation interval expired: after sending a HelloRequest message to the Client, the DUT (Server only) does not receive the TLS Session Renegotiation request from the Client.	The DUT (Server only) shall perform the following actions: - Raise the security event "Alarm: session renegotiation interval expired". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.4 IEC 62351-3:2014, Clause 7	M
6.3.23	During the session renegotiation, the Remote Station negotiates a TLS version different from the initial handshake.	The DUT shall perform the following actions: - Raise the security event "Alarm: TLS version change detected" - Close the TCP/IP connection	IEC 62351-3:2014, 5.2 IEC 62351-3:2014, Clause 7 PICS	M
6.3.24	During the session renegotiation, the DUT is not able to access the CRL and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event "Warning: CRL not accessible". - Maintain the TCP/IP connection and continue the TLS renegotiation procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT
6.3.25	During the session renegotiation, the CRL is not updated (validity time expired) and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event "Warning: CRL expired". - Maintain the TCP/IP connection and continue the TLS renegotiation procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 1)	PIXIT

No.	Test	Action	Reference	Required
6.3.26	During the session renegotiation, the DUT is not able to access to the OCSP responder and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: OCSP responder not accessible”. - Maintain the TCP/IP connection and continue the TLS renegotiation procedure.	IEC 62351-3:2014, 5.6.4.4 (see Note 2)	PICS
6.3.27	During the session renegotiation, The DUT is able to access to the OCSP responder but the OCSP response expired and the certificate received is valid.	The DUT shall perform the following actions: - Raise a security event “Warning: OCSP response expired”. - Maintain the TCP/IP connection and continue the TLS renegotiation procedure.	IEC 62351-3:2014, 5.6.4.4	PICS
6.3.28	During session renegotiation, the Remote Station does not provide the certificate.	The DUT shall perform the following actions: - Raise the security event “Alarm: Certificate unavailable” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.3	M
6.3.29	During session renegotiation, the DUT receives a Remote Station’s certificate having size longer than the maximum certificate size supported.	The DUT shall perform the following actions: - Raise the security event “Alarm: TLS certificate size exceeded” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.2 IEC 62351-3:2014, Clause 7 PICS	M
6.3.30	During session renegotiation, the DUT receives a Remote Station’s certificate referring to a CA for which the certificate is not installed in the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: certificate validation: CA certificate not available” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.2	M
6.3.31	During session renegotiation, the DUT receives a Remote Station’s certificate referring to a CA for which the certificate is installed in the DUT, but the individual Remote Station certificate’s is not specifically configured in the DUT.	The DUT shall perform the following actions: - Raise the security event “Alarm: certificate validation: trusted individual certificate not available” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.3 IEC 62351-3:2014, Clause 7	M
6.3.32	During session renegotiation, the DUT (Server only) is NOT able to provide a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	The DUT (Server only) shall perform the following actions: - Raise the security event “Alarm: CA certificate not found” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS
6.3.33	During session renegotiation, the DUT (Client only) receives a Remote Station’s certificate NOT belonging to any of the Certificate Chains selected in the Trusted CA Indication of the last ClientHello message transmitted.	The DUT (Client only) shall perform the following actions: - Raise the security event “Alarm: certificate validation: CA certificate not available” - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.1 IEC 62351-3:2014, Clause 7	PICS

No.	Test	Action	Reference	Required
6.3.34	During session renegotiation, the DUT receives an expired Remote Station's certificate.	The DUT shall perform the following actions: - Raise the security event "Alarm: Expired certificate" - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.5	M
6.3.35	During session renegotiation, the DUT receives a revoked Remote Station's certificate.	The DUT shall perform the following actions: - Raise the security event "Alarm: Revoked certificate" - Close the TCP/IP connection	IEC 62351-3:2014, 5.6.4.4	M
6.3.36	During session renegotiation, the DUT receives a Remote Station's certificate with a public key length equal to the minimum for legacy mode and is supported by the DUT.	The DUT shall perform the following actions: - Raise the security event "Warning: Minimum key length". - Maintain the TCP/IP connection and continue the TLS handshake procedure.	IEC 62351-3:2014, 5.6.4.7 PICS	M
6.3.37	During session renegotiation, the DUT receives a Remote Station's certificate with a public key length shorter than the minimum supported.	The DUT shall perform the following actions: - Raise the security event "Alarm: Insufficient key length". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.7	M
6.3.38	During session renegotiation, the DUT receives a Remote Station's certificate specifying an unsupported certificate signature algorithm.	The DUT shall perform the following actions: - Raise the security event "Alarm: Algorithm not supported". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.6 PIXIT	M
6.3.39	During session renegotiation, the DUT receives a Remote Station's certificate with a NOT valid signature.	The DUT shall perform the following actions: - Raise the security event "Alarm: certificate validation: certificate signature could not be validated". - Close the TCP/IP connection.	IEC 62351-3:2014, 5.6.4.6	M

(1) The test cases testing the inability to access the CRL or the CRL validity during TLS first handshake or TLS renegotiation can be performed if the CRL repository is external to the DUT. The CRL location shall be declared in the PIXIT.

(2) The test cases testing the inability to access the OCSP responder during TLS first handshake or TLS renegotiation can be performed by interrupting the connection between the DUT and the OCSP responder.

7 Tests Results Chart

7.1 Verification of Configuration Parameters

The results of the tests cases in Subclause 5.2 need to be charted in the Table 4.

Table 4 – Test results chart: Verification of configuration parameters

Configuration Parameters		√.......... indicates the Test Case has PASSED FAIL...... indicates the Test Case has FAILED N.A....... indicates that Configuration Value is NOT SUPPORTED by the device Empty....... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in IEC 62351-3	
Test	**No.**	**Description**	**Result**
Configuration Parameters	5.2.1	Station Type (Client, Server)	
	5.2.2	TCP IP Port to be used for secure communication	
	5.2.3	TLS Versions	
	5.2.4	TLS Cipher Suites	
	5.2.5	Public Key Lengths	
	5.2.6	Certificates Revocation Check methods	
	5.2.7	Certificate Revocation Check Interval	
	5.2.8	TLS Session Renegotiation Interval	
	5.2.9	TLS Session Resumption Interval	
	5.2.10	Number of CA supported	
	5.2.11	Maximum certificate size	

7.2 Verification of IEC 62351-3 requirements

The results of the tests cases in Subclauses 6.2 and 6.3 need to be charted in the Table 5.

Table 5 – Test results chart: Verification of IEC 62351-3 requirements

Verification of Procedures **IEC 62351-3 requirements**		Record the test cases result on the right for each configuration value supported (see clause 6): √.......... indicates the Test Case has PASSED FAIL...... indicates the Test Case has FAILED N.A....... indicates that Configuration Value is NOT SUPPORTED by the device Empty....... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in IEC 62351-3	**Station Type**	
			Client Station	**Server Station**
Test	**No.**	**Description**	**Result**	
Normal Procedure	6.2.1	The DUT (Client only) initiates the TCP/IP connection to the Server using remote station TCP/IP port specified for secure communication.		■
	6.2.2	The DUT (Server only) accepts the TCP/IP connection on TCP/IP port specified for secure communication.	■	
	6.2.3	The DUT (Client only) performs the Initial TLS Handshake upon the connection is established and no previous TLS Session was established.		■
	6.2.4	The DUT (Server only) performs Session Renegotiation at the configured interval for Session Renegotiation, in an ongoing TLS Session by sending the HelloRequest to the client.	■	
	6.2.5	If the DUT (Client only) does not receive a TLS session renegotiation request (HelloRequest) from the Server at the expected interval, the DUT initiates the TLS session renegotiation by sending the ClientHello to the Server.		■
	6.2.6	If CRL certificate check method is used, at least one TLS renegotiation is synchronized with (performed immediately after) the CRL update.		
	6.2.7	If OCSP certificate check method is supported, the TLS Session Renegotiation is performed at the Configured interval for Certificate Revocation check.		
	6.2.8	The DUT supports at least minimum number of root CAs (has the corresponding number of root CA certificates installed locally).		
	6.2.9	The DUT accepts any Remote Station certificate from one or more authorized CA locally configured, after successful validation.		
	6.2.10	The DUT accepts one or more specific Remote Station certificate (locally configured) from one or more authorized CA (locally configured).		
	6.2.11	During the initial handshake the DUT (Client only) provides the Trusted CA Indication in the ClientHello message.		■
	6.2.12	During the initial handshake, the DUT (Server only), in the Server Certificate message, provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	■	

Verification of Procedures **IEC 62351-3 requirements**		Record the test cases result on the right for each configuration value supported (see clause 6): √.......... indicates the Test Case has PASSED FAIL...... indicates the Test Case has FAILED N.A....... indicates that Configuration Value is NOT SUPPORTED by the device Empty....... indicates the Test Case was NOT PERFORMED Black Box... indicates the Test Case is NOT APPLICABLE in IEC 62351-3	**Station Type**	
			Client Station	**Server Station**
Test	**No.**	**Description**	**Result**	
Normal Procedure *(continued)*	6.2.13	During the initial handshake, the DUT performs Mutual Authentication with the Remote Station.		
	6.2.14	During the initial handshake, the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is supported.		
	6.2.15	During the initial handshake, the TLS Session Extension defined in RFC5746 is supported.		
	6.2.16	During the initial handshake, The DUT accept remote certificates having size limited to the maximum certificate size supported.		
	6.2.17	During the initial handshake, the process of accessing the CRL to check the status of the received certificate, does not cause the established TCP/IP connection or the initial handshake to be terminated, if the received certificate is valid.		
	6.2.18	During the initial handshake, the process of accessing the OCSP responder to check the status of the received certificate, does not cause the established TCP/IP connection or the initial handshake to be terminated, if the received certificate is valid.		
	6.2.19	During the session renegotiation, the DUT (Client only) provides the Trusted CA Indication in the ClientHello message.		■
	6.2.20	During the session renegotiation, the DUT (Server only), in the Server Certificate message, provides a certificate selected from the Certificate Chain specified in the Trusted CA Indication of the last ClientHello message received.	■	
	6.2.21	During the session renegotiation, the DUT performs Mutual Authentication with the Remote Station.		
	6.2.22	During the session renegotiation, the Message Authentication Code (MAC) option, with the specific algorithm indicated in the cipher suites selected, is supported.		
	6.2.23	During the session renegotiation, the TLS Session Extension defined in RFC5746 is supported.		

Verification of Procedures **IEC 62351-3 requirements**		Record the test cases result on the right for each configuration value supported (see clause 6): √………. indicates the Test Case has PASSED FAIL…… indicates the Test Case has FAILED N.A……. indicates that Configuration Value is NOT SUPPORTED by the device Empty……. indicates the Test Case was NOT PERFORMED Black Box… indicates the Test Case is NOT APPLICABLE in IEC 62351-3	**Station Type**	
			Client Station	**Server Station**
Test	**No.**	**Description**	**Result**	
Normal Procedure *(continued)*	6.2.24	During the session renegotiation, The DUT accept remote certificates having size limited to the maximum certificate size supported.		
	6.2.25	During the session renegotiation, the process of accessing the CRL to check the status of the received certificate, does not cause the established TCP/IP connection or the TLS session to be terminated, if the received certificate is valid.		
	6.2.26	During the session renegotiation, the process of accessing the OCSP responder to check the status of the received certificate, does not cause the established TCP/IP connection or the TLS session to be terminated, if the received certificate is valid.		
	6.2.27	The DUT (Client only) is able to perform the TLS Session Resumption (initiated by sending the ClientHello message to the Server) upon the TCP/IP connection is re-established, if a previous TLS Session was dropped within the Configured interval for Session Renegotiation.		■
	6.2.28	The DUT (Client only) is able to perform the TLS Session Resumption (initiated by sending the ClientHello message to the Server) at the Configured interval for Session Resumption, in an ongoing TLS Session.		■
	6.2.29	The DUT (Server only) is able to perform the TLS Session Resumption (by sending the HelloRequest message to the Client) at the Configured interval for Session resumption, in an ongoing TLS Session.	■	
Resiliency Test	6.3.1	During the initial handshake, the Remote Station proposes TLS version 1.1 and this version is supported by the DUT.		
	6.3.2	During the initial handshake, the Remote Station proposes TLS version 1.0 and this version is supported by the DUT.		
	6.3.3	During the initial handshake, the Remote Station proposes TLS version prior to 1.2 and not supported by the DUT.		