INTERNATIONAL STANDARD

IEC 61400-25-5

First edition
2006-12

Wind turbines –

Part 25-5:
Communications for monitoring and control of wind power plants – Conformance testing

Reference number
IEC 61400-25-5:2006(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**

- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

IEC 61400-25-5

First edition
2006-12

Wind turbines –

Part 25-5: Communications for monitoring and control of wind power plants – Conformance testing

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE X

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

WIND TURBINES –

Part 25-5: Communications for monitoring and control of wind power plants – Conformance testing

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

International Standard IEC 61400-25-5 has been prepared by IEC technical committee 88: Wind turbines.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The text of this standard is based on the following documents:

FDIS	Report on voting
88/277/FDIS	88/283/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

A list of all parts of the IEC 61400 series, under the general title *Wind turbines* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

The IEC 61400-25 series defines communication for monitoring and control of wind power plants. The modeling approach of the IEC 61400-25 series has been selected to provide abstract definitions of classes and services such that the specifications are independent of specific protocol stacks, implementations, and operating systems. The mapping of these abstract classes and services to a specific communication profile may be found in IEC 61400-25-4[1].

This part of IEC 61400-25 defines the methods and abstract test cases for conformance testing of devices used in wind power plants. The intended readers are test system developers.

NOTE 1 It is recommended to obtain a common knowledge of the standards IEC 61400-25-1, IEC 61400-25-2, IEC 61400-25-3, and IEC 61400-25-4 before reading this part.

NOTE 2 Abbreviations used in IEC 61400-25-5 may be listed in Clause 3 or may be found in other parts of IEC 61400-25 that are relevant for conformance testing.

[1] To be published.

WIND TURBINES –

Part 25-5: Communications for monitoring and control of wind power plants – Conformance testing

1 Scope

The focus of the IEC 61400-25 series is on the communications between wind power plant components such as wind turbines and actors such as SCADA Systems. Internal communication within wind power plant components is outside the scope of the IEC 61400-25 series.

The IEC 61400-25 series is designed for a communication environment supported by a client-server model. Three areas are defined, that are modelled separately to ensure the scalability of implementations:

1) wind power plant information models,
2) information exchange model, and
3) mapping of these two models to a standard communication profile.

The wind power plant information model and the information exchange model, viewed together, constitute an interface between client and server. In this conjunction, the wind power plant information model serves as an interpretation frame for accessible wind power plant data. The wind power plant information model is used by the server to offer the client a uniform, component-oriented view of the wind power plant data. The information exchange model reflects the whole active functionality of the server. The IEC 61400-25 series enables connectivity between a heterogeneous combination of client and servers from different manufacturers and suppliers.

As depicted in Figure 1, the IEC 61400-25 series defines a server with the following aspects:

– Information provided by a wind power plant component, e. g., “wind turbine rotor speed” or “total power production of a certain time interval” is modelled and made available for access. The information modelled in the standard is defined in part IEC 61400-25-2,
– services to exchange values of the modelled information defined in part IEC 61400-25-3,
– mapping to a communication profile, providing a protocol stack to carry the exchanged values from the modelled information (part IEC 61400-25-4).

The IEC 61400-25 series only defines how to model the information, information exchange and mapping to specific communication protocols. The IEC 61400-25 series excludes a definition of how and where to implement the communication interface, the application program interface and implementation recommendations. However, the objective of the IEC 61400-25 series is that the information associated with a single wind power plant component (such as the wind turbine) is accessible through a corresponding logical device.

This part of IEC 61400-25 specifies standard techniques for testing of conformance of implementations, as well as specific measurement techniques to be applied when declaring performance parameters. The use of these techniques will enhance the ability of users to purchase systems that integrate easily, operate correctly, and support the applications as intended.

NOTE The role of the test facilities for conformance testing and certifying the results are outside of the scope of IEC 61400-25-5.

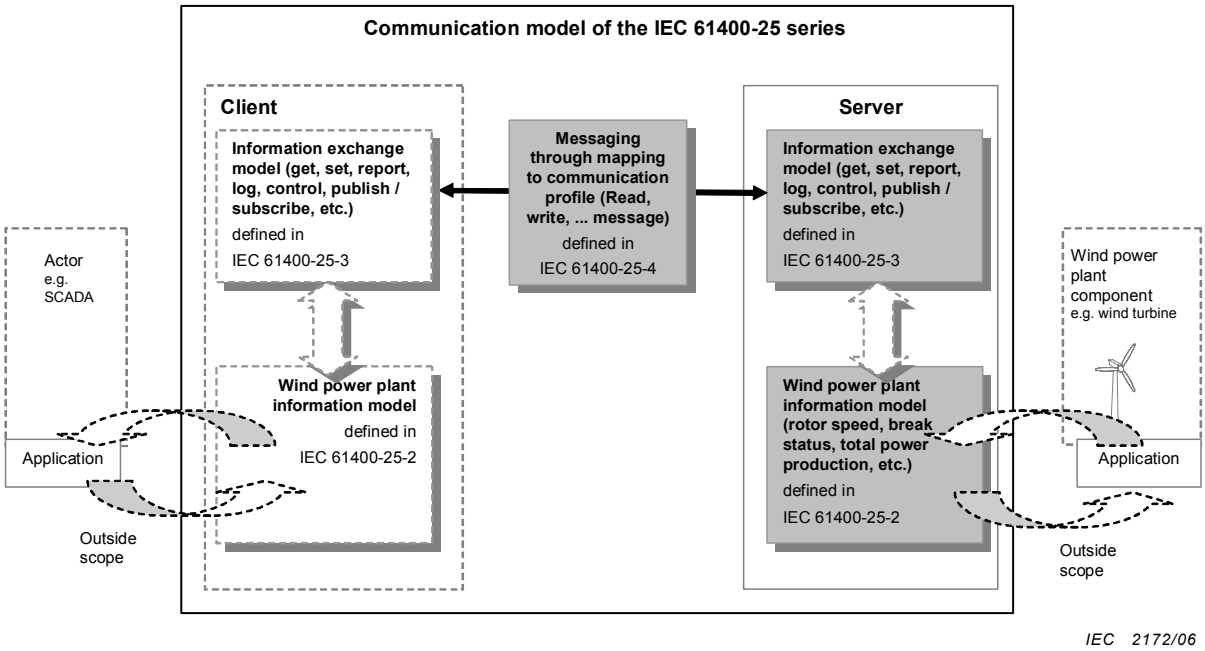

Figure 1 – Conceptual communication model of the IEC 61400-25 series

2 Normative references

The following referenced documents are indispensable for the application 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 61400-25 (all parts), *Wind turbines - Part 25: Communications for monitoring and control of wind power plants*

IEC 61850-7-1:2003, *Communication networks and systems in substations – Part 7-1: Basic communication structure for substations and feeder equipment – Principles and models*

IEC 61850-7-2:2003, *Communication networks and systems in substations – Part 7-2: Basic communication structure for substations and feeder equipment – Abstract communication service interface (ACSI)*

IEC 61850-7-4:2003, *Communication networks and systems in substations – Part 7-4: Basic communication structure for substations and feeder equipment – Compatible logical node and data classes*

ISO/IEC 9646 (all parts), *Information technology – Open Systems Interconnection – Conformance testing methodology and framework*

3 Terms and definitions

For the purpose of this document, the terms and definitions defined in IEC 61400-25-1 and the following apply.

3.1
Factory Acceptance Test
FAT
customer agreed functional tests of the specifically manufactured substation automation system or its parts using the parameter set for the planned application.

The FAT shall be carried out in the factory of the manufacturer or other agreed-upon location by the use of process simulating test equipment

3.2
interoperability
ability of two or more devices from the same vendor (or different vendors) to exchange information and use that information for correct co-operation. A set of values defined corresponds with the quantities or values of another set

3.3
Model Implementation Conformance Statement
MICS
details the standard data object model elements supported by the system or device

3.4
negative test
test to verify the correct response of a device or a system when subjected to:

– IEC 61400-25 series conformant information and services which are not implemented in the device or system under test,

– non IEC 61400-25 series conformant information and services sent to the device or system under test.

3.5
Protocol Implementation Conformance Statement
PICS
summary of the capabilities of the system to be tested

3.6
Protocol Implementation Extra Information For Testing
PIXIT
the Protocol Implementation eXtra Information for Testing document contains system specific information regarding the capabilities of the system to be tested and which are outside the scope of the IEC 61400-25 series

NOTE The PIXIT is not subject to standardisation.

3.7
routine test
performed by the manufacturer in order to ensure device operation and safety

3.8
Site Acceptance Test
SAT
verification of each data and control point and the correct functionality within the WPP and its operating environment at the whole installed plant by use of the final parameter set. The SAT is the precondition for the WPP being put into operation.

3.9
system test
verification of correct behaviour of the WPP components and of the overall WPP under various application conditions

NOTE The system test marks the final stage of the development of a WPP system component.

3.10
test equipment
all tools and instruments which simulate and verify the input/outputs of the operating environment of the WPP such as wind turbine, switchgear, transformers, network control centres or connected telecommunication units on the one side, and the communication links between the system components of the WPP on the other

3.11
test facility
organisation able to provide appropriate test equipment and trained staff for conformance testing

NOTE The management of conformance tests and the resulting information should follow a quality system.

3.12
type test
verification of correct behaviour of the systems components of the WPP by use of the system tested software under the test conditions corresponding with the technical data

NOTE The type test marks the final stage of the hardware development and is the precondition for the start of the production. This test shall be carried out with system components which have been manufactured through the normal production cycle.

3.13
witness point
point, defined in the appropriate document at which an inspection will take place on an activity. The activity may proceed without the approval of the initiator of the conformance test. The test facility provides a written notice to the initiator at an agreed time prior to the witness point. The initiator or his representative has the right, but is NOT obligated, to verify the witness point

4 Abbreviated terms

ACSI	Abstract Communication Service Interface
BRCB	Buffered Report Control Block
DUT	Device Under Test
FAT	Factory Acceptance Test
GI	General Interrogation
HMI	Human Machine Interface
IED	Intelligent Electronic Device
IP	Inter-networking protocol internet Protocol
LCB	Log Control Block
LD	Logical Device
LN	Logical Node
MICS	Model Implementation Conformance Statement
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
RCB	Report Control Block
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SCSM	Specific Communication Service Mapping
SoE	Sequence-of-Events
SUT	System Under Test
TPAA	Two Party Application Association
URCB	Unbuffered Report Control Block
UTC	Coordinated Universal Time
WPP	Wind Power Plant

5 Introduction to conformance testing

5.1 General

There are many steps involved from the development and production of a device to the proper running of a complete system designed according the specific needs of a customer. Suitable test steps are incorporated in this process.

Many internal tests during the development of a device (or a system kit) result in a type test (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 part of the IEC 61400-25 series, the term type test is restricted to the functional behaviour of the device excluding communication.

Continuing routine tests in the production chain are necessary to ensure a constant quality of delivered devices in accordance with the quality procedures of the producer.

A conformance test is the type test for communication and – since communication establishes a system – the basic integrated systems test of the incorporated system components. As a global communications standard, the IEC 61400-25 series includes standardised conformance tests to insure that all suppliers comply with applicable requirements.

Type tests and conformance tests do not completely guarantee that all functional and performance requirements are met. However, when properly performed, such tests significantly reduce the risk of costly problems occurring during system integration in the factory and on-site.

Conformance testing does not replace project specific system tests such as the FAT and SAT. The FAT and SAT are based on customer requirements for a dedicated WPP 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 WPP system is performing as specified.

5.2 Conformance test procedures

In general, conformance testing of the communication behaviour of a system component should address the functional requirements and performance requirements of typical applications supported by these devices in a WPP.

Conformance testing demonstrates the capability of the Device Under Test (DUT) to operate with other system components in a specified way according to the IEC 61400-25 series.

Conformance testing requires consideration of the following issues:

– The problem of all testing is the completeness of the tests. The number of all possible situations can be very large. It may be possible to cover all normal operating cases, but this may not be true for all failure cases.
– It is impossible to test all system configurations using system components from different world-wide suppliers. Therefore, standardised test architecture with device simulators should be used. The use of such test architecture implies agreement about its configuration and the test procedures applied in order to achieve compatible results.
– A communication standard does not standardise the functions of the communicating equipment. Therefore, the failure modes of the functions are outside the scope of this part of the IEC 61400-25 series. But both the existence of distributed functions and the impact of function response in devices on the data flow, create some interdependence.
– Depending on the definition range of the IEC 61400-25 series, some properties of the device may be proven by information and documents provided with the DUT for the conformance testing instead of the conformance test itself.

The conformance test establishes that the communication of the DUT works according the IEC 61400-25 series.

Since the IEC 61400-25 series defines no new communication stacks, the conformance to all seven ISO/OSI layers may be proven by documentation that communication stack software compliant with the corresponding specifications is implemented and may have been pre-tested and optionally certified. In the standard conformance test, only the application according to ACSI can be tested.

5.3 Quality assurance and testing

5.3.1 General

In order to assure the quality during conformance testing, a quality assurance system has to be in place.

In general, quality surveillance is used to monitor and verify the status of components during all phases of the conformance tests. For this purpose, inspections are carried out, based on hold and witness points that are indicated by the initiator or its representative in the test and the inspection plan that is supplied by the test facility. These inspections are process related and will provide information and confidence on the quality of the tests. Quality surveillance will reduce the risks of failure during the FAT and SAT.

5.3.2 Quality plan

5.3.2.1 Conformance test quality plan

The test facility will supply, for evaluation, a quality plan for the conformance test.

The plan shall describe all measures for the scope of work and/or deliveries in the areas of organisation, time, information and quality. There is only one plan for the test facility and its sub-suppliers.

The conformance test quality plan is proposed to contain the following:

– A complete and detailed description of the work methods. This will help insure that all verifiable activities will fulfil all applicable requirements and conditions as stated in the scope of work during the time allowed.
– A detailed description of all tasks to be performed, including references to the schedule, an overview of the involved staff, materials and work methods as well as relevant methods and procedures.
– A detailed description of the organisation, including the assignments, tasks and responsibilities of mentioned staff during the different stages of the test programs. The description shall include all tests, inspections, research and audits during the various stages of the tests and the dates on which they will take place. These descriptions will be part of the test and inspection plan.
– A method for handling deviations, changes and modifications during all stages of the test.
– A sign off procedure and a description of the documentation to be supplied.

5.3.2.2 Test and inspection plan

The conformance test quality plan shall contain a test and inspection plan. In this plan, the test facility specifies, for all phases of the tests:

– what will be inspected, tested and registered;
– the purpose of the inspections and tests;
– the procedures and standards to which inspections, tests and registrations will be performed;

– the expected results of the inspections and tests;
– identification of persons to perform the inspections, tests and registrations.

The test facility is responsible for the correct and timely performance of all activities mentioned in the test and inspection plan.

The test facility will include a proposal for so called hold, witness and review points in the test and inspection plan.

There are several methods to perform a hold or witness point. The initiator of the conformance test or a representative can be present during the execution of a test or inspection. It is also possible to review the associated quality documents, e.g. checklists, verification and validation documents. This review can take place at the test facilities site during the execution of a test or inspection can be made at the initiator's site.

All hold and witness points will be announced by the test facility at least a predefined time before they take place. A period of at least one week is recommended, depending on the time needed for making travel arrangements and the availability of the needed resources.

The initiator of a conformance test has the right to conduct audits on the quality system of the test facility and its sub-suppliers. The test facility shall co-operate and provide access to all locations applicable for the conformance test. The initiator's right to check the quality of the conformance test does not dismiss the test facility from its responsibilities.

Inspections and tests by the initiator of a conformance test shall be possible at mutually agreeable times at the locations, offices and factories of the test facility and all applicable third parties and sub-suppliers.

5.4 Testing

5.4.1 General

Conformance testing shall be customised for each device under test based on the capabilities identified in the PICS, PIXIT and MICS provided by the vendor. When submitting devices for testing, the following shall be provided:

– device for testing;
– Protocol Implementation Conformance Statement (PICS);
– Protocol Implementation eXtra Information for Testing (PIXIT) statement;
– Model Implementation Conformance Statement (MICS);
– instruction manuals detailing the installation and operation of the device.

The requirements for conformance testing fall into two categories:

a) static conformance requirements (define the requirements the implementation shall fulfil);
b) dynamic conformance requirements (define the requirements that arise from the protocol used for a certain implementation).

The static and dynamic conformance requirements shall be defined in a Protocol Implementation Conformance Statement or PICS. The PICS serves three purposes:

1) selection of the appropriate set of tests;
2) ensure that the tests appropriate to a claim of conformance are performed;
3) provide the basis for the review of the static conformance.

Concrete PICS shall be as defined for the SCSMs.

A Model Implementation Conformance Statement or MICS shall be provided detailing the standard data object model elements supported by the system or device.

In addition to the PICS, a PIXIT document shall be provided.

The process of assessing the conformance is shown in Figure 2.

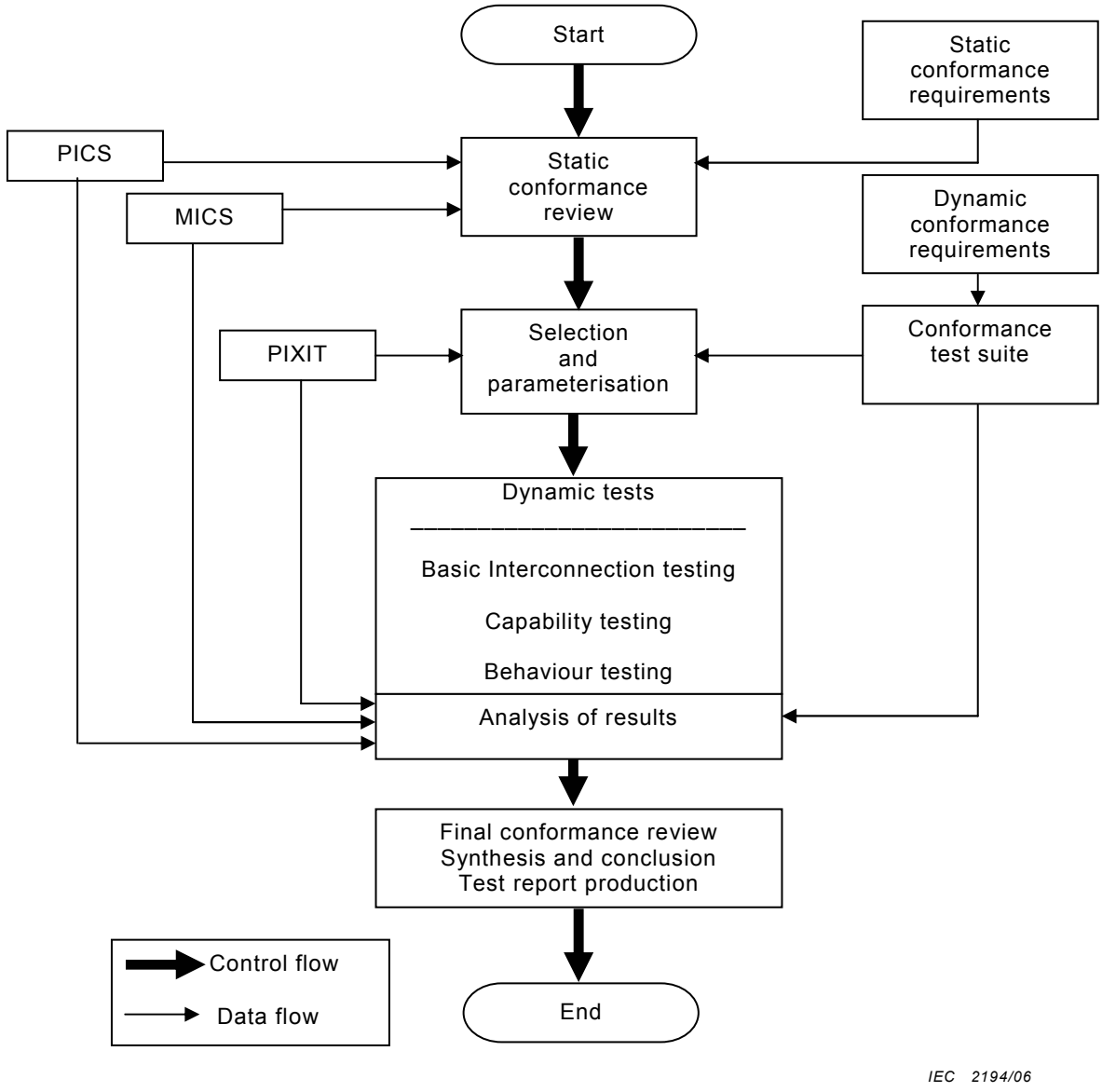

Figure 2 – Conceptual conformance assessment process

5.4.2 Device testing

A single device shall be conformance tested against a single test device.

The device specific conformance tests contain the positive and negative testing of the following as appropriate:

– inspection of the documentation and version control of the device,
– test of device configuration file against the device related object model (IEC 61400-25-2),
– test of communication stack implementation against applicable SCSM (IEC 61400-25-4),
– test of implemented ACSI services against ACSI definition (IEC 61400-25-3),

– test of device specific extensions according to rules given by the IEC 61400-25 series in general.

5.5 Documentation of conformance test report

A conformance test report shall include the following information:

– A reference list of all documents that describe or specify any qualifying tests that have been performed. These documents may include the vendor's standard operating and testing procedures, and local, national and international standards. International standards shall be cited by document number, date, Clause and Sub clauses. References to other documents shall include a complete source address and document identification. A complete and contextually accurate summary or extract of the document may be included for convenience.
– A list of any specialised test equipment or computer programs used for performing the conformance tests.
– Name and address of the vendor.
– Name and address of the initiator of the conformance test (if different from vendor name).
– Name of the tested device.
– All of the variants (hardware, firmware, etc.) of tested device.
– Name and address of the test facility.
– Date of issue of test report.
– Name and signature of the tester.
– Unique reference number.
– A list of test items performed to verify conformance.
– Comments and problems found.
– For each test item, the following subjects shall be documented:
  - description of the test item with the objective of the test, the test procedure and the expected result;
  - reference to the IEC 61400-25 series part, chapter and paragraph;
  - unique identifier per test item;
  - test result: passed, failed, inconclusive, not applicable;
  - comparison of the test result to the expected result.

Changes or alterations to the device made at any point in the test, particularly those made to correct a test deficiency, shall be completely described.

Conformance test documentation shall be supplied to the initiator.

6 Device related conformance testing

6.1 General guidelines

6.1.1 Test methodology

Communication testing needs at least two devices to communicate with each other. Comprehensive interoperability testing of all possible products is not feasible. Therefore, the test concept shall include test devices, test configurations, and test scenarios.

The dynamic behaviour should be tested properly by using well-defined test cases.

Special attention shall be given to communication equipment such as star-couplers, switches, etc., which shall support all requested features of the IEC 61400-25 series but not introduce additional contingencies and limitations.

The impact of the communication method (client-server, FTP/IP etc.) used by the device under test shall be considered properly in the test procedures. Verification of functional applications is not part of a conformance test even if advanced tools may offer such analysis.

6.1.2 Test system architectures

In order to be able to perform a device test, a minimum test set-up is necessary (see Figure 3). Beside the DUT, a device (for example, a simulator) which acts as a client and server is required to initiate and generate messages and record and process resulting information. Background load on the network may be provided by an additional load simulator, which may also contain a master for time synchronisation (the time sync master). An optional HMI on the network may be used for independent monitoring of the test system. The optional HMI may include a network monitoring facility and the engineering software on a system and device level. Network analyzers shall be used to monitor the system for errors during testing.

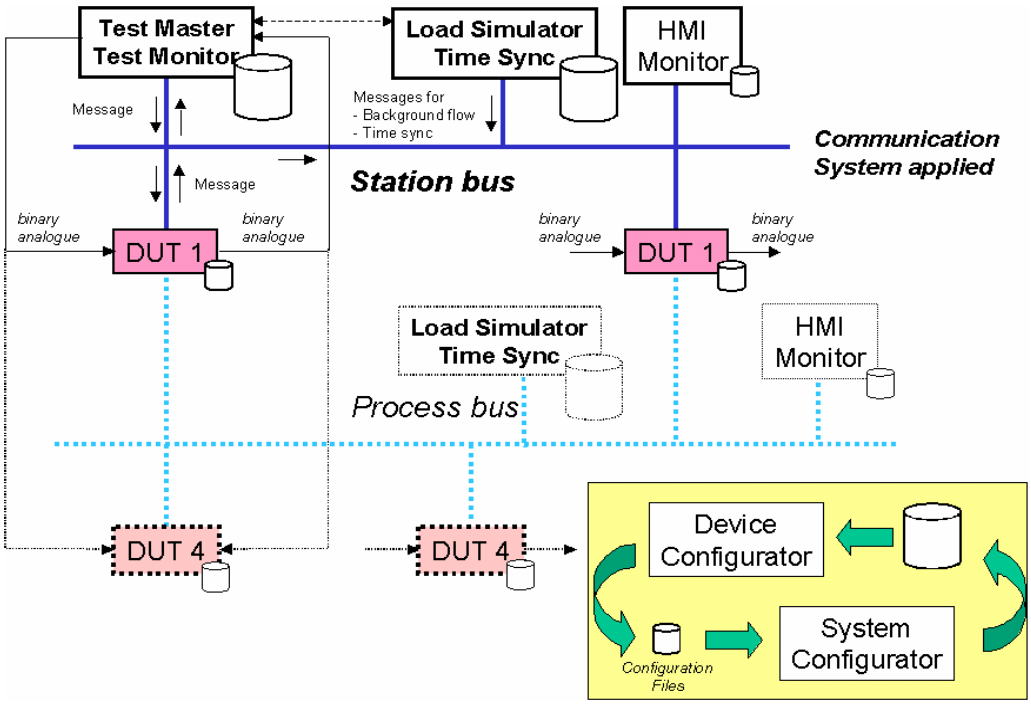

Figure 3 – Conceptual test system architecture

In the case of testing devices with client-server roles, the test system shall provide connection points for server devices, for client devices and for devices acting as both.

The test system shall include documentation regarding the following points:

– test configuration of the test system hardware;
– test configuration of the test system software;
– test simulator or background load simulator or time sync master.

6.2 Standard test procedures

6.2.1 Inspection of documentation and version control of the device

The following issues shall be addressed during the test:

– PICS,
– version control, and
– vendor documentation.

6.2.2 Test of basic system related communication functions

The following issues shall be addressed during the test:

– clock synchronisation;
– time stamping;
– loss of communication.

6.3 Conformance test procedures

6.3.1 General

This Subclause describes the test procedure requirements, test structure, the test cases (what is to be tested) and the format and a few examples of test procedures (how it is to be tested).

6.3.2 Test procedure requirements

The test procedure requirements are:

– The test cases describe what shall be tested; the test procedures describe how a test engineer or a test system shall perform the test.
– Test cases include a reference to the applicable paragraph(s) in the referenced document(s).
– The test results shall be reproducible in the same test lab and in other test labs.
– Support automated testing with minimal human intervention, as far as reasonably possible.
– The tests shall focus on situations that cannot easily be tested during, for example, a factory or site acceptance test, and prevent inter-operability risks, for example:
  - check behaviour of the device on delayed, lost, double and out of order packets,
  - configuration, implementation, operation risks,
  - mismatching names, parameters, settings, or data types,
  - exceeding certain limits, ranges or timeouts,
  - force situations to test negative responses,
  - check all (control) state machine paths, and
  - force simultaneous control operations from multiple clients.
– The ACSI tests focus on the application layer (mapping).

– The Device Under Test (DUT) is considered as a black box. The I/O and the communication interface are used for testing.
– The test includes testing the versions, data model and configuration file, and the use of applicable ISO/IEC 9646 series terminology.

The test procedures shall be formatted as outlined in Figure 4. With this format, the test procedures document can also be used as test report. A few test procedure examples are depicted in Annex A.

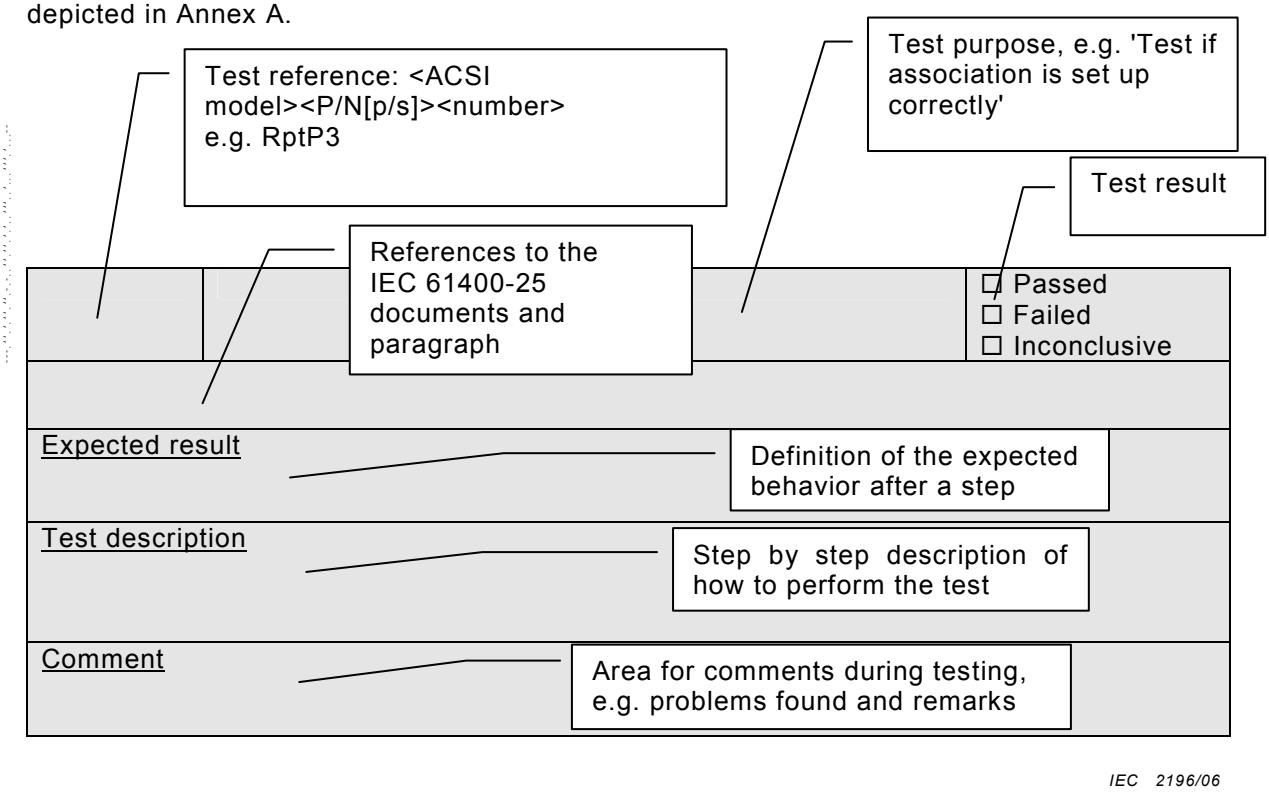

Figure 4 – Test procedure format

6.3.3 Test structure

The server test cases are structured as follows:

a) Documentation and version control (IEC 61400-25-5).
b) Data model (IEC 61400-25-2).
c) Mapping of ACSI models and services (IEC 61400-25-3); the corresponding sub clauses that define the abstract test cases are given in brackets:
   – application association (6.3.4.5)
   – server, logical device, logical node, and data model (6.3.4.6)
   – data set (6.3.4.3)
   – reporting (6.3.4.7)
   – logging (6.3.4.9)
   – control (6.3.4.10)
   – time and time synchronization (6.3.4.11)

6.3.4 Test cases to test a server

6.3.4.1 General

This part of the IEC 61400-25-5 series specifies abstract test cases (see 6.3.4.5 to 6.3.4.12). The abstract test cases shall be used for the definition of concrete test cases to run in tests.

NOTE 1 The concrete syntax of test cases depends on the test system environment, i.e., mainly on the test script language. The concrete test cases are to be provided by test facilities agreed upon by the market participants.

NOTE 2 The server tests may require a base load generator. The definition of base load is beyond the scope of this part of the IEC 61400-25 series.

6.3.4.2 Documentation and version control test procedure overview

Check if the manufacturer's PICS, MICS and PIXIT documentation and hardware and software versions of the DUT match (IEC 61400-25-4).

6.3.4.3 Data model test cases

The data model test cases shall:

– verify presence of mandatory objects for each LN (presence = M, optional = O),
– verify non-presence of conditional presence false objects,
– verify data type of all objects for each LN,
– verify data attribute values from the device are in specified range (this is a continuous effort during the whole conformance test).

The test result is a list of object references with data type, common data class, data attribute type, M/O presence indication (from IEC 61400-25-2).

The data model extensions shall be checked according to the standardised extension rules including the use of namespaces. The manufacturer-specific data model extensions shall be documented. To enable this, the MICS shall include definitions of the specific logical nodes, common data classes and data attribute types in the same format as IEC 61400-25-2.

The data model mapping shall be verified:

– verify name length and object expansion;
– verify the organisation of functional components;
– verify the naming of control blocks and logs.

6.3.4.4 Mapping of ACSI models and services test cases

Test items shall be grouped together in tables. The tables shall reflect the services specified in IEC 61400-25-3:

– Application association (Ass);
– Server, Logical device, Logical node, Data, and Data Attribute model (Srv);
– Report control model (Rpt);
– Log control model (Log);
– Control model (Ctl);
– Time and time synchronisation model (Tm).

Test cases are defined for each ACSI model and services in the following categories:

– positive = verification of normal conditions, typically resulting in response+
– negative = verification of abnormal conditions, typically resulting in response-

A test case is mandatory when the applicable ACSI model and ACSI service is supported by the DUT. This is specified in the PICS according to IEC 61850-7-2, Annex A.

6.3.4.5 Application association

6.3.4.5.1 Positive

Test case	Test case description
S_Ass1	Associate and release a TPAA association (IEC 61850-7-2, 7.4).
S_Ass2	Associate and client-abort TPAA association (IEC 61850-7-2, 7.4).
S_Ass3	Associate with maximum number of clients simultaneously (PIXIT).

6.3.4.5.2 Negative

Test case	Test case description
S_AssN1	Check that with incorrect authentication parameters and authentication turned on at server, the association fails, and with authentication turned off, the server associates (IEC 61850-7-2, 7.4).
S_AssN2	Check that with incorrect association parameters at server or client the association fails (IEC 61850-7-2, 7.4, PIXIT).
S_AssN3	Set up maximum+1 associations, verify the last associate is refused.
S_AssN4	Disconnect the communication interface, the DUT shall detect link lost within a specified period.
S_AssN5	Interrupt and restore the power supply, the DUT shall accept an association request when ready.

6.3.4.6 Server, Logical Device, Logical Node, and Data model

6.3.4.6.1 Positive

Test case	Test case description
S_Srv1	Request GetServerDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2, 6.2.2).
S_Srv2	For each GetServerDirectory(LOGICAL-DEVICE) response issue a GetLogicalDeviceDirectory request and check response (IEC 61850-7-2, 8.2.1).
S_Srv3	For each GetLogicalDeviceDirectory response issue a GetLogicalNodeDirectory(DATA) request and check response (IEC 61850-7-2, 9.2.2).
S_Srv4	For each GetLogicalNodeDirectory(DATA) response issue a – GetDataDirectory request and check response (IEC 61850-7-2, 10.4.4), – GetDataDefinition request and check response (IEC 61850-7-2, 10.4.5), – GetDataValues request and check response (IEC 61850-7-2, 10.4.2)
S_Srv5	Issue one GetDataValues request with the maximum number of data values and check response.
S_Srv6	For each write enabled DATA object, issue a SetDataValues request and check response (IEC 61850-7-2, 10.4.2).
S_Srv7	Issue one SetDataValues request with the maximum number of data values and check response.
S_Srv8	Request GetAllDataValues for each functional constraint and check response (IEC 61850-7-2, 9.2.3).

6.3.4.6.2 Negative

Test case	Test case description
S_SrvN1	Request the following data services with wrong parameters (unknown object, name case mismatch, wrong logical device or wrong logical node) and verify response- service error – ServerDirectory(LOGICAL-DEVICE) (IEC 61850-7-2, 6.2.2), – GetLogicalDeviceDirectory (IEC 61850-7-2, 8.2.1), – GetLogicalNodeDirectory(DATA) (IEC 61850-7-2, 9.2.2), – GetAllDataValues (IEC 61850-7-2, 9.2.3), – GetDataValues (IEC 61850-7-2, 10.4.2), – SetDataValues (IEC 61850-7-2, 10.4.3),

Test case	Test case description
	– GetDataDirectory (IEC 61850-7-2, 10.4.4), – GetDataDefinition (IEC 61850-7-2, 10.4.5).
S_SrvN2	Request SetDataValues of ENUMERATED data with out-of-range value and verify response- service error (IEC 61850-7-2, 10.4.2).
S_SrvN3	Request SetDataValues with mismatching data type (e.g. int-float) and verify response- service error (IEC 61850-7-2, 10.4.2).
S_SrvN4	Request SetDataValues for read-only data values and verify response- service error (IEC 61850-7-2, 10.4.2).

6.3.4.7 Data set model

6.3.4.7.1 Positive

Test case	Test case description
S_Ds1	Request GetLogicalNodeDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2, 9.2.2). For each response, issue a: - GetDataSetValues request and check response (IEC 61850-7-2 Subclause 11.3.2), - GetDataSetDirectory request and check response (IEC 61850-7-2 Subclause 11.3.6).
S_Ds2	Request a persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2, 11.3.4) and verify that the non-persistent data set is visible for another client.
S_Ds3	Request a non-persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2, 11.3.4) and verify that the persistent data set is not visible for another client.
S_Ds4	Create and delete a persistent dataset, create the dataset again with the same name with one extra data value/re-ordered member and check the members.
S_Ds5	Create and delete a non-persistent dataset, create the dataset again with the same name with one extra data value/re-ordered member and check the members.
S_Ds6	Create a non-persistent dataset, release/abort the association, associate again and check that the dataset has been deleted (IEC 61850-7-2, 11.1).
S_Ds7	Create a non-persistent dataset, release/abort the association, associate again and check that the dataset is still present (IEC 61850-7-2, 11.1).
S_Ds8	Create and delete a persistent dataset and verify that every data set can be created normally: repeat the process of creating and deleting once.
S_Ds9	Create and delete a non-persistent dataset and verify that every data set can be created normally: repeat the process of creating and deleting once.
S_Ds10	Verify SetDataSetValues/GetDataSetValues with GetDataValues and SetDataValues.

6.3.4.7.2 Negative

Test case	Test case description
S_DsN1	Request the following data set services with wrong parameters (unknown object, name case mismatch, wrong logical device or wrong logical node) and verify response- service error – GetDataSetValues (IEC 61850-7-2, 11.3.2), – SetDataSetValues (IEC 61850-7-2, 11.3.3), – CreateDataSet (IEC 61850-7-2, 11.3.4), – DeleteDataSet (IEC 61850-7-2, 11.3.5), – GetDataSetDirectory (IEC 61850-7-2, 11.3.6).
S_DsN2	Create a persistent dataset with the same name twice, and verify response- service error.
S_DsN3	Create a non-persistent dataset with the same name twice, and verify response- service error.
S_DsN4	Create more than maximum of persistent datasets and verify response- service error.
S_DsN5	Create more than maximum of non-persistent datasets and verify response- service error.

Test case	Test case description
S_DsN6	Create a persistent dataset with more than maximum number of elements and verify response- service error.
S_DsN7	Create a non-persistent dataset with more than maximum number of elements and verify response-service error.
S_DsN8	Create a persistent dataset with unknown members and verify response- service error.
S_DsN9	Create a non-persistent dataset with unknown members and verify response- service error.
S_DsN10	Delete a (pre-defined) non-deletable dataset, and verify response- service error.
S_DsN11	Delete a persistent dataset twice, and verify response- service error.
S_DsN12	Delete a non-persistent dataset twice, and verify response- service error.
S_DsN13	Delete a dataset referenced by (report) control class, and verify response- service error (IEC 61850-7-2, 11.1).
S_DsN14	Request SetDataSetValues with one or more read-only members, and verify response- service error.

6.3.4.8 Reporting model

6.3.4.8.1 Positive

Test case	Test case description
S_Rpt1	Request GetLogicalNodeDirectory(BRCB) and check response. Request GetBRCBValues of all responded BRCB's.
S_Rpt2	Request GetLogicalNodeDirectory(URCB) and check response. Request GetURCBValues of all responded URCB's.
S_Rpt3	Request AddSubscription and check response+ message (IEC 61400-25-3, 9.8.2). Request GetxRCBValues of all responding LN's.
S_Rpt4	Request RemoveSubscription and check response+ message (IEC 61400-25-3, 9.8.3).
S_Rpt5	Verify the reporting of optional fields of a URCB. Configure/enable a URCB with all useful optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, and/or entryID (IEC 61850-7-2, 14.2.3.2.2.1), force/trigger a report and check that the reports contain the enabled optional fields (IEC 61850-7-1, 14.3.1).
S_Rpt6	Verify the reporting of optional fields of a BRCB (see Rpt5).
S_Rpt7	Verify the reporting of optional fields of a xRCB set-up by AddSubscription (IEC 61400-25-3, 9.8.2, Table 10) (Optional fields see Rpt 4).
S_Rpt8	Verify the trigger conditions of a URCB – Configure and enable a URCB with all useful optional fields: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, and entryID and check that the reports are transmitted according to the following (supported) trigger conditions: • on integrity, • on update (dupd), • on update with integrity, • on data change (dchg), • on data and quality change, • on data and quality change with integrity period, • on data and quality change with integrity period and BufTime (integrity reports shall be transmitted immediately). – Verify the validity of the ReasonCode (IEC 61850-7-2, 14.2.3.2.2.9). – Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2, 14.2.3.2.3.2). – Verify that reports are only sent when RptEna is set to True. (IEC 61850-7-2, 14.2.2.5), when reporting is disabled, no reports shall be transmitted.

Test case	Test case description
S_Rpt9	Verify the trigger conditions of a BRCB (see Rpt8)
S_Rpt10	General interrogation Setting the GI attribute of an URCB shall start the general-interrogation process. One report with the current data values will be sent. After initiation of the general-interrogation, the GI attribute is reset to False. (IEC 61850-7-2, 14.2.2.13)
S_Rpt11	Segmentation of reports Verify that if a long report does not fit in one message, the report is split into sub-reports. Enable sequence-number and report-time-stamp optional field and check validity of (IEC 61850-7-2, 14.2.3.2.2.5): – SeqNum (not changed) – SubSeqNum (0 for first report, incrementing, roll-over) – MoreSeqmentsFollow – TimeOfEntry (not changed as SeqNum is not altered) (IEC 61850-7-2, 14.2.3.2.2.9) Verify that an update of a data value during sending of a segmented report caused by an integrity or general-interrogation trigger can be interrupted by a report with change of one of the data values with a new sequence number. (IEC 61850-7-2, 14.2.3.2.3.5) A new request for general-interrogation shall stop the sending of remaining segments of the GI-report that is still going on. A new GI-report shall start with a new sequence number and the sub-sequence number shall be 0 (IEC 61850-7-2, 14.2.3.2.3.4)
S_Rpt12	Configuration revision (IEC 61850-7-2, 14.2.2.7) – Verify that ConfRev represents a count of the number of times the configuration of the data set referenced by DatSet has been changed. Changes that are counted are: • deletion of a member of the data-set • re-ordering of members in the data-set ConfRev shall never be 0 (zero). – Verify that after a restart of the server, the value of ConfRev remains unchanged (IEC 61850-7-2, 14.2.2.7) – Verify that configuration changes data sets due to processing of services are not allowed, changes to be taken into account for the ConfRev are those made by local means such as system configuration (IEC 61850-7-2, 14.2.2.7, Note)
S_Rpt13	Buffer Time (IEC 61850-7-2, 14.2.2.9) – Verify that in the case where a second internal notification of the same member of a DATA-SET has occurred prior to the expiration of BufTim, the server (IEC 61850-7-2, 14.2.2.9): • shall for status information behave as if BufTim has expired and immediately send the report, restart the timer with value BufTim and process the second notification, or • may for analogue information behave as if BufTim has expired and immediately transmit the report for transmission, restart the timer with value BufTim and process the second notification, or • may for analogue information substitute the current value in the pending report with the new one. – Configure Buffer Time to 1 000 ms and force a data value change of multiple dataset members within buffer time. Server shall send not more than one report per buffer time with all the data values changes since last report. – Verify that the value 0 for buffer time indicates that the buffer time attribute is not used (IEC 61850-7-2, 14.2.2.9). – Verify that the BufTm value can contain at least the value 3 600 000 (= one hour in milliseconds)
S_Rpt14	Buffered reporting (BRCB) state machine (IEC 61850-7-2, 14.2.2.5 and Figure 20) – Verify events are buffered after the association is released. – Verify reporting is disabled after the association is lost. – Verify that reports not received while not associated are now received in the correct order (SOE) (IEC 61850-7-2, 14.2.1, IEC 61850-7-2, 14.2.2.5). – Do the same but now set PurgeBuf to True before enabling the reporting. No stored buffered reports shall be sent (IEC 61850-7-2, 14.2.2.14). – Verify that all buffered events are sent before integrity or general-interrogation report can be sent. (IEC 61850-7-2, 14.2.3.2.3.3, IEC 61850-7-2, 14.2.3.2.3.4). – Verify that after changing DatSet, the report buffer is purged. (IEC 61850-7-2, 14.2.2.5). – Force buffer overflow, the OptFlds buffer-overflow shall be set in the first report that is sent with events that occurred after the overflow (IEC 61850-7-2, 14.2.3.2.2.8).

6.3.4.8.2 Negative

Test case	Test case description
S_RptN1	Request GetxRCBValues with wrong parameters and verify response- service error (IEC 61850-7-2, 14.2.3.3.2).
S_RptN2	Configure reporting but omit setting one of the trigger options (dchg, qchg, dupd, integrity). When enabled, only one report is transmitted (the GI). No reports shall be sent when generating events (IEC 61850-7-2, 14.2.3.2.2.9).
S_RptN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2, 14.2.2.12).
S_RptN4	Incorrect configuration of a URCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set.
S_RptN5	Incorrect configuration of a BRCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set.
S_RptN6	Exclusive use of URCB and lost association. Configure a URCB and set the Resv attribute and enable it. Verify that another client cannot set any attribute of that URCB (IEC 61850-7-2, 14.2.4.5).
S_RptN7	Exclusive use of BRCB and lost association. Configure a BRCB and enable it. Verify another client can not set attributes value in this BRCB. (IEC 61850-7-2, 14.2.1).
S_RptN8	Configure unsupported URCB options (PIXIT). Configure unsupported trigger conditions, optional fields and related parameters.
S_RptN9	Configure unsupported BRCB options (PIXIT). Configure unsupported trigger conditions, optional fields and related parameters.
S_RptN10	Request AddSubscription with wrong parameters and verify response- service errors (IEC 61400-25-3, 9.8.2).
S_RptN11	Request RemoveSubscription with wrong parameters and verify response- service errors (IEC 61400-25-3, 9.8.3).

6.3.4.9 Log model

6.3.4.9.1 Positive

Test case	Test case description
S_Log1	Request GetLogicalNodeDirectory(LOG) and check response+.
S_Log2	Request GetLogicalNodeDirectory(LCB) and check response+.
S_Log3	Request GetLCBValues with functional constraint LG of all responded LCB's.
S_Log4	Request SetLCBValues with functional constraint LG when LCB is disabled.
S_Log5	Verify that the configured LOGs are shown by the DUT with reference LDname/LNname.LG.Logname.
S_Log6	Verify logging is independent of a limited set of external application associations or other communication transactions.
S_Log7	Verify a transition of LogEna from disable to enabled or from enabled to disabled shall cause a log entry to be placed into the log.
S_Log8	Configure and enable logging and check that the following logging trigger conditions place a correct entry in the log with the correct members of the data set – on integrity, – on update (dupd), – on update with integrity, – on data change (dchg), – on quality change (qchg), – on data and quality change,

Test case	Test case description
	– on data and quality change with integrity period.
S_Log9	Request QueryLogByTime and check response+.
S_Log10	Request QueryLogByEntry and check response+.
S_Log11	Request GetLogStatusValues and check response+, verify the responded entries indicate the oldest/newest entry ID/time available in the log.

6.3.4.9.2 Negative

Test case	Test case description
S_LogN1	Request following log services with wrong parameters (out of range entries, or non existent Dataset, LCB or Log) and verify response- service error – GetLCBValues (IEC 61850-7-2, 14.3.2.5), – SetLCBValues (IEC 61850-7-2, 14.3.2.6), – QueryLogByTime (IEC 61850-7-2, 14.3.5.2), – QueryLogByEntry (IEC 61850-7-2, 14.3.5.3), – GetLogStatusValues (IEC 61850-7-2, 14.3.5.4).
S_LogN2	Request SetLCBValues with functional constraint LG when LCB is enabled and verify response-service error.

6.3.4.10 Control model

6.3.4.10.1 General

The testing of the control model has been divided in the four possible control models that can be implemented:

1) Direct control with normal security.
2) SBO control with normal security.
3) Direct control with enhanced security.
4) SBO control with enhanced security.

6.3.4.10.2 Positive

Test case	Test case description
S_Ctl1	Force and check each path in control state machine for several control objects with control modes: a) direct with normal security (IEC 61850-7-2, 17.2.1), b) SBO-control with normal security (operate once/many) (IEC 61850-7-2, 17.2.2), c) direct with enhanced security (IEC 61850-7-2, 17.3.2), d) SBO-control with enhanced security (operate once/many) (IEC 61850-7-2, 17.3.3). Compare detailed state machine test cases for each control mode.
S_Ctl2	Verify that commands with test mode set are handled according to IEC 61400-25-2 or IEC 61850-7-4, and to PIXIT.
S_Ctl3	Select all SBO control objects and cancel them in opposite order.
S_Ctl4	Time Operate a second enhanced security control object before the activation time of the first control object.
S_Ctl5	Change control model using online services.

The following table contains a state machine test case for each path for “Direct operate with normal security” in IEC 61850-7-2, Figure 30, returning the device to the Ready State.

Test case	Test case description
S_DOns1	Path OperReq[test ok] resp+. Perform a correct Operate request.
S_DOns2	Path OperReq[test ok] resp+. Client requests TimOper resulting in Test not ok.
S_DOns3	Path OperReq[test not ok] resp-. Client requests Oper resulting in Test not ok.
S_DOns4	Path TimOperReq[test ok] + TimerExpired[test ok] resp+. Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test ok'. Verify the WaitForActionTime results in a timer expired ‘test ok’.
S_DOns5	Path TimOperReq[test ok] + TimerExpired[test not ok] resp-. Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test ok'. Force situation that the WaitForActionTime results in a timer expired ‘Test not ok’.

The following table contains a state machine test case for each path for “SBO with normal security” in IEC 61850-7-2, Figure 32, returning the device to the Unselected or Ready State.

Test case	Test case description
S_SBOns1	Path 1 SelectReq[test not ok] resp-: Select the device using Select with improper access rights. Verify the device returns to the Unselected state.
S_SBOns2	Path SelectReq[test ok] resp+: Select device correctly using Select. Verify that each of these paths will return the device to the Unselected state: – client requests Cancel, – client waits for timeout, – client requests TimOper resulting in Test not ok, – client requests Oper resulting in Test not ok, – client requests correct Operate Once.
S_SBOns3	Path SelectReq[test ok] resp+ and TimOperReq[test ok] resp+: Select device correctly using Select. Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Verify that each of these paths will return the device to the Unselected state: – Force situation that the WaitForActionTime results in a timer expired ‘Test not ok’, – Verify the WaitForActionTime results in a timer expired ‘Test ok, operate once’.
S_SBOns4	Path SelectReq[test ok] resp+ and OperReq[test ok, OPERATE MANY] resp+: Select device correctly using Select. Verify that sending a correct Operate Many request will return the device to the Ready state.
S_SBOns5	Path SelectReq[test ok] resp+ and TimOperReq[test ok] resp+ and TimerExpired[test ok, OPERATE MANY] resp+: Select device correctly using Select. Send a correct TimeActivatedOperate Many request. After the timer has expired, verify the device returns to the Ready State.

The following table contains a state machine test case for each path for “Direct operate with enhanced security” in IEC 61850-7-2, Figure 33, returning the device to the Ready State.

Test case	Test case description
S_DOes1	Path TimOperReq[test not ok] resp-: Send a TimeActivated Operate request, thereby making sure the device will generate a 'test not Ok'.
S_DOes2	Path OperReq[test not ok] resp-: Send an Operate request, thereby making sure the device will generate a 'test not Ok'.
S_DOes3	Path TimOperReq[test ok] resp+: Send a correct TimeActivated Operate request. Verify that each of these paths will return the device to the Ready state: – Client waits for timeout (test not ok), – Client requests correct Cancel.
S_DOes4	Path TimOperReq[test ok] resp+ and Timer expired [test ok] resp+: Send a correct TimeActivated Operate request. Verify the WaitForActionTime results in a timer expired ‘Test ok’. After the timer has expired, verify that each of these paths will return the device to the Ready state: – the output of the device moves to its new state, resulting in a state new, CmdTerm req+, – force the output of the device such that the output keeps its old state, resulting in a state old, CmdTerm req-, – force the output of the device such that the output reaches the 'between' state, resulting in a state between, CmdTerm req-.
S_DOes5	Path OperReq[test ok] resp+: Send a correct Operate request. After the timer has expired, verify that each of these paths will return the device to the Ready state: – the output of the device moves to its new state, resulting in a state new, CmdTerm req+, – force the output of the device such that the output keeps its old state, resulting in a state old, CmdTerm req-, – force the output of the device such that the output reaches the 'between' state, resulting in a state between, CmdTerm req-.

The following table contains a state machine test case for each path for “SBO with enhanced security” (see Figure 34 in IEC 61850-7-2) returning the device to the Unselected state or Ready State.

Test case	Test case description
S_SBOes1	Path 1 (returning to Unselected state): Select device using SelVal with improper access rights. Access shall be denied (IEC 61850-7-2, 17.2.2).
S_SBOes2	Path 2+3a/b/c/d (returning to Unselected state): Select device correctly using SelVal. Verify that each of these paths will return the device to the Unselected state: – client requests Cancel (3a), – client waits for timeout (3b), – client requests TimOper resulting in Test not ok (3c), – client requests Operate resulting in Test not ok (3d).
S_SBOes3	Path 2+4+8a/b/c (returning to Unselected state): Select device correctly using SelVal. Verify that each of these paths will return the device to the Unselected state: – perform a correct Operate Once request (8a), – perform a correct Operate Once request and force the output of the device such that the output keeps its old state (8b), – perform a correct Operate Once request and force the output of the device such that the output reaches the 'between' state (8c).

Test case	Test case description
S_SBOes4	Path 2+5+6 (returning to Unselected state): Select device correctly using SelVal. Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Force situation that the WaitForActionTime results in a timer expired ‘Test not ok’.
S_SBOes5	Path 2+5+7+8a/b/c (returning to Unselected state): Select device correctly using SelVal. Send a correct TimeActivatedOperate request. Verify the WaitForActionTime results in a timer expired ‘Test ok’. After the timer has expired, verify that each of these paths will return the device to the Unselected state: – perform a correct Operate Once request (8a), – perform a correct Operate Once request and force the output of the device such that the output keeps its old state (8b), – perform a correct Operate Once request and force the output of the device such that the output reaches the 'between' state (8c).
S_SBOes6	Path 2+4+9a/b/c (returning to the Ready state): Select device correctly using SelVal Send a correct Operate request. Verify that each of these paths will return the device to the Ready state: – perform a correct Operate Many request (9a), – perform a correct Operate Many request and force the output of the device such that the output keeps its old state (9b), – perform a correct Operate Many request and force the output of the device such that the output reaches the 'between' state (9c).
S_SBOes7	Path 2+5+7+9a/b/c (returning to the Ready state): Select device correctly [SelVal] Send a correct TimeActivatedOperate request. After the timer has expired, test each of these paths which will return the device to the Ready State: – perform a correct Operate Many request (9a), – perform a correct Operate Many request and force the output of the device such that the output keeps its old state (9b), – perform a correct Operate Many request and force the output of the device such that the output keeps reaches the 'between' state (9c).

6.3.4.10.3 Negative

Test case	Test case description
S_CtlN1	Operate (without select) for a SBO control object and verify the response- and AddCause (IEC 61850-7.2, 17.2.2).
S_CtlN2	Select twice, second select shall fail and verify the response- and AddCause (IEC 61850-7-2, 17.2.2).
S_CtlN3	Operate value is the same as the actual value (On-On, or Off-Off) and verify the response- and AddCause (IEC 61850-7-2, 17.2.2).
S_CtlN4	Select the same control object from 2 different clients, verify the response- and AddCause (IEC 61850-7-2, 17.2.2).
S_CtlN5	Select/Operate a unknown control object and verify the response- and AddCause (IEC 61850-7-2, 17.2.2).
S_CtlN6	Verify situations to set specific other applicable AddCause values (IEC 61850-7-2, 17.5.2.6).
S_CtlN7	Select an direct operate control object.
S_CtlN8	Operate a direct control object twice from 2 clients.
S_CtlN9	Operate with different value then the SelectWithValue of a SBOes control object.

6.3.4.11 Time and time synchronisation model

6.3.4.11.1 Positive

Test case	Test case description
S_Tm1	Verify the DUT supports the SCSM time synchronisation.
S_Tm2	Check that report/logging timestamp accuracy matches the documented timestamp quality of the server.

6.3.4.11.2 Negative

Test case	Test case description
S_TmN1	Verify that when time synchronisation communication lost is detected after a specified period.
S_TmN2	On synchronisation error, deviation beyond time stamp tolerance shall be detected.

6.3.4.12 Combination test

Positive

Test case	Test case description
S_Comb1	Test if reporting and control services keep on responding as specified while requesting other services – Combine server actions: Reporting, Logging, Time Sync with client request services • enable reporting, • enable logging, • enable time synch, • enable other supported services that consumes processing time at server, – Start requests of all supported request and control services. As soon as one request is responded, issue a new request. Continue this for 10 min • request logical server, logical node and data GetDataValues-services, • request GetDataSetValue-services, • request GetxRCBValue-services, • request QueryLog-services, • select and operate control objects.

6.3.5 Test cases to test a client

6.3.5.1 Application association

6.3.5.1.1 Positive

Test case	Test case description
C_Ass1	Associate and force client to release a TPAA association (IEC 61850-7-2, 7.4).
C_Ass2	Force the client to associate with maximum number of servers simultaneously (PIXIT).

6.3.5.1.2 Negative

Test case	Test case description
C_AssN1	Associate and server responds with negative answer due to AccessPointReference.
C_AssN2	Associate and server responds with negative answer due to AuthenticationParameter.
C_AssN3	Associate and server releases TPAA association (IEC 61850-7-2, 7.4). DUT should try to re-establish the association after the configured period (PIXIT).

Test case	Test case description
C_AssN4	Associate and server-abort TPAA association (IEC 61850-7-2, 7.4). DUT should try to re-establish the association after the configured period (PIXIT).
C_AssN5	Disconnect the communication interface, the DUT shall detect link lost within a specified period. Once the link is re-established, the DUT should try to establish the association again.
C_AssN6	Interrupt and restore the power supply, the DUT shall establish the configured associations when ready (PIXIT).

6.3.5.2 Server, Logical Device, Logical Node, and Data model

6.3.5.2.1 Positive

Test case	Test case description
C_Srv1	If client implements Autodescription (See Note 1), force the client to start the autodescription and check that the client requests a GetServerDirectory(LOGICAL-DEVICE) to all the logical devices of the configured servers (See Note 2).
C_Srv2	If client implements Autodescription, for each GetServerDirectory(LOGICAL-DEVICE) response, check that the client issues a GetLogicalDeviceDirectory request.
C_Srv3	If client “implements Autodescription”, for each GetLogicalDeviceDirectory response issue, check that the client issues a GetLogicalNodeDirectory(DATA) request.
C_Srv4	If client “implements Autodescription”, for each GetLogicalNodeDirectory(DATA) response, check that the client issues at least one of the following services: – GetDataDirectory request and check response (IEC 61850-7-2, 10.4.4), – GetDataDefinition request and check response (IEC 61850-7-2, 10.4.5).
C_Srv5	Verify that after startup, the client is able to update its view of the configured servers (PIXIT).
C_Srv6	For each write enabled DATA object, issue a SetDataValues request and check response (IEC 61850-7-2, 10.4.2).
C_Srv7	Request a SetDataValues of all the different basic types and check the services.
C_Srv8	Request GetAllDataValues for each functional constraint and check if the client updates its model (IEC 61850-7-2, 9.2.3).
NOTE 1 Implement Autodescription means that there is a way to configure the client to update the image of the model of one of the servers it has to communicate with using the ACSI services. NOTE 2 Configured servers means the servers that the client is configured to communicated with. The client at least needs to know the parameters to establish an association with them.	

6.3.5.2.2 Negative

Test case	Test case description
C_SrvN1	If client implements Autodescription, force the client to start the autodescription and check that the client still communicates with other servers when it requests the following services with no response/delayed response/negative response: - GetServerDirectory(LOGICAL-DEVICE), - GetLogicalDeviceDirectory, - GetLogicalNodeDirectory(DATA), - GetDataDirectory, - GetDataDefinition.
C_SrvN2	Check that the client still works properly when it requests a GetAllDataValue in the following situation: - the server does not response, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with a wrong type.

Test case	Test case description
C_SrvN3	Check that the client still works properly when it requests a GetDataValue in the following situation: - the server does not response, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with a wrong type, - the value is out of the valid range for this data.
C_SrvN4	Check that the client still works properly when it requests a SetDataValue in the following situation: - the server does not response, - the response arrives later than the maximum allowed timeout, - the response is negative.
C_SrvN5	If client detects/notify changes in the “Quality” attribute, use the SERVER SIMULATOR to force different values in the Quality of the measured/status values monitored by the client and check the behaviour described in the PIXIT.
C_SrvN6	If client detects/notify changes in the timeStamp’s “TimeQuality” attribute, use the SERVER SIMULATOR to force different values in the TimeQuality of the measured/status values monitored by the client and check the behaviour described in the PIXIT.

6.3.5.3 DataSet model

6.3.5.3.1 Positive

Test case	Test case description
C_Ds1	If client implements Autodescription, force it to start autodescription and check if it requests a GetLogicalNodeDirectory(DATASET) of all the Logical Nodes of the configured servers.
C_Ds2	If client implements Autodescription, force it to start autodescription and check it requests a GetDataSetDirectory of all the DataSets of the server.
C_Ds3	Check that the GetDataSetValues update the information model of the client.
C_Ds4	If the client configures the datasets dynamically after starting up, check that the client sends the CreateDataSet services according to configuration (PIXIT).
C_Ds5	Request a DeleteDataSet service and check that the client sends the request properly and is able to process the response of the server.

6.3.5.3.2 Negative

Test case	Test case description
C_DsN1	If client implements Autodescription, force the client to start the autodescription and check that the client still communicates with other servers when it request the following services with no response/ delayed response/negative response: - GetLogicalNodeDirectory (DATASET), - GetDataSetDirectory.
C_DsN2	If client configures the datasets dynamically after starting up check that the client still communicates with other servers when it requests the following services with no response/ delayed response/negative response: - CreateDataSet, - DeleteDataSet.
C_DsN3	Check that the client still communicates with other servers properly when it requests a GetDataSetValue to one of them and the following situations happen: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with more/less elements than expected, - the response comes with different types in the elements.

Test case	Test case description
C_DsN4	Check that the client still communicates with other servers properly when it requests a SetDataSetValue to one of them and the following situations happen: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with more/less results than the number of elements in the DataSet.
C_DsN5	Check that the client will continue working properly if it requests a CreateDataSet and after getting a positive response, the server did not really create the dataset.
C_DsN6	Check that the client will continue working properly if it requests a DeleteDataSet of an existing dataset and after getting a positive response the server did not really delete it.

6.3.5.4 Reporting model

6.3.5.4.1 Positive

Test case	Test case description
C_Rpt1	If client implements autodescription, force it to start autodescription and check if it requests a GetLogicalNodeDirectory(URCB) of all the logical nodes of all configured servers.
C_Rpt2	If client implements autodescription, force it to start autodescription and check if it requests a GetLogicalNodeDirectory(BRCB) of all the logical nodes of all configured servers.
C_Rpt3	If the client configures the server's Unbuffered ReportControlBlock parameters after startup using SetURCBValues, check that the GetURCBValues/SetURCBValues are sent with the configured values.
C_Rpt4	If the client configures the server's Buffered ReportControlBlock parameters after startup using SetBRCBValues, check that the GetBRCBValues/SetBRCBValues are sent with the configured values.
C_Rpt5	If the client configures the server's ReportControlBlock parameters after startup using AddSubscription, check that the AddSubscription service was sent as configured.
C_Rpt6	Force the client to RemoveSubscription and check the request sent.
C_Rpt7	Verify the client is able to process the reports with different optional fields: Force the client to configure/enable a URCB with all useful optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, and/or entryID (IEC 61850-7-2, 14.2.3.2.2.1), force/trigger a report and check that the client is able to process the reports and updates its datamodel.
C_Rpt8	Verify the client is able to process the reports with different optional fields of a xRCB set-up by AddSubscription (IEC 61400-25-3, 9.8.2, Table 10).
C_Rpt9	Verify the client is able to process the reports with different trigger conditions: Configure and enable a xRCB with all useful optional fields: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, and entryID and check that the reports are transmitted according to the following (supported) trigger conditions: • on integrity, • on update (dupd), • on update with integrity, • on data change (dchg), • on data and quality change, • on data and quality change with integrity period, • on data and quality change with integrity period and BufTime (integrity reports shall be transmitted immediately).
C_Rpt10	Verify that the client is able to process reports that are segmented.
C_Rpt11	Verify that the client detects a change in the ConfRev attribute (Configuration revision (IEC 61850-7-2, 14.2.2.7)) of the Report Control Block.

6.3.5.4.2 Negative

Test case	Test case description
C_RptN1	If client implements Autodescription, force the client to start the autodescription and check that the client still communicates with other servers when it requests GetLogicalNodeDirectory (URCB) and GetLogicalNodeDirectory (BRCB) with no response/delayed response/negative response.
C_RptN2	Check that the client still works properly when it request a GetURCBValues/GetBRCBValues in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with a wrong type, - the value is out of the valid range for this data.
C_RptN3	Check that the client still works properly when it request a SetURCBValues/SetBRCBValues in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative.
C_RptN4	Check that the client still works properly when it request a AddSubscription in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative.
C_RptN5	Check that the client still works properly when it request a RemoveSubscription in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative.
C_RptN6	Report with not supported OptFlds. Check that the client does not collapse if it receives a Report with a non-configured or non-supported OptFlds.
C_RptN7	Report with not supported TrgOps. Check that the client does not collapse if it receives a Report with a non-configured or non-supported Trigger Option.
C_RptN8	Unexpected reports. - integrity reports with IntgPd set to 0, - GI reports not requested, - reports received from ReportControlBlock that has not been enabled.
C_RptN9	Bad format reports: - report with unknown DataSet, - report with incorrect references of the Data, - report with incorrect types in the Data. Check the behaviour described in the PIXIT.
C_RptN10	Reporting too fast. Check that the client does not collapse if it receives more Reports than expected in a period of time and verify the behaviour described in the PIXIT to control this situation.
C_RptN11	ConfRev.Check if the DUT detects a change in the ConfRev attribute of the Report Control Block.
C_RptN12	SqNum. Check the DUT shows an error if it receives a Report out of order.
C_RptN13	Integrity. Check the DUT shows an error if it activates Integrity in a server and no integrity-reports are sent back to it.

6.3.5.5 Log model

6.3.5.5.1 Positive

Test case	Test case description
C_Log1	If client implements autodescription, force it to start autodescription and check if it requests a GetLogicalNodeDirectory (LOG) of all the logical nodes of all configured servers.
C_Log2	If client implements autodescription, force it to start autodescription and check if it requests a GetLogicalNodeDirectory(LCB) of all the logical nodes of all configured servers.
C_Log3	If client implements autodescription, force it to start autodescription and check if it requests a GeLogStatusValues of all the LOGs found with the GetLogicalNodeDirectory(LCB) services
C_Log4	If client implements autodescription, force it to start autodescription and check if it requests a GeLCBValues of all the LCBs found with the GetLogicalNodeDirectory(LCB) services
C_Log5	If the client configures the server's LogControlBlock parameters after startup using SetLCBValues, check that the GetLCBValues/SetLCBValues are sent with the configured values.
C_Log6	Force the client to enable the Logging of at least one LOG of the server and check that the client sent the request correctly.
C_Log7	Force the client to QueryLogByTime and check that the DUT updates its database with the Log entries received.
C_Log8	Force the client to QueryLogByEntry and check that the DUT updates its database with the Log entries received.

6.3.5.5.2 Negative

Test case	Test case description
C_LogN1	If client implements Autodescription, force the client to start the autodescription and check that the client still communicates with other servers when it requests GetLogicalNodeDirectory (LCB) and GetLogicalNodeDirectory (LOG) with no response/delayed response/negative response.
C_LogN2	Check that the client still works properly when it request a GetLCBValues/GetLogStatusValues in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative, - the response comes with a wrong type, - the value is out of the valid range for this data.
C_LogN3	Check that the client still works properly when it request a SetLCBValues in the following situation: - the server does not respond, - the response arrives later than the maximum allowed timeout, - the response is negative.
C_LogN4	LogEntry badly formed. Check that the client still works properly when it has received a LogEntry whose: - DataRef does not exist in the model, - DataValue is not of the type expected.
C_LogN5	LogEntry in bad order. Check that the client still works properly when it has received a LogEntry out of order.

6.3.5.6 Control model

6.3.5.6.1 General test cases

6.3.5.6.1.1 Positive

Test case	Test case description
C_Ctl1	Check if the client is able to set the TEST field in the commands (PIXIT).
C_Ctl2	Check if the client is able to set the CHECK (Synchro-Check or Interlock-Check bits) in the commands (PIXIT).
C_Ctl3	Check if the client is able to change control model using online services (PIXIT).

6.3.5.6.2 Specific test cases for the control models

The testing of the control model has been divided in the four possible control model that can be implemented:

1) Direct control with normal security.
2) SBO control with normal security.
3) Direct control with enhanced security.
4) SBO control with enhanced security.

6.3.5.6.3 Direct Control with Normal Security

6.3.5.6.3.1 Positive

Test case	Test case description
C_DOns1	OperReq[test ok] resp+ Perform a correct Operate request. Check that the client realizes the operation succeeded.
C_DOns2	OperReq[test not ok] resp- Client requests Oper resulting in Test not ok. Check that the client realizes the operation failed.
C_DOns3	TimOperReq[test not ok] resp- Client requests TimOper resulting in Test not ok Perform an incorrect TimOperate request and check that the client realizes the operation failed. Incorrect TimOperate request can be: - Incorrect time to operate. - Incorrect ctlVal. - Incorrect originator (PIXIT). - Incorrect Test or Check (PIXIT).
C_DOns4	TimOperReq[test ok] + TimerExpired[test ok] resp+ Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Verify the WaitForActionTime results in a timer expired ‘Test ok’ and that the client realizes the operation succeeded.
C_DOns5	TimOperReq[test ok] + TimerExpired[test not ok] resp- Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Force situation that the WaitForActionTime results in a timer expired ‘Test not ok’. Check that the client realizes the operation failed.

6.3.5.6.3.2 Negative

Test case	Test case description
C_DOnsN1	Incorrect Operate Check that the client detects the following situations: - Operate without response. - Operate with delayed response.
C_DOnsN2	Incorrect TimedActivatedOperate Check that the client detects the following situations: - TimedActivatedOperate without response. - TimedActivatedOperate with delayed response. - TimedActivated with positive first response and no second response after WaitForActionTime. - TimedActivated with negative first response and a second response positive after WaitForActionTime. - TimedActivated with negative first response and a second response negative after WaitForActionTime.

6.3.5.6.4 SBO control with normal security

6.3.5.6.4.1 Positive

Test case	Test case description
C_SBOns1	SelectReq[test not ok] resp-: Select a controllable object using Select with improper access rights. Verify the client notices that he has no right to control the variable.
C_SBOns2	SelectReq[test ok] resp+: Select a controllable object using Select with proper access rights. Verify the client notices that he has the right to access the variable.
C_SBOns3	OperReq[test ok] resp+ of selected object Perform a correct Operate request. Check that the client realizes that the operation succeeded.
C_SBOns4	OperReq[test not ok] resp- of selected object. Perform an incorrect Operate request. Check that the client realizes the operation failed.
C_SBOns5	TimOperReq[test ok] resp+ of selected object Perform a correct TimOperate request. Check that the client realizes the operation succeeded after the WaitForActionTime.
C_SBOns6	TimOperReq[test ok] resp- of selected object Perform an incorrect TimOperate request. Check that the client realizes that the operation failed.

6.3.5.6.4.2 Negative

Test case	Test case description
C_SBOnsN1	Incorrect Select. Check that the client detects the following situations: - Select without response. - Select with delayed response.
C_SBOnsN2	Incorrect Operate of selected object Check that the client detects the following situations: - Operate without response. - Operate with delayed response.

Test case	Test case description
C_SBOnsN3	Incorrect TimedActivatedOperate of selected object Check that the client detects the following situations: - TimedActivatedOperate without response. - TimedActivatedOperate with delayed response. - TimedActivated with positive first response and no second response after WaitForActionTime. - TimedActivated with negative first response and a second response positive after WaitForActionTime. - TimedActivated with negative first response and a second response negative after WaitForActionTime.

6.3.5.6.5 Direct control with enhanced security

6.3.5.6.5.1 Positive

Test case	Test case description
C_DOes1	TimOperReq[test not ok] resp-: Send a TimeActivated Operate request, thereby making sure that the device will generate a 'test not Ok'. Check that the client realizes the operation failed.
C_DOes2	OperReq[test not ok] resp-: Send an Operate request, thereby making sure the device will generate a 'test not Ok'. Check that the client realizes the operation failed.
C_DOes3	TimOperReq[test ok] resp+: Send a correct TimeActivated Operate request. - Check that the client realizes the operation request succeeded. - Check that the client notice the operation ended positively when it receives the CommandTermination+. - Check that the client notice the operation ended negatively when it receives the CommandTermination-.
C_DOes4	OperReq[test ok] resp+: Send a correct TimeActivated Operate request. - Check that the client realizes the operation request succeeded. - Check that the client notice the operation ended positively when it receives the CommandTermination+. - Check that the client notice the operation ended negatively when it receives the CommandTermination-.

6.3.5.6.5.2 Negative

Test case	Test case description
C_DOesN1	Incorrect Operate Check that the client detects the following situations: - Operate without response. - Operate with delayed response.
C_DOesN2	Incorrect TimedActivatedOperate Check that the client detects the following situations: - TimedActivatedOperate without response. - TimedActivatedOperate with delayed response. - TimedActivated with positive first response and no second response after WaitForActionTime.

Test case	Test case description
	- TimedActivated with negative first response and a second response positive after WaitForActionTime. - TimedActivated with negative first response and a second response negative after WaitForActionTime.
C_DOesN3	OperReq[test ok] resp+ without CommandTermination. Check the client shows an error when after a positive Operate it does not receive any CommandTermination.
C_DOesN4	TimedActivatedOperateReq [test ok] resp+ without CommandTermination. Check the client shows an error when after a positive TimedActivatedOperate it does not receive any CommandTermination.

6.3.5.6.6 SBO control with enhanced security

6.3.5.6.6.1 Positive

Test case	Test case description
C_SBOes1	SelectWithvalue with improper access rights. Select device using SelVal with improper access rights. Check the client notices that he has no access to the controllable object.
C_SBOes2	SelectWithvalue access rights. Select device using SelVal with access rights. Check the client executes the control order after getting access to the controllable object.
C_SBOes3	OperReq[test ok] resp+ of selected object Perform a correct Operate request. Check that the client realizes that the operation succeeded and detects the CommandTermination with the result of the order.
C_SBOes4	OperReq[test not ok] resp- of selected object. Perform an incorrect Operate request. Check that the client realizes that the operation failed.
C_SBOes5	TimOperReq[test ok] resp+ of selected object Perform a correct TimOperate request. Check that the client realizes that the operation succeeded after the WaitForActionTime and detects the CommandTermination with the result of the order.
C_SBOes6	TimOperReq[test ok] resp- of selected object Perform an incorrect TimOperate request. Check that the client realizes the operation failed.

6.3.5.6.6.2 Negative

Test case	Test case description
C_SBOesN1	Incorrect SelectWithValue. Check that the client detects the following situations: - SelectWithValue without response. - SelectWithValue with delayed response.
C_SBOesN2	Incorrect Operate of selected object Check that the client detects the following situations: - Operate without response. - Operate with delayed response.
C_SBOesN3	Incorrect TimedActivatedOperate of selected object Check that the client detects the following situations: - TimedActivatedOperate without response. - TimedActivatedOperate with delayed response. - TimedActivated with positive first response and no second response after WaitForActionTime. - TimedActivated with negative first response and a second response positive after WaitForActionTime. - TimedActivated with negative first response and a second response negative after WaitForActionTime.

Test case	Test case description
C_SBOesN4	Operate of selected object without CommandTermination. Check the client shows an error when after a positive Operate it does not receive any CommandTermination.
C_SBOesN5	TimedActivatedOperate of selected object without CommandTermination. Check the client shows an error when after a positive TimedActivatedOperate it does not receive any CommandTermination.

6.3.5.7 Time and time synchronisation model

Both the IEC 61400-25 series client and server behaves as a client in case of synchronization. The test cases defined for the server are valid for the client.

6.3.6 Acceptance criteria

The intent is to show how all requirements are testable under specified background loads.

Evaluation criteria for testing the Device-Under-Test (DUT) include:

– Specific design characteristics to be validated.
– Checkpoints identified for anomalous conditions.

There are always three possibilities for a test result according to the ISO/IEC 9646 series:

– Pass (verdict) – A test verdict given when the observed test outcome gives evidence of conformance to the conformance requirement(s) on which the test purpose of the test case is focused, and when no invalid test event has been detected.
– Fail (verdict) – A test verdict given when the observed test outcome either demonstrates non-conformance with respect to (at least one of) the conformance requirement(s) on which the test purpose of the test case is focused, or contains at least one invalid test event, with respect to the relevant specification(s).
– Inconclusive (verdict) – A test verdict given when the observed test outcome is such that neither pass nor fail verdict can be given. Such a result shall be always resolved to find out if this behaviour results from the standard, from the implementation or from the test procedure.

In general, a dynamic test case is passed when the DUT behaves as specified in the IEC 61400-25 series and the PIXIT, the test cases are failed when the DUT behaves differently to what is specified in the IEC 61400-25 series and PIXIT. When not specified in the IEC 61400-25 series and in the PIXIT, the DUT shall keep on responding to syntactically correct messages and shall ignore syntactically incorrect messages.

7 Performance tests

7.1 General

The IEC 61400-25 series does not specify any specific performance requirements for applications operating in the IEC 61400-25 series environment, but a series of essential metrics are identified. Based on this fact, this Clause defines the essential metrics identified within devices such that documented product claims supporting those requirements can be compared across vendors.

7.2 Communications latency

7.2.1 Transfer time

The communications transfer time requirements is identified as an essential performance metric. The Transfer time is the time required to deliver a process value from a sending physical device to the process logic of a receiving device. The transfer time is defined in terms of three intervals:

t_a: the time required for the sending device to transmit the process value,

t_b: the time required for the network to deliver the message, and

t_c: the time required for the receiving device to deliver the value to its process logic.

The interval t_b is a determined by the network infrastructure and is not an attribute of the device. From a device testing point of view, only output and input latencies can be measured, t_a and t_c are estimated from the measured latencies.

– measured output latency = estimated input processing time + estimated t_a

– measured input latency = estimated output processing time + estimated t_b

The vendors of network components like switches shall define and document the amount of the latency time that is due to estimated processing time for all priorities supported by the network components.

The estimated input processing time of a WPP device is the time required for input signal conditioning (e.g., debouching, sampling, etc.).

The estimated output processing time of a WPP device is the time required for output signal activation (e.g., contact delays, I/O scan rate, etc.).

The performance metrics to be measured in the WPP devices depend on which of the IEC 61400-25 series services are used to deliver the process values. The IEC 61400-25 series defines three basic mechanisms: Reporting, Logging and Controls. When tested from a black box perspective, each of these mechanisms yields two possible metrics that can be tested.

7.2.2 Methodology

The following time interval measurements shall be made between a physical input (or message) change and the appearance of a message on the output media (or physical output):

– report output latency;

– logging output latency;

– control output latency.

A test system (see Figure 5) shall measure an output latency time by generating a sequence of physical input triggers to the WPP device and measuring the time delay to the corresponding message generated by the device. The mean latency time and the standard deviation shall be computed across the responses to 1 000 input triggers. The vendor shall define and document the amount of the latency time which is due to estimated output processing time.

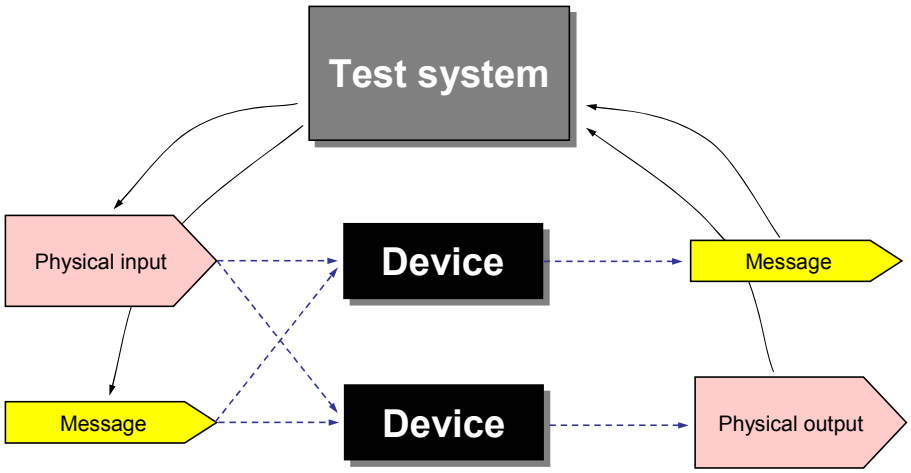

Figure 5 – Performance testing (black box principle)

The results to be documented for each latency test, shall be the measured values and the two corresponding estimated values. The measured values shall be the mean values and the standard deviation of the latency time computed across 1 000 tests.

7.3 Time synchronisation and accuracy

7.3.1 Time Sync test introduction

The objective of this test is to verify the ability of the WPP device to communicate time stamp information about an instrumented event. An accurate time stamp relies on several separate functions including clock accurately decoding the received signal, accurate synchronisation of device clock to the received signal, timely device detection of change of state and accurate use of device clock value to time stamp data.

NOTE 1 WPP devices requiring a very high time accuracy may use a directly connected external time source (radio or satellite clock).

Time synchronisation is used for the synchronisation of the device clock values when no direct external time source is available to the WPP. During synchronisation across the WPP system network, one device with a precision time source acts as the time master. A second device of the same type may be defined to act as a backup time master. The time source of the time master device is typically provided by an external source.

The time accuracy metrics defined in this Subclause, represent measures of time stamp accuracy for the WPP when an external source is provided or when the device relies on the time synchronisation mechanism with a time master respectively.

NOTE 2 This test is essential due to the nature of networked WPP devices being used to design systems of interoperable devices working in a coordinated fashion. These, and other device performance measures, are essential information for predicting performance, functionality and reliability of designs executed by networked WPP devices. No specific performance benchmarks are expected to be met, however, verification and publication of actual performance measures is necessary to be conformant. Using these published performance measures; design engineers can predict the performance of the interconnected devices and thus the performance of system. Furthermore, engineers will be able to identify suitable devices for specific applications. Performance measures will be made on the device under test connected to a network with pre-defined configuration and traffic. It is understood that if the network traffic changes, the system performance may change. It is also understood that if the processing load on the device changes, the device performance may change.

7.3.2 Time Sync test methodology

The time synchronisation test requires a test system (see Figure 6) consisting of a data change generator function and a time master function, each connected to a common external clock source (e.g. radio or satellite clock). The change generator function triggers physical events within the WPP device, with accurate times recorded for each event. A test system analyser function retrieves the time stamp of each event from the WPP device and compares it with the recorded time of the event generation.

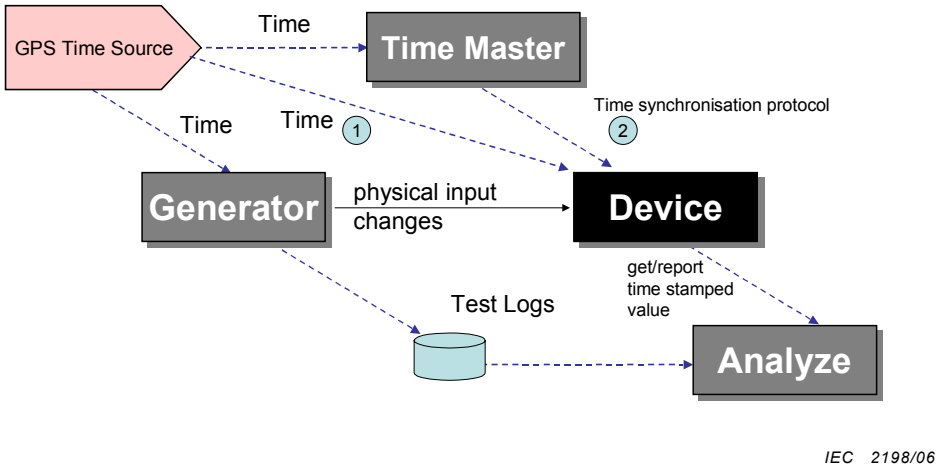

Figure 6 – Time synchronisation and accuracy test setup

Time from external source

The first accuracy measurement is made with the WPP device directly receiving time from the same external source used by the test system (1). A sequence of 1 000 change events is generated, and the mean and standard deviation from the mean is computed over the differences between the event times and the retrieved time stamps.

Time from time synchronisation protocol

The second accuracy measurement is made with the WPP device using the time synchronisation protocol with the Time Master function in the test system. A sequence of 1 000 change events is generated, and the mean and standard deviation from the mean is computed over the differences between the event times and the retrieved time stamps. The event sequence generation shall be coordinated with the time synchronisation protocol. The event sequence shall begin just after the device requests synchronisation with the Time Master function. If synchronisation is requested during the sequence, the sequence is interrupted while the synchronisation protocol exchange is completed.

7.3.3 Testing criteria

Time synchronisation accuracy shall be tested relative to UTC (as provided by the time reference used by the test generator).

NOTE 1 The jitter caused by network components like switches is assumed to be negligible.

The vendors of network components like switches shall define and document the amount of the latency time that is due to estimated processing time for all priorities supported by the network components.

The vendors of WPP devices shall define and document the time drift of the device's internal clock.

NOTE 2 The drift is independent of the time synchronization.

7.4 Stability test

A test to verify the stability of the product over a continuous period shall be conducted with the product configured as it will be used in the field. A duration of 240 hours shall suffice. The test shall include periods of operation under normal activity conditions and operation under heavy activity conditions. All functions shall be operating with simulated inputs throughout the test.

Annex A
(informative)

Examples of test procedure template

A.1 Example 1

RptP1	GetLogicalNodeDirectory(BRCB) and GetBRCBValues	☐ Passed ☐ Failed ☐ Inconclusive
IEC 61400-25-3, xx IEC 61400-25-2, yy		
Expected result 1) DUT sends GetLogicalNodeDirectory(BRCB) Response+ 2) DUT sends GetBRCBValues Response+		
Test description 1) For each logical node Client requests GetLogicalNodeDirectory(BRCB) 2) For each BRCB Client requests GetBRCBValues()		
Comment		

A.2 Example 2

RptP2	GetLogicalNodeDirectory(URCB) and GetURCBValues	☐ Passed ☐ Failed ☐ Inconclusive
IEC 61850-7-2, 9.2.2 and 14.2.5.3 IEC 61850-8-1, 12.3.1 and 17.2.4		
Expected result 1) DUT sends GetLogicalNodeDirectory(URCB) Response+ 2) DUT sends GetURCBValues Response+		
Test description 1) For each logical node Client requests GetLogicalNodeDirectory(URCB) 2) For each BRCB Client requests GetURCBValues()		
Comment		

Bibliography

IEC 61850-2:2003, *Communication networks and systems in substations – Part 2: Glossary*

IEC 61850-4:2002, *Communication networks and systems in substations – Part 4: System and project management*

IEC 61850-5:2003, *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models*

IEC 61850-6:2004, *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-3:2003, *Communication networks and systems in substations – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes*

IEC 61850-8-1:2004, *Communication networks and systems in substations – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

ISBN 2-8318-8910-3

ICS 27.180

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND