INTERNATIONAL STANDARD

IEC 61850-10

First edition
2005-05

Communication networks and systems in substations –

Part 10: Conformance testing

Reference number
IEC 61850-10:2005(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 On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.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 61850-10

First edition
2005-05

Communication networks and systems in substations –

Part 10: 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

COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATIONS –

Part 10: 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 61850-10 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

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

FDIS	Report on voting
57/742/FDIS	57/749/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.

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

IEC 61850 consists of the following parts, under the general title *Communication networks and systems in substations*:

Part 1: Introduction and overview

Part 2: Glossary

Part 3: General requirements

Part 4: System and project management

Part 5: Communication requirements for functions and device models

Part 6: Configuration description language for communication in electrical substations related to IEDs

Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models

Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)

Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes

Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes

Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3

Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link

Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3

Part 10: Conformance testing

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 edition of this standard may be issued at a later date.

INTRODUCTION

This part of IEC 61850 is part of a set of specifications which details a layered substation communication architecture.

This part of IEC 61850 defines:

- the methods and abstract test cases for conformance testing of devices used in substation automation systems, and
- the metrics to be measured within devices according to the requirements defined in IEC 61850-5.

The intended readers are test system developers.

NOTE 1 Tests regarding EMC requirements and environmental conditions are subject to IEC 61850-3 and not included in this part of IEC 61850.

NOTE 2 It is recommended that IEC 61850-5 and IEC 61850-7-1 be read first in conjunction with IEC 61850-7-2, IEC 61850-7-3, and IEC 61850-7-4.

NOTE 3 Abbreviations used in IEC 61850-10 are listed in Clause 4 or may be found in other parts of IEC 61850 that are relevant for conformance testing.

COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATIONS –

Part 10: Conformance testing

1 Scope

This part of IEC 61850 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 the system integrator to integrate IEDs easily, operate IEDs correctly, and support the applications as intended.

NOTE 1 The role of the test facilities for conformance testing and certifying the results are beyond the scope of this part of IEC 61850.

NOTE 2 The test approach and test system design to test a client device is likely to be different across the broad range of clients. There are many possibilities to test clients. The client tests are beyond the scope of this part of IEC 61850. It is intended to define client test requirements during the maintenance of this part.

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

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

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

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

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

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

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

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

IEC 61850-8-1, *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*

IEC 61850-9-1, *Communication networks and systems in substations – Part 9-1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link*

IEC 61850-9-2, *Communication networks and systems in substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

ISO/IEC 9646-1, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts*

ISO/IEC 9646-2, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification*

ISO/IEC 9646-4, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 4: Test realization*

ISO/IEC 9646-5, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 5: Requirements on test laboratories and clients for the conformance assessment process*

ISO/IEC 9646-6, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 6: Protocol profile test specification*

3 Terms and definitions

For the purpose of this document, the terms and definitions provided in IEC 61850-2 as well as the following definitions 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 as specified in a specific customer specification. The FAT will be carried out in the factory of the manufacturer or other agreed-upon location by the use of process simulating test equipment.

3.2
hold point
point, defined in the appropriate document beyond which an activity shall not proceed without the approval of the initiator of the conformance test. The test facility shall provide a written notice to the initiator at an agreed time prior to the hold point. The initiator or his representative is obligated to verify the hold point and approve the proceeding of the activity.

3.3
interoperability
ability of two or more IEDs from the same vendor (or different vendors) to exchange information and use that information for correct co-operation.

A set of values having defined correspondence with the quantities or values of another set.

3.4
Model Implementation Conformance Statement
MICS
details the standard data object model elements supported by the system or device

3.5
negative test
test to verify the correct response of a system or a device when subjected to:

– IEC 61850 series conformant information and services which are not implemented in the system or device under test;

– non IEC 61850 series conformant information and services sent to the system or device under test

3.6
Protocol Implementation Conformance Statement
PICS
summary of the communication capabilities of the system or device to be tested

3.7
Protocol Implementation eXtra Information for Testing
PIXIT
the Protocol Implementation eXtra Information for Testing document contains system or device specific information regarding the communication capabilities of the system or device to be tested and which are outside the scope of the IEC 61850 series. The PIXIT is not subject to standardisation.

3.8
routine test
performed by the manufacturer in order to ensure device operation and safety

3.9
Site Acceptance Test
SAT
verification of each data and control point and the correct functionality within the SAS and between the SAS and its operating environment at the whole installed plant by use of the final parameter set as specified in a specific customer specification. The SAT is the precondition for the SAS being put into operation.

3.10
system related test
verification of correct behaviour of the IEDs and of the overall SAS under specific application conditions. The system related test is part of the final stage of the development of IEDs as belonging to a SAS-product family.

3.11
test equipment
all tools and instruments which simulate and verify the input/outputs of the operating environment of the SAS such as switchgear, transformers, network control centres or connected telecommunication units on the one side, and the serial links between the IEDs of the SAS on the other

3.12
test facility
organisation able to provide appropriate test equipment and trained staff for conformance testing. The management of conformance tests and the resulting information should follow a quality system.

3.13
type test
verification of correct behaviour of the IEDs of the SAS by use of the system tested software under the test conditions corresponding with the technical data

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

3.14
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
ASDU	Application Service Data Unit
BRCB	Buffered Report Control Block
CDC	Common Data Class
CT	Current Transducer
DTD	Document Type Definition
DUT	Device Under Test
FAT	Factory Acceptance Test
GI	General Interrogation
GoCB	GOOSE Control Block
GOOSE	Generic Object Oriented Substation Events
GSE	Generic Substation Event
GSSE	Generic Substation Status Event
GsCB	GSSE Control Block
HMI	Human Machine Interface
ICD	IED Capability Description
IED	Intelligent Electronic Device
IP	Internet Protocol
LCB	Log Control Block
LD	Logical Device
LN	Logical Node
MC	MultiCast
MCAA	Multicast Application Association
MICS	Model Implementation Conformance Statement
MMS	Manufacturing Message Specification (ISO 9506 series)
MSVCB	Multicast Sampled Value Control Block
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
RTU	Remote Terminal Unit
SAS	Substation Automation System

SAT	Site Acceptance Test
SAV	Sampled Analogue Value (IEC 61850-9 series)
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description.
SCL	Substation Configuration Language
SCSM	Specific Communication Service Mapping
SGCB	Setting Group Control Block
SoE	Sequence-of-Events
SSD	System Specification Description
SUT	System Under Test
SV	Sampled Values
SVC	Sampled Value Control
TCP	Transport Control Protocol
TPAA	Two Party Application Association
URCB	Unbuffered Report Control Block
USVCB	Unicast Sampled Value Control Block
UTC	Coordinated Universal Time
VT	Voltage Transducer
XML	eXtensible Markup Language

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.

The quality system of the producer/supplier forms the basis of reliable testing in development and production activities.

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 document, the term type test is restricted to the functional behaviour of the device.

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 system related test of the incorporated IEDs. As a global communications standard, the IEC 61850 series includes standardised conformance tests to ensure 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 related tests such as the FAT and SAT. The FAT and SAT are based on specific customer requirements for a dedicated substation automation system and are done by the system integrator and normally witnessed by the customer. These tests increase the confidence level that all potential problems in the system have been identified and solved. These tests establish that the delivered substation automation system is performing as specified.

5.2 Conformance test procedures

In general, conformance testing of the communication behaviour of an IED should address the functional requirements and performance requirements of typical applications supported by these devices in a SAS. IEC 61850-4 defines a general classification of quality tests, which are used within this part.

Conformance testing demonstrates the capability of the DUT to operate with other IEDs in a specified way according to the IEC 61850 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 IEDs from different world-wide suppliers. Therefore, a standardised test architecture with device simulators should be used. The use of such a test architecture implies agreement about its configuration and the test procedures applied in order to achieve compatible and reproducible 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 61850 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 standard, 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 61850 series. The IEC 61850 series is focussed on interoperability using data, function and device models including all services above or at the application level (ACSI). In addition, performance classes are addressed.

Since the IEC 61850 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. This shall be clearly demonstrated by the test facility. This applies to the quality systems of all sub-suppliers.

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 conformance test quality plan shall meet the requirements of ISO 9001. The plan shall describe all measures for the scope of work and/or deliveries in the areas of budget, organisation, time, information and quality. There is only one plan for the test facility and its sub-suppliers.

The conformance test quality plan shall also contain the following:

– A complete and detailed description of the work methods. This will help ensure 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;
– by whom the inspections, tests and registrations will be performed.

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

The test facility shall provide 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 facility's site during the execution of a test or inspection can be made at the initiator's site in which case the test facility shall provide all relevant documentation to the initiator.

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.

5.3.2.3 Audits requested by initiator

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 ready for testing;
– Protocol Implementation Conformance Statement (PICS). A standard PICS, also known as PICS proforma shall be supplied (see IEC 61850-7-2, Annex A);
– 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:

1) Static conformance requirements (define the requirements the implementation shall fulfil);
2) 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.

A standard PICS shall be supplied.

Concrete PICS shall be as defined for the SCSMs.

A Model Implementation Conformance Statement or MICS shall be provided detailing the data object model elements supported by the system or device. The MICS is implemented in the file SCD (Substation configuration description) according to IEC 61850-6.

In addition to the PICS, a Protocol Implementation eXtra Information for Testing or PIXIT document shall be provided.

The process of assessing the conformance is shown in Figure 1.

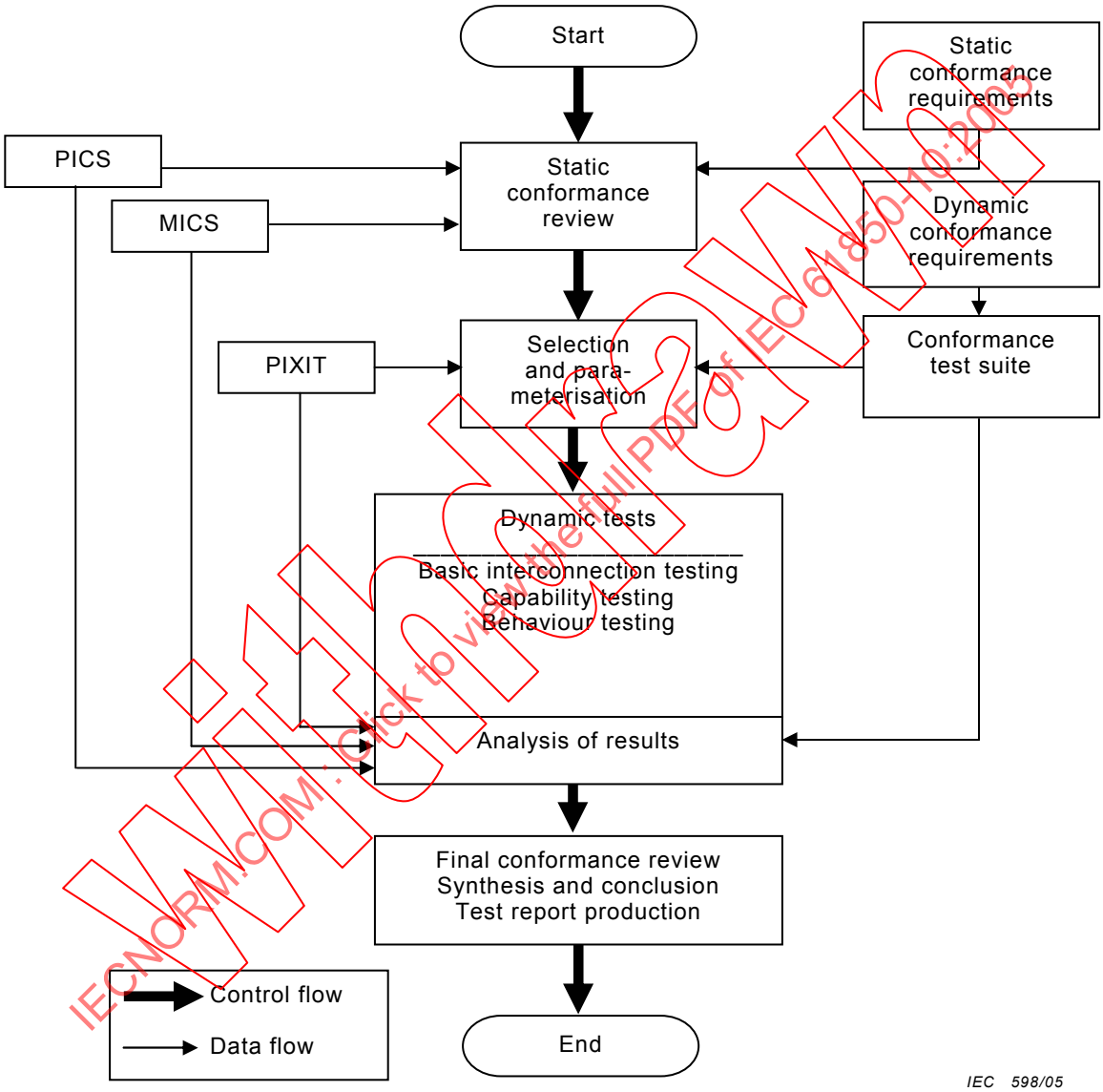

Figure 1 – Conceptual conformance assessment process

5.4.2 Use of SCL files

The DUT shall be delivered with an ICD file.

The test entity shall generate from the ICD file, the corresponding SCD file based on the configuration of the test system. If the test entity requires that the initiator of a conformance test also provides the SCD file, then the test entity shall provide the SSD file and the SCD file of the test system.

5.4.3 Device testing

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

NOTE The device test may require a base load generator. The definition of base load is beyond the scope of this part of the IEC 61850 series. The use of priorities according to IEC 61850-8-1 and IEC 61850-9-2 mitigates the use of base load simulation for time critical information exchange like for GSE and sampled value exchange.

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 (IEC 61850-4);
– test of device configuration file against standardised syntax (schema) (IEC 61850-6);
– test of device configuration file against the device related object model (IEC 61850-7-4, IEC 61850-7-3);
– test of communication stack implementation against applicable SCSM (IEC 61850-8-1, IEC 61850-9-1, and IEC 61850-9-2);
– test of implemented ACSI services against ACSI definition (IEC 61850-7-2);
– test of device specific extensions according to rules given by the IEC 61850 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 subclauses. 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 the tested device.
– Name and address of the test facility.
– Date of issue of the 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 procedure how to perform the test and the expected result;
  - reference to the IEC 61850 series Part, Clause and Subclause;
  - unique identifier per test item;
  - test result: Passed, Failed, Inconclusive, Not applicable or <empty> = not tested;
  - 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. The consequences and requirements of re-testing of a server device – if required – shall be specified in corresponding test plans and test reports.

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.

NOTE Messages have to be generated to test the communication capabilities. Hardwired stimuli (contacts, voltages, currents, etc.) and stimuli coming over a serial link if applicable should be used if applicable.

Special attention shall be given to communication equipment such as star-couplers, switches, etc. which shall support all requested features of the standard but not introduce additional contingencies and limitations. The impact of the communication method (client-server, GOOSE, GSSE, etc.) used by the DUT shall be considered properly in the test procedures. Verification of functional applications (use of GOOSE messages) 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 2, which depicts the set-up for station bus, the process bus, and DUTs). 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.

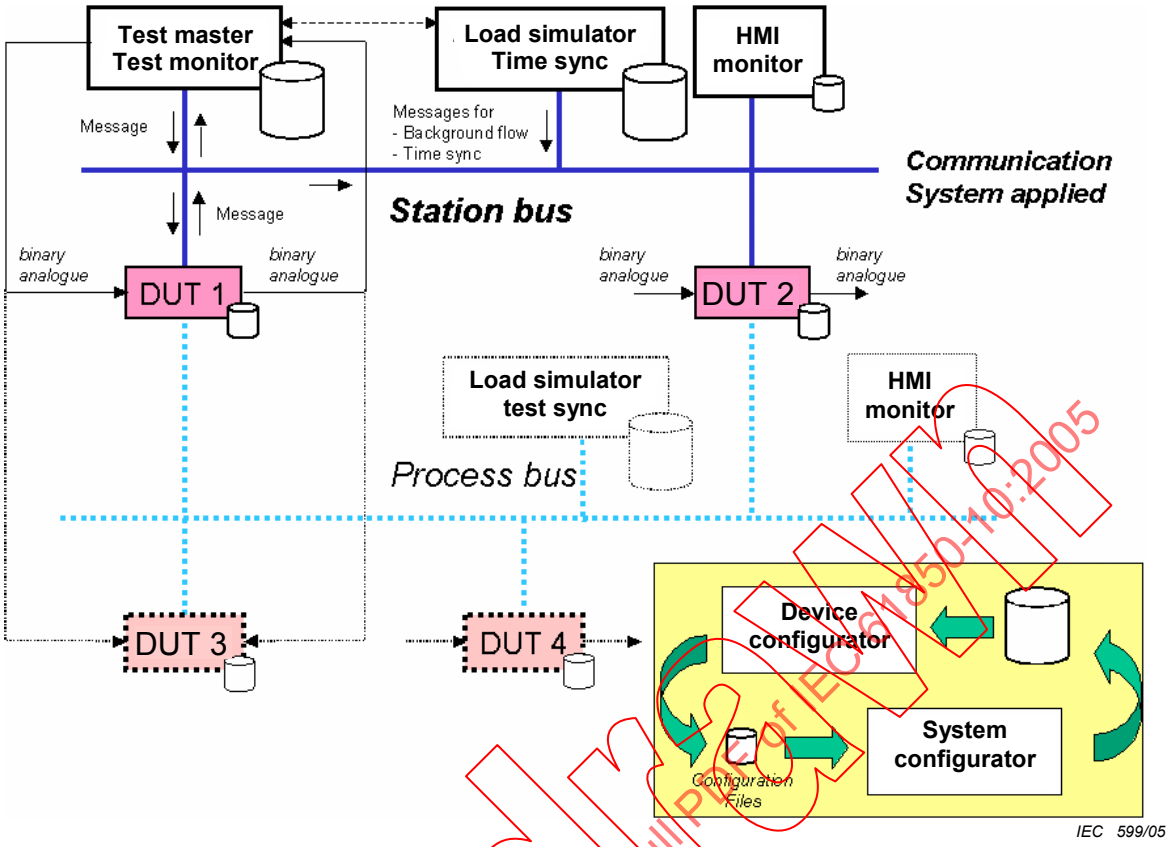

Figure 2 – Conceptual test system architecture

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:

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

6.2 Conformance test procedures

6.2.1 General

This subclause describes the test procedure requirements, test structure, the test cases (what is to be tested), the format and a few examples of test procedures (how to be tested) which are given in Annex A.

6.2.2 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 can't 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 9646 series terminology.

The test procedures shall be formatted as outlined in Figure 3. With this format, the test procedures document can also be used as test report. A few test procedure examples are depicted in Annex A.

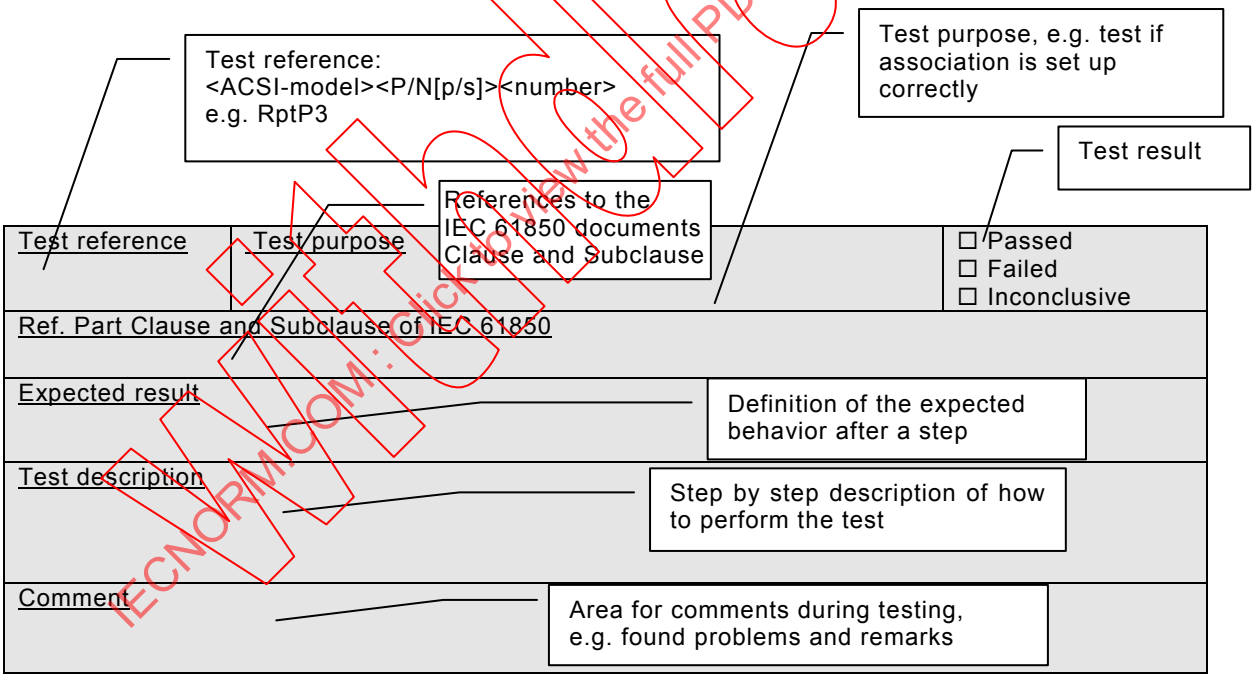

Figure 3 – Test procedure format

IEC 600/05

6.2.3 Test structure

The server test cases are structured as follows:

a) Documentation and version control (IEC 61850-4).
b) Configuration file (IEC 61850-6).
c) Data model (IEC 61850-7-3 and IEC 61850-7-4).

d) Mapping of ACSI models and services (IEC 61850-7-2 and applicable SCSM); the corresponding subclauses that define the abstract test cases are given in brackets:
   – application association model (6.2.4.6)
   – server, logical device, logical node, and data model (6.2.4.7)
   – data set model (6.2.4.8)
   – substitution model (6.2.4.9)
   – setting group control model (6.2.4.10)
   – reporting model (6.2.4.11)
   – log model (6.2.4.12)
   – generic substation events model (6.2.4.13)
   – transmission of sampled values model (6.2.4.14)
   – control model (6.2.4.15)
   – time and time synchronization model (6.2.4.16)
   – file transfer model (6.2.4.17)
   – combination test case (6.2.4.18)

6.2.4 Test cases to test a server

6.2.4.1 General

This part of the IEC 61850 series specifies abstract test cases (see 6.2.4.6 to 6.2.4.18). The abstract test cases shall be used for the definition of test procedures to run in tests.

NOTE 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.

6.2.4.2 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 61850-4).

6.2.4.3 Configuration file test cases

Test if the ICD configuration file conforms to the SCL XML schema definition according to IEC 61850-6.

Check if the ICD configuration file corresponds with the actual data, data types and services exposed by the DUT on the network.

Change end-user configurable parameters in the SCD configuration file, configure the DUT using the SCD configuration file (using the supplied configuration tool) and check the configuration using online services corresponds with the SCD file.

6.2.4.4 Data model test cases

The data model test cases shall

– verify the presence of mandatory objects for each LN (presence = M, optional = O, and conditional = C);
– verify that conditional objects are present and correct;
– verify the data type of all objects for each LN; and
– verify that data attribute values from the device are in the 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/C presence indication (from IEC 61850-7-3 and IEC 61850-7-4), snapshot attribute values and applicable error indication.

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 61850-7-3 and IEC 61850-7-4. These definitions are found also in the ICD file and by the response of the service GetDirectory if applicable.

The data model mapping shall be verified:

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

6.2.4.5 Mapping of ACSI models and services test cases

Test items shall be grouped together in tables. The tables shall reflect the services specified in the models in 5.2 of IEC 61850-7-2:

– Application association (Ass);
– Server, Logical device, Logical node, Data, and Data Attribute model (Srv);
– Data set model (Dset);
– Setting group model (Sg);
– Report control model (Rpt);
– Log control model (Log);
– Generic object oriented system-wide events (Goo);
– Control model (Ctl);
– Substitution model (Sub);
– Transmission of sampled values model (Sv);
– Time and time synchronisation model (Tm);
– File transfer model (Ft).

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. The test result interpretation (passed/failed) depends on the declared IED capabilities e.g. in the ICD file as well as on the test result.

6.2.4.6 Application association model

6.2.4.6.1 Positive test cases

The test cases listed in Table 1 shall apply.

Table 1 – Positive test cases

Test case	Test case description
Ass1	Associate and release a TPAA association (IEC 61850-7-2 Subclause 7.4)
Ass2	Associate and client-abort TPAA association (IEC 61850-7-2 Subclause 7.4)
Ass3	Associate with maximum number of clients simultaneously (PIXIT)

6.2.4.6.2 Negative test cases

The test cases listed in Table 2 shall apply.

Table 2 – Negative test cases

Test case	Test case description
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, Subclause 7.4)
AssN2	Check that with incorrect association parameters at server or client the association fails (IEC 61850-7-2 Subclause 7.4, PIXIT)
AssN3	Disconnect the communication interface, the DUT shall detect link lost within a specified period
AssN4	Interrupt and restore the power supply, the DUT shall accept an association request when ready

6.2.4.7 Server, logical device, logical node, and data model

6.2.4.7.1 Positive test cases

The test cases listed in Table 3 shall apply.

Table 3 – Positive test cases

Test case	Test case description
Srv1	Request GetServerDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2, Subclause 6.2.2)
Srv2	For each GetServerDirectory(LOGICAL-DEVICE) response, issue a GetLogicalDeviceDirectory request and check response (IEC 61850-7-2, Subclause 8.2.1)
Srv3	For each GetLogicalDeviceDirectory response, issue a GetLogicalNodeDirectory(DATA) request and check response (IEC 61850-7-2, Subclause 9.2.2)
Srv4	For each GetLogicalNodeDirectory(DATA) response, issue a – GetDataDirectory request and check response (IEC 61850-7-2, Subclause 10.4.4) – GetDataDefinition request and check response (IEC 61850-7-2, Subclause 10.4.5) – GetDataValues request and check response (IEC 61850-7-2, Subclause 10.4.2)
Srv5	Issue one GetDataValues request with the maximum number of data values and check response
Srv6	For each write enabled DATA object, issue a SetDataValues request and check response (IEC 61850-7-2, Subclause 10.4.2)
Srv7	Issue one SetDataValues request, with the maximum number of data values and check response
Srv8	Request GetAllDataValues for each functional constraint and check response (IEC 61850-7-2, Subclause 9.2.3)

6.2.4.7.2 Negative test cases

The test cases listed in Table 4 shall apply.

Table 4 – Negative test cases

Test case	Test case description
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, Subclause 6.2.2) – GetLogicalDeviceDirectory (IEC 61850-7-2, Subclause 8.2.1) – GetLogicalNodeDirectory(DATA) (IEC 61850-7-2, Subclause 9.2.2) – GetAllDataValues (IEC 61850-7-2, Subclause 9.2.3) – GetDataValues (IEC 61850-7-2, Subclause 10.4.2) – SetDataValues (IEC 61850-7-2, Subclause 10.4.3) – GetDataDirectory (IEC 61850-7-2, Subclause 10.4.4) – GetDataDefinition (IEC 61850-7-2, Subclause 10.4.5)
SrvN2	Request SetDataValues of ENUMERATED data with out-of-range value and verify response– service error (IEC 61850-7-2 Subclause 10.4.2)
SrvN3	Request SetDataValues with mismatching data type (e.g. int-float) and verify response– service error (IEC 61850-7-2 Subclause 10.4.2)
SrvN4	Request SetDataValues for read-only data values and verify response– service error (IEC 61850-7-2 Subclause 10.4.2)

6.2.4.8 Data set model

6.2.4.8.1 Positive test cases

The test cases listed in Table 5 shall apply.

Table 5 – Positive test cases

Test case	Test case description
Dset1	Request GetLogicalNodeDirectory(DATA-SET) and check response (IEC 61850-7-2 Subclause 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)
Dset2	Request a persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2 Subclause 11.3.4) and verify that the persistent data set is visible for another client
Dset3	Request a non-persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2 Subclause 11.3.4) and verify that the non-persistent data set is not visible for another client
Dset4	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
Dset5	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
Dset6	Create a non-persistent dataset, release/abort the association, associate again and check the dataset has been deleted (IEC 61850-7-2 Subclause 11.1)
Dset7	Create a persistent dataset, release/abort the association, associate again and check the dataset is still present (IEC 61850-7-2 Subclause 11.1)
Dset8	Create and delete a persistent data set and verify that every data set can be created normally; repeat the process of creating and deleting one time
Dset9	Create and delete a non-persistent data set and verify that every data set can be created normally; repeat the process of creating and deleting one time
Dset10	Verify SetDataSetValues/GetDataSetValues with GetDataValues and SetDataValues

6.2.4.8.2 Negative test cases

The test cases listed in Table 6 shall apply.

Table 6 – Negative test cases

Test case	Test case description
DsetN1	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 Subclause 11.3.2) - SetDataSetValues (IEC 61850-7-2 Subclause 11.3.3) - CreateDataSet (IEC 61850-7-2 Subclause 11.3.4) - DeleteDataSet (IEC 61850-7-2 Subclause 11.3.5) - GetDataSetDirectory (IEC 61850-7-2 Subclause 11.3.6)
DsetN2	Create a persistent dataset with the same name twice, and verify response– service error
DsetN3	Create a non-persistent dataset with the same name twice, and verify response– service error
DsetN4	Create more than maximum number of persistent data sets and verify response– service error
DsetN5	Create more than maximum number of non-persistent datasets and verify response– service error
DsetN6	Create a persistent dataset with more than maximum number of members and verify response– service error
DsetN7	Create a non-persistent dataset with more than maximum number of members and verify response– service error
DsetN8	Create a persistent dataset with unknown members, and verify response– service error
DsetN9	Create a non-persistent dataset with unknown members, and verify response– service error
DsetN10	Delete a (pre-defined) non-deletable dataset, and verify response– service error
DsetN11	Delete a persistent dataset twice, and verify response– service error
DsetN12	Delete a non-persistent dataset twice, and verify response– service error
DsetN13	Delete a dataset referenced by a (report) control class, and verify response– service error (IEC 61850-7-2 Subclause 11.1)
DsetN14	Request SetDataSetValue with a dataset with one or more read-only members, and verify response– service error

6.2.4.9 Substitution model

6.2.4.9.1 Positive test cases

The test cases listed in Table 7 shall apply.

Table 7 – Positive test cases

Test case	Test case description
Sub1	Disable subEna and set subVal, subMag, subCMag, subQ and verify that the substituted values are not transmitted when subEna is disabled and are transmitted when subEna enabled (IEC 61850-7-2 Subclause 12)
Sub2	Verify that in case the association fails, the substituted values shall remain unchanged

6.2.4.9.2 Negative test cases

The test case listed in Table 8 shall apply.

Table 8 – Negative test cases

Test case	Test case description
SubN1	Verify setting of subVal, subMag, subCMag, subQ (if subEna is true) results in an immediate value change of the corresponding process attribute(s) (Clause 12)

6.2.4.10 Setting group control model

6.2.4.10.1 Positive test cases

The test cases listed in Table 9 shall apply.

Table 9 – Positive test cases

Test case	Test case description
Sg1	Request GetLogicalNodeDirectory(SGCB) and check response+
Sg2	Verify the following setting group state machine path (IEC 61850-7-2 Clause 13 and Figure 18); – SelectEditSGValues – Use SetSGValues [FC=SE] to change values – Use GetSGValues [FC=SE] to verify the new values – ConfirmEditSgValues
Sg3	Verify the following setting group state machine path (IEC 61850-7-2 Clause 13 and Figure 18); – SelectActiveSG of the first setting group – Use GetSGValues [FC=SG] to verify that the values are of the first setting group – Repeat for all setting groups
Sg4	Verify that after loss of association the client can use SelectEditSg again to copy the values to the edit buffer (IEC 61850 7-2 Clause 13.3.3.1)

6.2.4.10.2 Negative test cases

The test cases listed in Table 10 shall apply.

Table 10 – Negative test cases

Test case	Test case description
SgN1	Request the following setting group services with wrong parameters (out of range values, or non existent/null setting group) and verify response– service error – SelectActiveSG (IEC 61850-7-2 Subclause 13.3.2) – SelectEditSGValues (IEC 61850-7-2 Subclause 13.3.3) – SetSGValues (IEC 61850-7-2 Subclause 13.3.4) – ConfirmEditSgValues (IEC 61850-7-2 Subclause 13.3.5) – GetSGValues (IEC 61850-7-2 Subclause 13.3.6) – GetSGCBValues (IEC 61850-7-2 Subclause 13.3.7)
SgN2	Request SetSGValues on an active setting group (FCDA or FCD with FC=SG), verify response– service error
SgN3	Request SetSGValues (FC=SE) and then SelectEditSGValues another setting group, verify that changes will be lost
SgN4	Request SelectEditSGValues of the first setting group, change one value and SelectEditSgValues of the second setting group without (ConfirmEditSgValues). Verify the response–

6.2.4.11 Reporting model

6.2.4.11.1 Positive test cases

The test cases listed in Table 11 shall apply.

Table 11 – Positive test cases

Test case	Test case description
Rpt1	Request GetLogicalNodeDirectory(BRCB) and check response Request GetBRCBValues of all responded BRCB's
Rpt2	Request GetLogicalNodeDirectory(URCB) and check response Request GetURCBValues of all responded URCB's
Rpt3	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 Subclause 14.2.3.2.2.1), force/trigger a report and check the reports contain the enabled optional fields (IEC 61850-7-2 Subclause 14.2.1)
Rpt4	Verify the reporting of optional fields of a BRCB (see Rpt3)
Rpt5	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 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 Subclause 14.2.3.2.2.9) – Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2 Subclause 14.2.3.2.3.2) – Verify that reports are only sent when RptEna is set to True. (IEC 61850-7-2 Subclause 14.2.2.5), when reporting is disabled no reports shall be transmitted
Rpt6	Verify the trigger conditions of a BRCB (see Rpt5)
Rpt7	General interrogation for URCB 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 Subclause 14.2.2.13)
Rpt8	General interrogation for BRCB See Rpt7.
Rpt9	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 Subclause 14.2.3.2.2.5): – SeqNum (not changed) – SubSeqNum (0 for first report, incrementing, roll-over) – MoreSegmentsFollow – TimeOfEntry (not changed as SeqNum is not altered) (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 14.2.3.2.3.4)

Test case	Test case description
Rpt10	Configuration revision (IEC 61850-7-2 Subclause 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 Subclause 14.2.2.7) – Verify that configuration changes of 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 Subclause 14.2.2.7, Note)
Rpt11	Buffer Time (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 14.2.2.9) – Verify that the BufTm value can contain at least the value 3 600 000 (= one hour in milliseconds)
Rpt12	Buffered reporting (BRCB) state machine (IEC 61850-7-2 Subclause 14.2.2.5 and Figure 20) – Verify that events are buffered after the association is released – Verify that 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 Subclause 14.2.1, IEC 61850-7-2 Subclause 14.2.2.5) – Do the same but now set PurgeBuf to True before enabling the reporting. No stored buffered reports shall be send (IEC 61850-7-2 Subclause 14.2.2.14) – Verify that all buffered events are sent before an integrity or general-interrogation report can be sent (IEC 61850-7-2 Subclause 14.2.3.2.3.3, IEC 61850-7-2 Subclause 14.2.3.2.3.4) – Verify that after changing DatSet, the report buffer is purged. (IEC 61850-7-2 Subclause 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 Subclause 14.2.3.2.2.8)

6.2.4.11.2 Negative test cases

The test cases listed in Table 12 shall apply.

Table 12 – Negative test cases

Test case	Test case description
RptN1	Request GetxRCBValues with wrong parameters and verify response– service error (IEC 61850-7-2 Subclause 14.2.3.3.2)
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 Subclause 14.2.3.2.2.9)
RptN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2 Subclause 14.2.2.12)
RptN4	Incorrect configuration of a URCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set
RptN5	Incorrect configuration of a BRCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set
RptN6	Exclusive use of URCB and lost association Configure a URCB and set the Resv attribute and enable it. Verify that by any client only RptEna can be set to FALSE, and no other attribute can be written (IEC 61850-7-2 Subclause 14.2.4.5)
RptN7	Exclusive use of BRCB and lost association Configure a BRCB and enable it. Verify that another client can not set attributes value in this BRCB. (IEC 61850-7-2 Subclause 14.2.1)
RptN8	Configure unsupported URCB options (PIXIT) Configure unsupported trigger conditions, optional fields and related parameters
RptN9	Configure unsupported BRCB options (PIXIT) Configure unsupported trigger conditions, optional fields and related parameters

6.2.4.12 Log model

6.2.4.12.1 Positive test cases

The test cases listed in Table 13 shall apply.

Table 13 – Positive test cases

Test case	Test case description
Log1	Request GetLogicalNodeDirectory(LOG) and check response+
Log2	Request GetLogicalNodeDirectory(LCB) and check response+
Log3	Request GetLCBValues with functional constraint LG of all responded LCB's
Log4	Request SetLCBValues with functional constraint LG when LCB is disabled
Log5	Verify that logging is independent of a limited set of external application associations or other communication transactions
Log6	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
Log7	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 – on data and quality change with integrity period
Log8	Request QueryLogByTime and check response+
Log9	Request QueryLogByEntry and check response+
Log10	Request GetLogStatusValues and check response+, verify that the responded entries indicate the oldest/newest entry ID/time available in the log

6.2.4.12.2 Negative test cases

The test cases listed in Table 14 shall apply.

Table 14 – Negative test cases

Test case	Test case description
LogN1	Request the 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 Subclause 14.3.2.5) – SetLCBValues (IEC 61850-7-2 Subclause 14.3.2.6) – QueryLogByTime (IEC 61850-7-2 Subclause 14.3.5.2) – QueryLogByEntry (IEC 61850-7-2 Subclause 14.3.5.3) – GetLogStatusValues (IEC 61850-7-2 Subclause 14.3.5.4)
LogN2	Request SetLCBValues with functional constraint LG when LCB is enabled and verify response– service error

6.2.4.13 Generic substation events model

6.2.4.13.1 Positive test cases (DUT publish)

The test cases listed in Table 15 shall apply.

Table 15 – Positive test cases

Test case	Test case description
Goo1	Request GetLogicalNodeDirectory(GoCB) and check response+
Goo2	Request GetLogicalNodeDirectory(GsCB) and check response+
Goo3	GOOSE messages are published periodically, check the GOOSE data with configured data; that sqNum is incremented, that stNum has not changed. (IEC 61850-7-2 Subclause 15.2.3.5, IEC 61850-7-2 Subclause 15.2.3.6)
Goo4	Verify for GOOSE and GSSE that sqNum and stNum have the initial value one (1) (IEC 61850-7-2 Subclause 15.2.3.5 and 15.2.3.6, IEC 61850-7-2 Subclause 15.3.4.3 and 15.3.4.4)
Goo5	Force data change of a data value in the GSE dataset, DUT shall publish GOOSE messages as specified/configured, stNum is incremented
Goo6	Verify GOOSE services: request service with legal parameters and check respond (IEC 61850-7-2 Subclause 15.2.2) – GetReference (IEC 61850-7-2 Subclause 15.2.2.3) – GetGOOSEElementNumber (IEC 61850-7-2 Subclause 15.2.2.4) – GetGoCBValues (IEC 61850-7-2 Subclause 15.2.2.5) – SetGoCBValues (IEC 61850-7-2 Subclause 15.2.2.6)
Goo7	Verify GSSE services: request service with legal parameters and check respond (IEC 61850-7-2 Subclause 15.2.2) – GetReference (IEC 61850-7-2 Subclause 15.3.3.3) – GetGSSEElementNumber (IEC 61850-7-2 Subclause 15.3.3.4) – GetGsCBValues (IEC 61850-7-2 Subclause 15.3.3.5) – SetGsCBValues (IEC 61850-7-2 Subclause 15.3.3.6)
Goo8	Disable GSE, verify that changing parameters with SetGo/GsCBValues are active (IEC 61850-7-2 Subclause 15.2.2.5, IEC 61850-7-2 Subclause 15.2.2.6)
Goo9	Verify the sending of current data as initial GOOSE message on device power-up (IEC 61850-7-2 Subclause 15.1)
Goo10	Verify GoEna enables and disables the sending of Gooses (7.2 Subclause 15.2.1.3)

Test case	Test case description
Goo11	Configuration revision (IEC 61850-7-2 Subclause 15.2.1.6)
Goo12	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 – changing the value of the attribute DatSet – ConfRev shall never be 0 (zero) – verify that after a restart of the server, the value of ConfRev remains unchanged
Goo13	Verify that attribute NdsCom is True if DatSet is not yet configured (is NULL) (IEC 61850-7-2 Subclause 15.2.1.7)

6.2.4.13.2 Positive test cases (DUT subscribe)

The test cases listed in Table 16 shall apply.

Table 16 – Positive test cases

Test case	Test case description
GsePs1	Send single GOOSE message with new data and check if the message is received and the data has the new value by, for example, checking binary output, event list, logging or MMI
GsePs2	Send single GOOSE message with the Test parameter set. Check behaviour as specified in PIXIT

6.2.4.13.3 Negative test cases (DUT publish)

The test cases listed in Table 17 shall apply.

Table 17 – Negative test cases

Test case	Test case description
GseNp1	Services: request GOOSE/GSSE service with illegal parameters and verify response– service error (IEC 61850-7-2 Subclause 15.2.2)
GseNp2	Verify that NULL for MemberReference in GetGOOSEElementNumber indicates that no member of the referenced data set is defined. (IEC 61850-7-2 Subclause 15.2.2.4.2.2)
GseNp3	Verify that NULL for Datalabel in GSSE GetReference indicates that no member is defined for the respective DataOffset. (IEC 61850-7-2 Subclause 15.3.3.3.3.2)
GseNp4	GOOSE: Verify that if Gooses are enabled (GoEna = True), no attributes of the GoCB control block can be set except for GoEna. (IEC 61850-7-2 Subclause 15.2.1.3)
GseNp5	GSSE: Verify that if Gooses are enabled (GsEnable = True), no attributes of the GsCB control block can be set except for GsEnable. (IEC 61850-7-2 Subclause 15.3.3.6.3)
GseNp6	Verify that if the number or size of values being conveyed by the elements in the dataset exceeds the SCSM determined maximum number, NdsCom is set to True. (IEC 61850-7-2 Subclause 15.2.1.7)

6.2.4.13.4 Negative test cases (DUT subscribe)

The test cases listed in Table 18 shall apply.

Table 18 – Negative test cases

Test case	Test case description
GseNs1	Check behavior of DUT as specified in PIXIT on – Missing GSE message – Double GSE message – Delayed GSE message – Out of order GSE message
GseNs2	Check behaviour of DUT when the data set configuration mismatches: too many elements, too few elements, element out of order, or element with wrong type

6.2.4.14 Transmission of sampled values model

6.2.4.14.1 Positive test cases (DUT subscribe)

The test cases listed in Table 19 shall apply.

Table 19 – Positive test cases

Test case	Test case description
Sv1	Send MSV messages with new data and check if the message is received and the data has the new value
Sv2	Send USV messages with new data and check if the message is received and the data has the new value

6.2.4.14.2 Positive test cases (DUT publish)

The test cases listed in Table 20 shall apply.

Table 20 – Positive test cases

Test case	Test case description
SvPp1	Request GetLogicalNodeDirectory(MSVCB) and check response+
SvPp2	Request GetLogicalNodeDirectory(USVCB) and check response+
SvPp3	Verify that the transmission of sampled values matches the setting in the xSVCB
SvPp4	Verify that the xSVCB is located in LLN0
SvPp5	Configuration revision (IEC 61850-7-2 Subclause 16.2.1.6)
SvPp6	Verify that ConfRev represents a count of the number of times the configuration with regards to xSVCB has been changed. Changes that shall be counted are: – deletion of a member of the data-set – re-ordering of members in the data-set – any change of a value of the attribute of the data set whose functional constraint equals CF – changing a value of an attribute of xSVCB – ConfRev shall never be 0 (zero) – Verify that after a restart of the server, the value of ConfRev remains unchanged

6.2.4.14.3 Negative test cases (DUT subscribe)

The test cases listed in Table 21 shall apply.

Table 21 – Negative test cases

Test case	Test case description
SvNs1	Check behavior of DUT as specified in PIXIT on – Missing USV/MSV message – Double USV/MSV message – Delayed USV/MSV message – Out of order USV/MSV message
SvNs2	Check behaviour of DUT when the USV/MSV data set configuration mismatches: too many elements, not enough elements, element out of order, or element with wrong type

6.2.4.14.4 Negative test cases (DUT publish)

The test cases listed in Table 22 shall apply.

Table 22 – Negative test cases

Test case	Test case description
SvNp1	Verify that when SVCB is enabled, no changes of the attributes of the SVCB other than disabling shall be allowed
SvNp2	When SVCB is disabled, set unconfigurable attributes in the SVCB and verify the response– service error

6.2.4.15 Control model

6.2.4.15.1 Positive test cases

The test cases listed in Table 23 shall apply.

Table 23 – Positive test cases

Test case	Test case description
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 Subclause 17.2.1) b) SBO-control with normal security (operate once/many) (IEC 61850-7-2 Subclause 17.2.2) c) direct with enhanced security (IEC 61850-7-2 Subclause 17.3.2) d) SBO-control with enhanced security (operate once/many) (IEC 61850-7-2 Subclause 17.3.3) Compare detailed state machine test cases for each control mode
Ctl2	Verify that commands with test mode set are handled according to IEC 61850-7-4 and PIXIT
Ctl3	Select to some SBO control objects and cancel them in opposite order
Ctl4	Time operate a second enhanced security control object before the activation time of the first control object
Ctl5	Change control model using online services

Table 24 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.

Table 24 – Test cases for SBOes

Test case	Test case description
SBOes1	Path SelValReq[test not ok] rsp–: Select device using SelVal with improper access rights. Access shall be denied (IEC 61850-7-2 Subclause 17.2.2)
SBOes2	Path SelValReq[test ok] rsp+: 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)
SBOes3	Path SelValReq[test ok] rsp+ and OperReq[test ok] rsp+: 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)
SBOes4	Path SelValReq[test ok] rsp+ and TimOperReq[test ok] rsp+: 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’
SBOes5	Path SelValReq[test ok] rsp+ and TimOperReq[test ok] rsp+ and TimerExpired [test ok] rsp+: Select device correctly using SelVal Send a correct TimeActivatedOperate request Verify that 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)
SBOes6	Path SelValReq[test ok] rsp+ and OperReq[test ok, OPERATE MANY] rsp+: 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)
SBOes7	Path SelValReq[test ok] rsp+ and TimOperReq[test ok, OPERATE MANY] rsp+ and TimerExpired [test ok] rsp+: 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 reaches the 'between' state (9c)

Table 25 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.

Table 25 – Test cases for DOns

Test case	Test case description
DOns1	Path OperReq[test ok] rsp+ Perform a correct Operate request
DOns2	Path OperReq[test ok] rsp+ Client requests TimOper resulting in Test not ok
DOns3	Path OperReq[test not ok] rsp– Client requests Oper resulting in Test not ok
DOns4	Path TimOperReq[test ok] + TimerExpired[test ok] rsp+ Send a TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Verify that the WaitForActionTime results in a timer expired ‘Test ok’
DOns5	Path TimOperReq[test ok] + TimerExpired[test not ok] rsp– 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’

Table 26 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.

Table 26 – Test cases for SBOns

Test case	Test case description
SBOns1	Path 1 SelectReq[test not ok] rsp–: Select the device using Select with improper access rights. Verify that the device returns to the Unselected state.
SBOns2	Path SelectReq[test ok] rsp+: 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
SBOns3	Path SelectReq[test ok] rsp+ and TimOperReq[test ok] rsp+: 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 that the WaitForActionTime results in a timer expired ‘Test ok, operate once’
SBOns4	Path SelectReq[test ok] rsp+ and OperReq[test ok, OPERATE MANY] rsp+: Select device correctly using Select Verify that sending a correct Operate Many request will return the device to the Ready state
SBOns5	Path SelectReq[test ok] rsp+ and TimOperReq[test ok] rsp+ and TimerExpired[test ok, OPERATE MANY] rsp+: Select device correctly using Select Send a correct TimeActivatedOperate Many request After the timer has expired, verify that the device returns to the Ready state