IEC 61400-25-5

Edition 2.0 2017-09

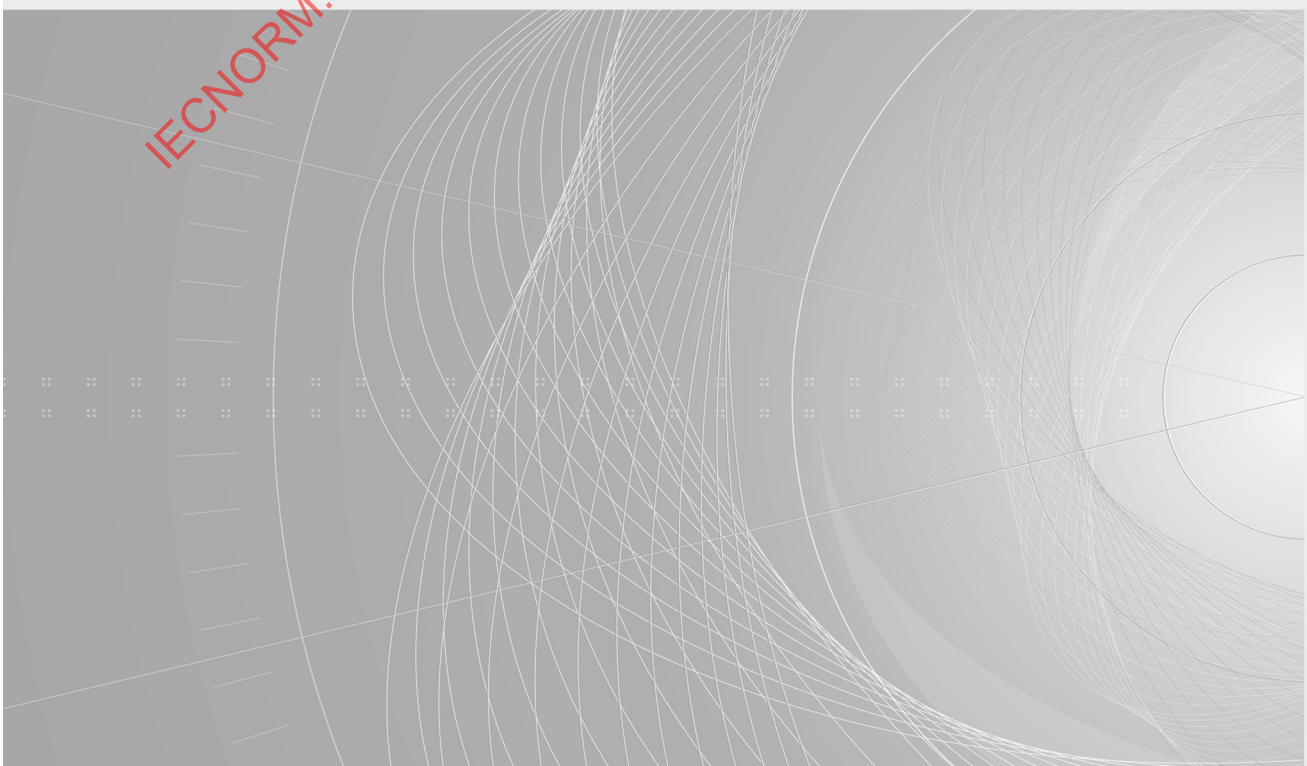
INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Wind energy generation systems – Part 25-5: Communications for monitoring and control of wind power plants – Compliance testing

Systèmes de génération d'énergie éolienne – Partie 25-5: Communications pour la surveillance et la commande des centrales éoliennes – Essai de conformité



IEC 61400-25-5:2017-09(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC 61400-25-5

Edition 2.0 2017-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Wind energy generation systems – Part 25-5: Communications for monitoring and control of wind power plants – Compliance testing

Systèmes de génération d'énergie éolienne – Partie 25-5: Communications pour la surveillance et la commande des centrales éoliennes – Essai de conformité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 27.180

ISBN 978-2-8322-8805-4

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

WIND ENERGY GENERATION SYSTEMS –

Part 25-5: Communications for monitoring and control of wind power plants – Compliance 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

This second edition cancels and replaces the first edition published in 2006. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- Harmonization with structure and test cases in IEC 61850-10:2012.
- The use of SCL in the compliance testing process is out of the scope for this edition, but will be considered for Edition 3.
- Reduction of overlap between standards and simplification by increased referencing to the IEC 61850 standard series.

- All test cases applying SCL files are still not a part of the present document as the SCL specifications for wind power domain are still pending to be published.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
88/643/FDIS	88/650/RVD

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

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

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

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

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

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

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The focus of IEC 61400-25 (all parts) 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 IEC 61400-25 (all parts).

IEC 61400-25 (all parts) 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:

a) wind power plant information models,

b) information exchange model, and

c) 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. IEC 61400-25 (all parts) enables connectivity between a heterogeneous combination of client and servers from different manufacturers and suppliers.

As depicted in Figure 1, IEC 61400-25 (all parts) 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 document is defined in IEC 61400-25-2,

– services to exchange values of the modelled information defined in IEC 61400-25-3,

– mapping to a communication profile, providing a protocol stack to carry the exchanged values from the modelled information (IEC 61400-25-4).

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

The intended readers for the present document are device or system and/or system component manufacturers and test system developers/providers.

NOTE Abbreviations used in IEC 61400-25-5 are listed in Clauses 3 and 4 or can be found in other parts of IEC 61400-25 standard series that are relevant for compliance testing.

WIND ENERGY GENERATION SYSTEMS –

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

1 Scope

This part of IEC 61400-25 specifies standard techniques for testing of compliance 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.

This part of IEC 61400-25 defines:

- the methods and abstract test cases for compliance testing of server and client devices used in wind power plants,
- the metrics to be measured in said devices according to the communication requirements specified in IEC 61400-25 (all parts).

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

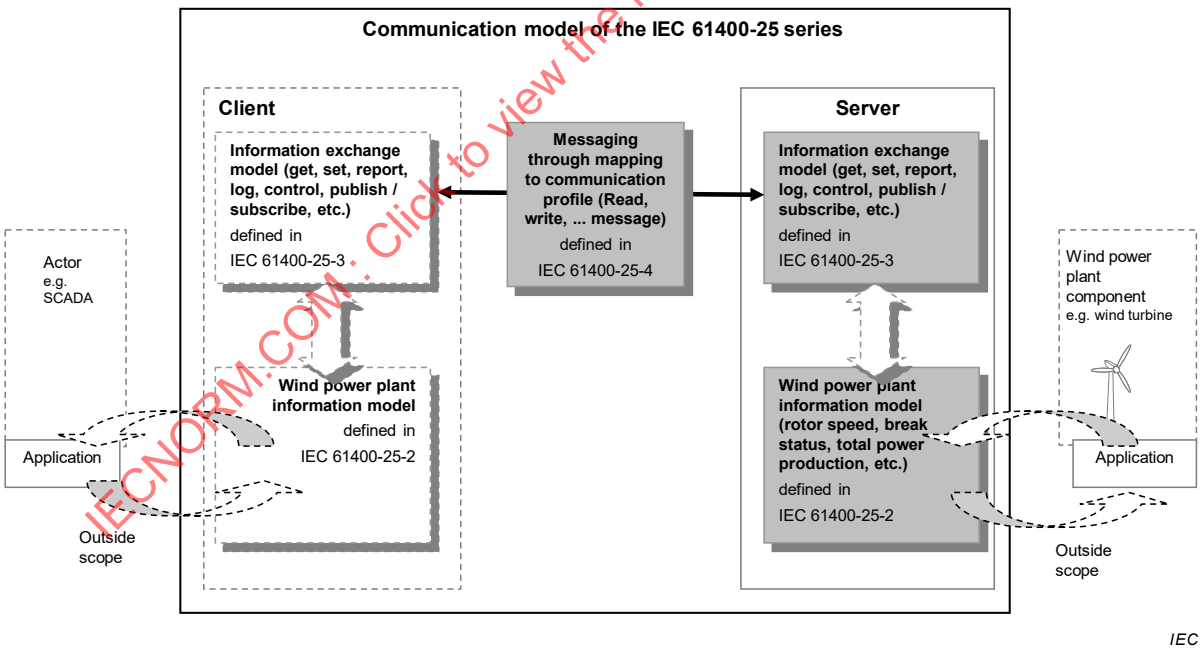


Figure 1 – Conceptual communication model of the IEC 61400-25 standard series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61400-25 (all parts), *Wind turbines – Part 25: Communications for monitoring and control of wind power plants*

IEC 61400-25-1:2006, *Wind turbines – Part 25-1: Communications for monitoring and control of wind power plants – Overall description of principles and models*

IEC 61400-25-2:2015, *Wind turbines – Part 25-2: Communications for monitoring and control of wind power plants – Information models*

IEC 61400-25-3:2015, *Wind turbines – Part 25-3: Communications for monitoring and control of wind power plants – Information exchange models*

IEC 61400-25-4:2016, *Wind energy generation systems – Part 25-4: Communications for monitoring and control of wind power plants – Mapping to communication profile*

IEC 61850-4:2011, *Communication networks and systems for power utility automation – Part 4: System and project management*

IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-1:2011, *Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models*

IEC 61850-7-2:2010, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-3:2010, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-10:2012, *Communication networks and systems for power utility automation – Part 10: Conformance testing*

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

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
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

Note 1 to entry: 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
hold point
point, defined in the appropriate document beyond which an activity shall not proceed without the approval of the initiator of the compliance test

Note 1 to entry: The test facility shall provide a written notice to the initiator at an agreed time prior to the hold point.

Note 2 to entry: 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 devices from the same vendor (or different vendors) to exchange information and use that information for correct co-operation

Note 1 to entry: Set of values defined corresponds with the quantities or values of another set.

3.4
model implementation compliance statement
MICS
statement that 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 device or a system when subjected to:

– IEC 61400-25 (all parts) conformant information and services which are not implemented in the device or system under test,
– non IEC 61400-25 (all parts) conformant information and services sent to the device or system under test

3.6
protocol implementation compliance statement
PICS
statement with the summary of the communication capabilities of the system or device to be tested

3.7
protocol implementation extra information for testing
PIXIT
statement with system or device specific information to be tested and which is outside the scope of IEC 61400-25 (all parts)

Note 1 to entry: The PIXIT is not subject to standardisation.

3.8
routine test
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 WPP and its operating environment at the whole installed plant by use of the final parameter set

Note 1 to entry: The SAT is the precondition for the WPP being put into operation.

3.10
system test
verification of correct behaviour of the WPP components and of the overall WPP under various application conditions

Note 1 to entry: The system test marks the final stage of the development of a WPP system component.

3.11
system related test
verification of correct behaviour of the IEDs and of the overall PUAS under specific application conditions

Note 1 to entry: The system related test is part of the final stage of the development of IEDs as belonging to a PUAS-product family.

3.12
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

3.13
test facility
organisation able to provide appropriate test equipment and trained staff for compliance testing

Note 1 to entry: The management of compliance tests and the resulting information should follow a quality system.

3.14
technical issues compliance statement
TICS
statement with device specific information regarding the implemented technical issues detected after publication of the standard

Note 1 to entry: The TICS is not subject to standardisation.

3.15
type test
verification of correct behaviour of the IEDs (systems components) of the WPP by use of the system tested software under the test conditions corresponding with the technical data

Note 1 to entry: 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.

3.16
witness point
point, defined in the appropriate document, at which an inspection will take place on an activity

Note 1 to entry: The activity may proceed without the approval of the initiator of the compliance 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
CDC	Common Data Class
DUT	Device Under Test
FAT	Factory Acceptance Test
GI	General Interrogation
HMI	Human Machine Interface
ICD	IED capability subscription
IED	Intelligent Electronic Device
IID	Instantiated IED description
IP	Inter-networking protocol internet Protocol
LCB	Log Control Block
LD	Logical Device
LN	Logical Node
MICS	Model Implementation Compliance Statement
PICS	Protocol Implementation Compliance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
PUAS	Power Utility Automation System
RCB	Report Control Block
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SCSM	Specific Communication Service Mapping
SGCB	Setting Group Control Block
SoE	Sequence-of-Events
SUT	System Under Test
TICS	Technical Issues Compliance Statement
TPAA	Two Party Application Association
TUT	Tool Under Test
URCB	Unbuffered Report Control Block
UTC	Coordinated Universal Time
WPP	Wind Power Plant

5 Introduction to compliance 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 component 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 IEC 61400-25 (all parts), 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 compliance 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, IEC 61400-25 (all parts) includes standardised compliance tests to ensure that all suppliers comply with applicable requirements.

Type tests and compliance 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.

Compliance 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 Compliance test procedures

In general, compliance 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.

Compliance testing demonstrates the capability of the Device Under Test (DUT) to operate with other systems or system components in a specified way according to IEC 61400-25 (all parts).

Compliance 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 IEC 61400-25 (all parts). 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 IEC 61400-25 (all parts), some properties of the device may be proven by information and documents provided with the DUT for the compliance testing instead of the compliance test itself.

The compliance test establishes that the communication of the DUT works according to IEC 61400-25 (all parts). IEC 61400-25 (all parts) is focused on interoperability using data objects, functions and device models including services above or at the application level (ACSI).

Since IEC 61400-25 (all parts) defines no new communication stacks, the compliance 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 compliance 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 compliance testing, a quality assurance system has to be in place. This shall be clearly demonstrated by the test facility and apply as well to the quality assurance system of any sub-supplier.

In general, quality surveillance is used to monitor and verify the status of components during all phases of the compliance 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 Compliance test quality plan

The test facility will supply, for evaluation, a quality plan for the compliance 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 compliance test quality plan is proposed to 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 compliance 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 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 compliance 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. The hold or witness point can take place at the test facilities site during the execution of a test, or an inspection can be made at the initiator's site in which case the test facilitator shall provide all relevant documents 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 compliance 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 compliance test. The initiator's right to check that the quality of the compliance test does not dismiss the test facility from its responsibilities.

Inspections and tests by the initiator of a compliance 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

Compliance 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 compliance statement (PICS);
– protocol implementation extra information for testing (PIXIT) statement;
– model implementation compliance statement (MICS); technical issues compliance statement (TICS);
– instruction manuals detailing the installation and operation of the device.

The requirements for compliance testing fall into two categories:

- static compliance requirements (defines the requirements the implementation shall fulfil);
- dynamic compliance requirements (defines the requirements that arise from the protocol used for a certain implementation).

The static and dynamic compliance requirements shall be defined in a protocol implementation compliance statement or PICS. The PICS serves three purposes:

a) selection of the appropriate set of tests;
b) ensure that the tests appropriate to a claim of compliance are performed;
c) provide the basis for the review of the static compliance.

A standard PICS shall be provided.

Concrete PICS shall be as defined for the SCSMs.

A model implementation compliance statement or MICS shall be provided detailing the standard data object model elements supported by the system or device. The MICS is implemented in the ICD of IID file according to IEC 61850-6.

A technical issues compliance statement (TICS) shall be provided detailing the implemented technical issues after publication of the standard.

In addition to the PICS, a protocol implementation extra information for testing (PIXIT) document shall be provided.

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

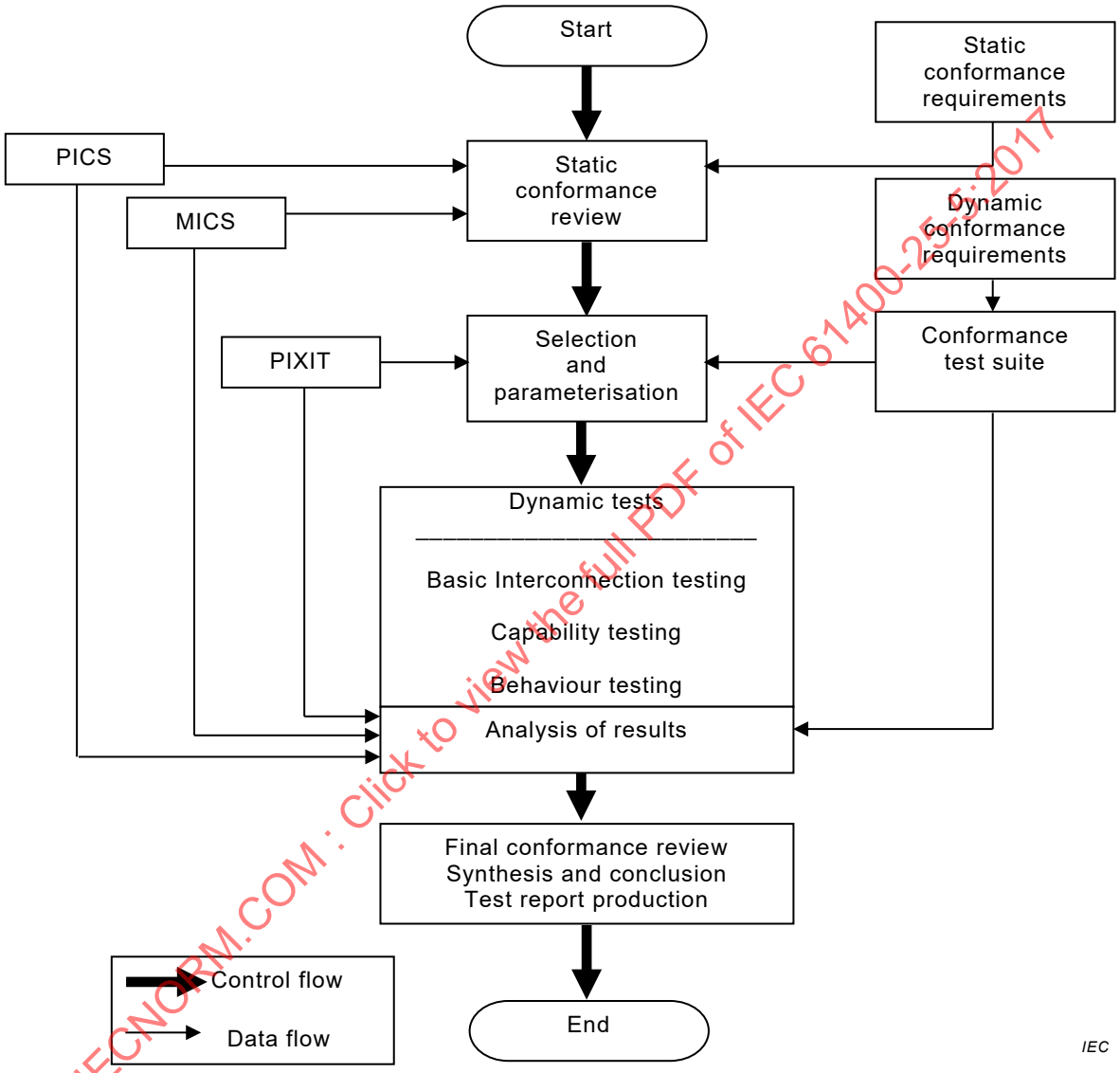


Figure 2 – Conceptual compliance assessment process

5.4.2 Device testing

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

The device-specific compliance 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 IEC 61400-25 (all parts) in general.

5.5 Documentation of compliance test report

A compliance 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, clauses 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 compliance tests.
– Name and address of the vendor.
– Name and address of the initiator of the compliance 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 compliance.
– 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 IEC 61400-25 series (all parts), clause and subclause;
  - 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. The consequences and requirements of re-testing of a device – if required – shall be specified in corresponding test plans and test reports.

Compliance test documentation shall be supplied to the initiator.

6 Device related compliance testing

6.1 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 IEC 61400-25 (all parts), 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 compliance test even if advanced tools may offer such analysis.

6.2 Compliance test procedures

6.2.1 General

Subclause 6.2 describes the test procedure requirements, test structure, the abstract test cases (what is to be tested). The format and two examples of test procedures (how it is to be tested) are given in Annex A.

6.2.2 Test procedure requirements

The test procedure requirements are:

– The abstract 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 3. With this format, the test procedures document can also be used as test report. A few test procedure examples are given in Annex A.

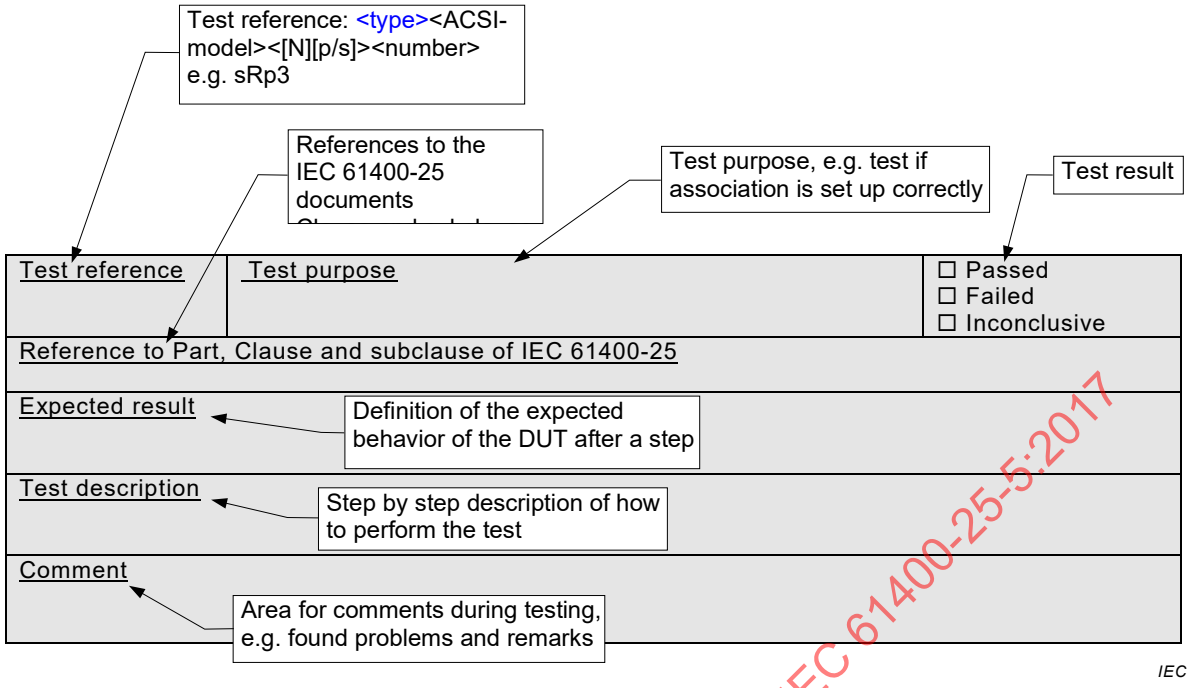


Figure 3 – Test procedure format

6.2.3 Test structure

The server test cases are structured as follows:

– Documentation and version control (IEC 61400-25-5).
– Data model (IEC 61400-25-2).
– Mapping of ACSI models and services (IEC 61400-25-3).
– All test cases are inherited from IEC 61850-10:2012 where applicable for IEC 61400-25 (all parts).

6.2.4 Test cases to test a server device

6.2.4.1 General

This part of IEC 61400-25 specifies the test system architecture and abstract test cases for a server device. The abstract test cases shall be used for the definition of test procedures to run in tests.

The SCSM-specific test procedures shall be provided by test facilities agreed upon by the market participants

6.2.4.2 Test system architecture to test a server device

In order to be able to perform a device test, a minimum test set-up is necessary. The test architecture contains (see Figure 4):

– the DUT;
– a client simulator to initiate and generate TPAA messages and record and process resulting information;
– a master for time synchronisation (the time sync master);
– engineering tool software to configure the DUT;
– a protocol/network analyser to monitor and store all the network traffic for each test case;
– a signal generator to force binary and analogue events, controlled by the test master or test engineer.

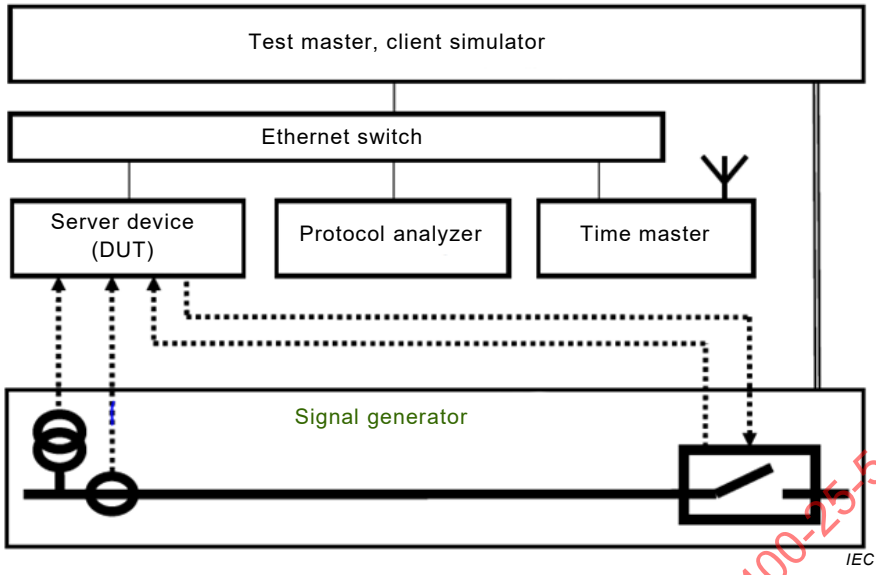


Figure 4 – Test system architecture to test a server device

The test system shall include documentation regarding test system hardware and test system software.

6.2.4.3 Documentation and version control test procedure overview

The test cases listed in Table 1 shall apply.

Table 1 – Server documentation test cases

Test case	Test case description
sDoc1	Check if the major/minor software version in the PICS documentation and the DUT do match (IEC 61850-4). PICS shall contain the ACSI compliance statement according to IEC 61400-25-3
sDoc2	Check if the major/minor software version manufacturer PIXIT documentation and software version of the DUT do match (IEC 61850-4). PIXIT shall indicate the required information as requested in the test cases
sDoc3	Check if the major/minor software version manufacturer MICS documentation and software version of the DUT do match (IEC 61850-4). MICS shall indicate the semantics of all non-standard Logical Nodes, Data Objects, Data Attributes and enumeration
sDoc4	Check if the major/minor software version manufacturer TICS documentation and software version of the DUT do match (IEC 61850-4). TICS shall indicate the implemented technical issues

6.2.4.4 Data model test cases

The test cases listed in Table 2 shall apply.

Table 2 – Server data model test cases

Test case	Test case description
sMdl1	Verify presence of mandatory objects for each LN. Passed when all objects/attributes are present
sMdl2	Verify presence of conditional presence true objects for each LN. Passed when all objects/attributes are present
sMdl3	Verify non-presence of conditional presence false objects. Passed when these objects/attributes are not present
sMdl4	Verify data model mapping according to applicable SCSM concerning name length and object expansion. Passed when mapping is according to applicable SCSM
sMdl5	Verify data model mapping according to applicable SCSM concerning organisation of functional components. Passed when mapping is according to applicable SCSM
sMdl6	Verify data model mapping according to applicable SCSM concerning naming of control blocks and logs. Passed when mapping is according to applicable SCSM
sMdl7	Verify data type of all objects for each LN. Passed when data type of all objects/attributes do match with IEC 61400-25-2, IEC 61400-25-3 and the applicable SCSM
sMdl8	Verify data attribute values from the device are in specified range (this is a continuous effort during the whole compliance test). Passed when all values are in range
sMdl9	Check if manufacturer specific data model extensions are implemented according to the extension rules in IEC 61400-25-2 (only when extensions are implemented). Passed when all extensions are implemented according to the specified rules
sMdl10	Check if the order of the data attributes is within the Data Object types match with IEC 61400-25-2. Passed when all attributes are in matching order
sMdl11	Check the maximum name length of Logical Device, Logical Node, data sets and control blocks according to IEC 61850-7-2:2010, 22.2 and the applicable SCSM.
sMdl12	Check that the rules for multiple data object instantiation are kept (IEC 61850-7-1, IEC 61850-7-4).
sMdl13	Check that the logical device name space refers to IEC 61400-25-2:2015.
sMdl14	Check the correct use of name spaces for non-WPP applications.

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 applicable service models specified in IEC 61850-7-2:2010, Figure 3:

– Application association (sAss);
– Server, Logical device, Logical node, Data, and Data Attribute model (sSrv);
– Data set model (sDs);
– Unbuffered report control model (sRp);
– Buffered report control model (sBr);
– Log control model (sLog);
– Control model (sCtl);
– Time synchronisation model (sTm).

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 61850-7-2:2010, 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

6.2.4.6.1 Positive test cases

The test cases listed in Table 3 shall apply.

Table 3 – Association positive test cases

Test case	Test case description
sAss1	Associate and release a TPAA association (IEC 61850-7-2:2010, 8.3).
sAss2	Associate and client-abort TPAA association (IEC 61850-7-2:2010, 8.3).
sAss3	Associate with maximum number of clients simultaneously (PIXIT).

6.2.4.6.2 Negative test cases

The test cases listed in Table 4 shall apply.

Table 4 – Association negative test cases

Test case	Test case description
sAssN1	Check that with incorrect authentication parameters and authentication turned on at server, the association fails, and with authentication turned off, the server associates (IEC 61850-7-2:2010, 8.3).
sAssN2	Check that with incorrect association parameters at server or client the association fails (IEC 61850-7-2:2010, 8.3, PIXIT).
sAssN3	Set up maximum+1 associations, verify the last associate is refused.
sAssN4	Disconnect the communication interface, the DUT shall detect link lost within a specified period.
sAssN5	Interrupt and restore the power supply, the DUT shall accept an association request when ready.
sAssN6	Verify the re-use of dropped association resources

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 5 shall apply.

Table 5 – Server positive test cases

Test case	Test case description
sSrv1	Request GetServerDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2:2010, 7.2.2)
sSrv2	For each GetServerDirectory(LOGICAL-DEVICE) response issue a GetLogicalDeviceDirectory request and check response (IEC 61850-7-2:2010,9.2.1)
sSrv3	For each GetLogicalDeviceDirectory response issue a GetLogicalNodeDirectory(DATA) request and check response (IEC 61850-7-2:2010, 10.2.2)
sSrv4	For each GetLogicalNodeDirectory(DATA) response issue a – GetDataDirectory request and check response (IEC 61850-7-2:2010, 11.4.4) – GetDataDefinition request and check response (IEC 61850-7-2:2010, 11.4.5) – GetDataValues request and check response (IEC 61850-7-2:2010, 11.4.2)
sSrv5	Issue one GetDataValues request with the maximum number of data values and check response
sSrv6	For each write enabled DATA object issue a SetDataValues request and check response (IEC 61850-7-2:2010, 11.4.3)
sSrv7	Issue one SetDataValues request with the maximum number of data values and check response
sSrv8	Request GetAllDataValues for each functional constraint and check response (IEC 61850-7-2:2010, 10.2.3)
sSrv9	Evaluate the semantic of selected (volt/amp) analogue measurements: – Verify analogue value (plausibility check, not accuracy) – Verify quality bits, force situations to set specific quality bits – Verify (UTC) timestamp value and quality (plausibility check, not accuracy) – Verify scaling, range and units, change a setting and verify resulting value – Verify dead band, change dead band and verify result – Verify limit indications
sSrv10	Evaluate the semantic of selected status points: – Verify status value – Verify quality bits, force situations to set specific quality bits – Verify (UTC) timestamp value and quality (plausibility check, not accuracy)
sSrv11	Verify that when blkEna is set to true by an operator the quality bit oldData and operatorblocked is set by the server and the process data is not updated anymore; by an (internal) automatic function the quality oldData is set and the process data is not updated anymore (IEC 61850-7-3:2010, 6.2.6)
sSrv12	Verify Mod/Beh values: off, test, blocked – When Mod/Beh is off process data is not updated, Mod and Beh are updated, quality is set to invalid – When Mod/Beh is test or test-blocked the process data quality test is set – When Mod/Beh is on-blocked the process data quality operatorBlocked is set – (IEC 61850-7-4:2010, Annex A)
sSrv13	Verify logical device hierarchy; – the LLN0.GrRef should reference a valid logical device – the reference shall not result in a hierarchy loop – Beh value at higher level influences the lower levels correctly (i.e. like LD Beh influences LN behaviour dependent on LN Mod)

6.2.4.7.2 Negative test cases

The test cases listed in Table 6 shall apply.

Table 6 – Server negative test cases

Test case	Test case description
sSrvN1	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 61850-7-2:2010, 7.2.2), – GetLogicalDeviceDirectory (IEC 61850-7-2:2010, 9.2.1), – GetLogicalNodeDirectory(DATA) (IEC 61850-7-2:2010, 10.2.2), – GetAllDataValues (IEC 61850-7-2:2010, 10.2.3), – GetDataValues (IEC 61850-7-2:2010, 11.4.2), – SetDataValues (IEC 61850-7-2:2010, 11.4.3), – GetDataDirectory (IEC 61850-7-2:2010, 11.4.4), – GetDataDefinition (IEC 61850-7-2:2010, 11.4.5).
sSrvN2	Request SetDataValues of ENUMERATED data with out-of-range value and verify response- service error (IEC 61850-7-2:2010, 11.4.3).
sSrvN3	Request SetDataValues with mismatching data type (e.g. int-float) and verify response- service error (IEC 61850-7-2:2010, 11.4.3).
sSrvN4	Request SetDataValues for read-only data values and verify response- service error (IEC 61850-7-2:2010, 11.4.3).

6.2.4.8 Data set model

6.2.4.8.1 Positive test cases

The test cases listed in Table 7 shall apply.

Table 7 – Data set positive test cases

Test case	Test case description
sDs1	Request GetLogicalNodeDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2:2010, 10.2.2). For each response, issue a: – GetDataSetValues request and check response (IEC 61850-7-2:2010, 13.3.2), – GetDataSetDirectory request and check response (IEC 61850-7-2:2010, 13.3.6).
sDs2	Request a persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2:2010, 13.3.4) and verify that the non-persistent data set is visible for another client.
sDs3	Request a non-persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2:2010, 13.3.4) and verify that the persistent data set is not visible for another client.
sDs4	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.
sDs5	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.
sDs6	Create a non-persistent dataset, release/abort the association, associate again and check that the dataset has been deleted (IEC 61850-7-2:2010, 13.1).
sDs7	Create a non-persistent dataset, release/abort the association, associate again and check that the dataset is still present (IEC 61850-7-2:2010, 13.1).
sDs8	Create and delete a persistent dataset and verify that every data set can be created normally: repeat the process of creating and deleting once.
sDs9	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.
sDs10	Verify SetDataSetValues/GetDataSetValues with GetDataValues and SetDataValues.
sDs11	Verify that the maximum number of persistent data sets with the maximum number of members can be created for each of the specified maximum number of clients as specified
sDs12	Verify that the maximum number of non-persistent data sets with the maximum number of members can be created for each of the specified maximum number of clients as specified
sDs13	Verify that a non-persistent data set can be created with the maximum name length for data set and a data set member (IEC 61850-7-2:2010, 22.2)
sDs14	Verify that a persistent data set can be created with the maximum name length for data set and a data set member (IEC 61850-7-2:2010,22.2)

6.2.4.8.2 Negative test cases

The test cases listed in Table 8 shall apply.

Table 8 – Date set negative test cases

Test case	Test case description
sDsN1	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 61850-7-2:2010, 13.3.2) – SetDataSetValues (IEC 61850-7-2:2010, 13.3.3) – CreateDataSet (IEC 61850-7-2:2010, 13.3.4) – DeleteDataSet (IEC 61850-7-2:2010, 13.3.5) – GetDataSetDirectory (IEC 61850-7-2:2010, 13.3.6)
sDsN2	Create a persistent dataset with the same name twice, and verify response-service error
sDsN3	Create a non-persistent dataset with the same name twice, and verify response-service error
sDsN4	Continue to create persistent datasets until a correct response – service error is returned
sDsN5	Continue to create non-persistent datasets until correct response-service error is returned
sDsN6	Create a persistent dataset with unknown members and verify response-service error
sDsN7	Create a non-persistent dataset with unknown members and verify response-service error
sDsN8	Delete a (pre-defined) non-deletable dataset, and verify response-service error
sDsN9	Delete a persistent dataset twice, and verify response-service error
sDsN10	Delete a non-persistent dataset twice, and verify response-service error
sDsN11	Delete a persistent dataset referenced by (report) control class, and verify response-service error (IEC 61850-7-2:2010, 13.1)
sDsN12	Delete a non- persistent dataset referenced by (report) control class, and verify response-service error (IEC 61850-7-2:2010, 13.1)
sDsN13	Request SetDataSetValues with a dataset with one or more read-only members, and verify response-service error

6.2.4.9 Substitution model – Positive test cases

The test cases listed in Table 9 shall apply.

Table 9 – Substitution positive test cases

Test case	Test case description
sSub1	Disable subEna and set subVal, subMag, subCMag, subQ, subID and verify the substituted values are not transmitted when subEna is disabled and are transmitted when subEna is enabled (IEC 61850-7-3:2010, Table 64).
sSub2	Verify that in case the association fails, the substituted values shall remain unchanged
sSub3	Verify setting subVal, subMag, subCMag, subQ and subID is allowed and the substituted values are transmitted and Quality.Source is set to Substituted when subEna is enabled

6.2.4.10 Unbuffered reporting model

6.2.4.10.1 Positive test cases

The test cases listed in Table 10 shall apply.

Table 10 – Unbuffered reporting positive test cases

Test case	Test case description
sRpt1	Request GetLogicalNodeDirectory(URCB) and check response Request GetURCBValues of all responded URCB's
sRpt2	Verify the reporting of optional fields of a URCB Configure/enable a URCB with all optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, and/or data-reference (IEC 61850-7-2:2010, 17.2.3.2.2.1), force/trigger a report and check that the reports contain the enabled optional fields
sRpt3	Verify the trigger conditions of a URCB Configure and enable a URCB with 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 Verify the validity of the ReasonCode (IEC 61850-7-2:2010,17.2.3.2.2.9) Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2:2010,17.2.3.2.3.2) Verify that reports are only sent when RptEna is set to True (IEC 61850-7-2:2010,17.2.2.5), when reporting is disabled no reports should be transmitted
sRpt4	General interrogation (IEC 61850-7-2:2010,17.2.2.13) 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.
sRpt5	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 61850-7-2:2010, 17.2.3.2.2.5) – SeqNum (not changed) – SubSeqNum (0 for first report, incrementing, roll-over) – MoreSegmentsFollow – TimeOfEntry (not changed as SeqNum is not altered) (IEC 61850-7-2:2010,17.2.3.2.2.9) 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 61850-7-2:2010,17.2.3.2.3.5) 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 61850-7-2:2010,17.2.3.2.3.4)
sRpt6	Configuration revision (IEC 61850-7-2:2010,17.2.2.7) 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 Verify that after a restart of the server, the value of ConfRev is restored to its original value of the base local configuration OR the value is retained from the configuration prior to restart (PIXIT) Verify that the server increments the ConfRev in case the data sets changes due to processing of ACSI services ConfRev should never be 0 (zero) in case DatSet is not null.
sRpt7	Verify that after a restart of the server, the value of ConRev is restored to its original value of the base local configuration OR the value is retained from the configuration prior to restart (PIXIT).

Test case	Test case description
sRpt8	Buffer Time (IEC 61850-7-2:2010,17.2.2.9) 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 BufTm, the server: (IEC 61850-7-2:2010,17.2.2.9) • shall for status information behave as if BufTm has expired and immediately send the report, restart the timer with value BufTm and process the second notification or • may for analogue information behave as if BufTm has expired and immediately transmit the report for transmission, restart the timer with value BufTm 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 should 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 61850-7-2:2010,17.2.2.9) Verify that the BufTm value can contain at least the value 360 0000 (= 1 h in ms)
sRpt9	Verify that the DUT can send reports with data objects
sRpt10	Verify that the DUT can send reports with data attributes
sRpt11	Verify that the DUT can send any buffered events before the integrity report
sRpt12	Verify that when the LLN0 Behavior value is Off or On/Blocked, no data change/quality change reports should be transmitted anymore for the process values in this logical device (IEC 61850-7-4:2010, Annex A)
sRpt13	Verify that the server sets URCB Owner to a non-NULL value when the URCB is configured by a client and reset to NULL when a client releases the URCB
sRpt14	Verify that the DUT can process an URCB with maximum name length for RptID and Dataset (IEC 61850-7-2:2010, 22.2)

6.2.4.10.2 Negative test cases

The test cases listed in Table 11 shall apply.

Table 11 – Unbuffered reporting negative test cases

Test case	Test case description
sRpN1	Request GetURCBValues with wrong parameters and verify response- service error (IEC 61850-7-2:2010,17.2.5.3)
sRpN2	Configure reporting with trigger option GI (not dchg, qchg, dupd, integrity). When enabled, only GI reports are transmitted. No reports should be send when generating events (IEC 61850-7-2:2010,17.2.5.3)
sRpN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2:2010,17.2.2.12)
sRpN4	Incorrect configuration of a URCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set
sRpN5	Exclusive use of URCB and lost association Configure a URCB and set the Resv attribute and enable it. Verify another client cannot set any attribute of that URCB (IEC 61850-7-2:2010,17.2.4.5)
sRpN6	Configure unsupported URCB options (PIXIT); Configure unsupported trigger conditions, optional fields and related parameters
sRpN7	Verify that another client cannot configure a pre-assigned URCB
sRpN8	Verify that when TrgOps – GI is not set, the request to set GI to true shall fail

6.2.4.11 Buffered reporting model

6.2.4.11.1 Positive test cases

The test cases listed in Table 12 shall apply.

Table 12 – Buffered reporting positive test cases

Test case	Test case description
sBr1	Request GetLogicalNodeDirectory(BRCB) and check response Request GetBRCBValues of all responded BRCBs
sBr2	Verify the reporting of optional fields of a BRCB Configure/enable a BRCB with all optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, and/or entryID (IEC 61850-7-2:2010,17.2.3.2.2.1), force/trigger a report and check that the reports contain the enabled optional fields
sBr3	Verify the trigger conditions of a BRCB Configure and enable a BRCB with 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 Verify the validity of the ReasonCode (IEC 61850-7-2:2010,17.2.3.2.2.9) Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2:2010,17.2.3.2.3.2) Verify that reports are only sent when RptEna is set to True (IEC 61850-7-2:2010,17.2.2.5), when reporting is disabled no reports should be transmitted
sBr4	General interrogation (IEC 61850-7-2:2010,17.2.2.13) Setting the GI attribute of a BRCB 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.
sBr5	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 61850-7-2:2010,17.2.3.2.2.5) – SqNum (not changed) – SubSqNum (0 for first report, incrementing, roll-over) – MoreSeqmentsFollow – TimeOfEntry (not changed as SqNum is not altered) (IEC 61850-7-2:2010,17.2.3.2.2.9) 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 61850-7-2:2010,17.2.3.2.3.5) 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 61850-7-2:2010,17.2.3.2.3.4) Verify that when OptFlds=sequence-number is NOT set, neither SubSqNum nor SqNum are present in the sub-reports (17.2.3.2.2.4, 17.2.3.2.2.5).

Test case	Test case description
sBr6	Configuration revision (IEC 61850-7-2:2010,17.2.2.7) 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 Verify that after a restart of the server, the value of ConfRev is restored to its original value of the base local configuration OR the value is retained from the configuration prior to restart (PICS) Verify that the server increments the ConfRev in case the data sets changes due to processing of ACSI services ConfRev should never be 0 (zero) in case DatSet is not null
sBr7	Verify that after a restart of the server, the value of ConRev is restored to its original value of the base local configuration OR the value is retained from the configuration prior to restart (PIXIT).
sBr8	Buffer Time (IEC 61850-7-2:2010,17.2.2.9) 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 BufTm, the server: (IEC 61850-7-2:2010,17.2.2.9) • shall for status information behave as if BufTm has expired and immediately send the report, restart the timer with value BufTm and process the second notification or • may for analogue information behave as if BufTm has expired and immediately transmit the report for transmission, restart the timer with value BufTm 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 should 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 61850-7-2:2010,17.2.2.9) Verify that the BufTm value can contain at least the value 360 0000 (= 1 h in ms)
sBr9	Verify that the DUT can send reports with data objects
sBr10	Verify that the DUT can send reports with data attributes
sBr11	Verify that all buffered events shall be sent before integrity reports can be sent (IEC 61850-7-2:2010,17.2.3.2.3.3)
sBr12	Verify that all buffered events shall be sent before the GI report can be sent (IEC 61850-7-2:2010,17.2.3.2.3.4)
sBr13	Verify that the server sets BRCB Owner to a non-NULL value when the BRCB is configured by a client and reset to NULL when a client releases the BRCB. For at pre-assigned BRCB the server resets the Owner to the pre-assigned client address.
sBr14	Verify that the DUT can process a BRCB with maximum name length for RptID and DatSet (IEC 61850-7-2:2010, 22.2)
sBr20	Buffered reporting (BRCB) state machine (IEC 61850-7-2:2010,17.2.2.5, Figure 24) – Verify that events are buffered after the association is released – Verify that reporting is disabled after the association is lost – Verify that not received reports while not associated are received now in the correct order (SOE) (IEC 61850-7-2:2010,17.2.1, IEC 61850-7-2:2010,17.2.2.5) – Do the same but now set PurgeBuf to True before enabling the reporting. No stored buffered reports should be send (IEC 61850-7-2:2010,17.2.2.14) – Verify that after changing DatSet, the report buffer is purged. (IEC 61850-7-2:2010,17.2.2.5) Force buffer overflow, the OptFlds buffer-overflow should be set in the first report that is sent with events that occurred after the overflow (IEC 61850-7-2:2010,17 2.3.2.2.8)
sBr21	Buffered reporting (BRCB); buffering events (IEC 61850-7-2:2010,17.2.3.2.3.6) Verify that after the association is available again and after the client has set the EntryID, and enabled the BRCB, the BRCB shall start sending the reports of events that have been buffered. The BRCB shall use the sequence and subsequence numbers so that no gaps occur.

Test case	Test case description
sBr22	Verify that integrity reports are buffered
sBr23	Verify successful ResvTms behavior • On ResvTms = –1 the BRCB can be used by the configured client • On ResvTms = 0 a client can reserve the BRCB by writing a value and configure the BRCB • On lost association the reserved BRCB is released after the ResvTms number of seconds (ResvTms set to zero) On lost association, within ResvTms time none of other clients can reserve the BRCB except the one who did it originally (the client restores association)
sBr24	Verify that a SetBRCBValues request, for setting ResvTms, shall: • Generate a negative response if the BRCB's ResvTms value is –1. • Generate a negative response if the BRCB's ResvTms value is non-zero and if the SetBRCBValues request is being issued by another client for whom the BRCB is not reserved. Generate a negative response if the ResvTms value to be set is negative.
sBr25	Verify that a change of one of the following BRCB parameters purges the buffer: RptID, BufTm, TrgOps, IntgPd, DatSet. A change of OptFlds should not purge the buffer. (IEC 61850-7-2:2010,17.2.2.5)
sBr26	Verify that after setting an invalid, null or non-existing EntryID the DUT sends all reports in the buffer
sBr27	Verify that when the BRCB state is RptEna=FALSE a GetBRCBValues shall return the EntryID value that represents the last (newest) entry that has been entered into the buffer. And when the BRCB RptEna=TRUE: The value of EntryID, returned in a GetBRCBValues response, shall be the EntryID of the last EntryID formatted and queued for transmission.
sBr28	Verify that only the last buffered GI report is transmitted after a resync.

6.2.4.11.2 Negative test cases

The test cases listed in Table 13 shall apply.

Table 13 – Buffered reporting negative test cases

Test case	Test case description
sBrN1	Request GetBRCBValues with wrong parameters and verify response- service error (IEC 61850-7-2:2010,17.2.3.3.2)
sBrN2	Configure reporting with trigger option GI (not dchg, qchg, dupd, integrity). When enabled only GI reports are transmitted. No reports should be send when generating events (IEC 61850-7-2:2010,17.2.3.2.2.4)
sBrN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2:2010,17.2.2.11)
sBrN4	Incorrect configuration of a BRCB: configure when enabled, configure ConfRev and SqNum and configure with unknown data set
sBrN5	Exclusive use of BRCB and lost association Configure a BRCB and enable it. Verify another client cannot set attributes value in this BRCB. (IEC 61850-7-2:2010,17.2.1)
sBrN6	Configure unsupported BRCB options (PIXIT); Configure unsupported trigger conditions, optional fields and related parameters
sBrN7	Verify that another client cannot configure a pre-assigned BRCB
sBrN8	Verify that when TrgOps – GI is not set, the device does not send reports with reason code GI

6.2.4.12 Log model

6.2.4.12.1 Positive test cases

The test cases listed in Table 14 shall apply.

Table 14 – Log positive test cases

Test case	Test case description
sLog1	Request GetLogicalNodeDirectory(LOG) and check response+
sLog2	Request GetLogicalNodeDirectory(LCB) and check response+
sLog3	Request GetLCBValues with functional constraint LG of all responded LCBs
sLog4	Request SetLCBValues with functional constraint LG when LCB is disabled
sLog5	Verify that logging is independent of a limited set of external application associations or other communication transactions
sLog6	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
sLog7	Request QueryLogByTime and check response+
sLog8	Request QueryLogAfter and check response+
sLog9	Request GetLogStatusValues and check response+, verify that the responded entries indicate the oldest/newest entry ID/time available in the log
sLog10	Check that data is logged as defined in the settings of logical node GLOG. The corresponding reason code shall be "application-trigger"
sLog11	Verify that server can process a LCB and LOG with maximum name length for LCBRef, LogRef and DatSet (IEC 61850-7-2:2010, 22.2)
sLog12	Verify that log entries are volatile and not lost after reboot and power loss.

6.2.4.12.2 Negative test cases

The test cases listed in Table 15 shall apply.

Table 15 – Log negative test cases

Test case	Test case description
sLogN1	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 61850-7-2:2010,17.3.2.5) – SetLCBValues (IEC 61850-7-2:2010,17.3.2.6) – QueryLogByTime (IEC 61850-7-2:2010,17.3.5.2) – QueryLogAfter (IEC 61850-7-2:2010,17.3.5.3) – GetLogStatusValues (IEC 61850-7-2:2010,17.3.5.4)
sLogN2	Request SetLCBValues with functional constraint LG when LCB is enabled and verify response-service error

6.2.4.13 Control models

6.2.4.13.1 General

Testing of the control models has been divided in a general test and a list of test cases for the specific control models. The general test cases are as follows.

6.2.4.13.2 Control model general test cases

The test cases listed in Table 16 shall apply.

Table 16 – Control model test cases

Test case	Test case description
sCtl1	Force and check each path in control state machine for several control objects with control models • direct with normal security (IEC 61850-7-2:2010, 20.2.1) • SBO-control with normal security (IEC 61850-7-2:2010, 20.2.2) • direct with enhanced security (IEC 61850-7-2:2010, 20.3.2) • SBO-control with enhanced security (IEC 61850-7-2:2010, 20.3.3) Compare detailed test cases for each control model
sCtl2	Change control model using online services and verify that the control object responds according to the new control model
sCtl3	Time Operate a second enhanced security control object before the activation time of the first control object (PIXIT)
sCtl4	Verify that the stSeld attribute value is set/reset as specified in the state machines
sCtl5	Verify test flag in selectwithvalue/operate and Beh = test (IEC 61850-7-4:2010, Annex A ,Table A.1) • When LN Beh is "on", the control Requests are rejected with AddCause "Blocked-by-mode" • When LN Beh is “test/blocked”, the control requests are accepted • When LN Beh is "test", the control requests are accepted
sCtl6	Select all SBO control objects and cancel them in opposite order. In case a control action is blocked because another control is already running, the AddCause shall be "1-of-n-control"
sCtl7	Verify that with interlock or synchrocheck conditions the specified checks are performed and the command is executed accordingly (IEC 61850-7-2:2010, 20.5.2.7) • When the interlock check fails with AddCause "Blocked-by-interlocking" • When the interlock check passes • When the synchro check fails with AddCause "Blocked-by-synchrocheck" • When the synchro check passes
sCtl8	Operate (without select) a SBO control object and verify that the request is rejected with AddCause "Object-not-selected" (IEC 61850-7-2:2010, Table 54)
sCtl9	Select the same control object twice, verify that the second select request is rejected with AddCause "Object-already-selected" (IEC 61850-7-2:2010, Table 54) and the object remains in selected state (Operate.req is accepted)
sCtl10	Operate control value is the same as the actual status value (On-On or Off-Off) and verify that the control request is rejected with AddCause "Position-reached" (IEC 61850-7-2:2010, Table 54, PIXIT)
sCtl11	Select the same control object from 2 different clients. Verify that the control requests from the second client are rejected with AddCause "Locked-by-other-client" (IEC 61850-7-2:2010, Table 54)
sCtl12	Select/Operate an unknown control object and verify that the control requests are rejected with AddCause "Unknown" (IEC 61850-7-2:2010, Table 54)
sCtl13	Verify that the Select request on a direct operate control object is rejected with Addcause "Unknown" (IEC 61850-7-2:2010, Table 54)
sCtl14	Operate the same direct control object twice from 2 clients (IEC 61850-7-2:2010, Table 54, PIXIT) and verify that the last control request is rejected with AddCause "Command-already-in-execution"
sCtl15	Verify that the SBOes Operate or Cancel request with different control parameters than the SelectWithValue is rejected with AddCause: Inconsistent-parameters"

Test case	Test case description
sCtl16	Verify that when Loc is set remote control requests are rejected with AddCause "Blocked-by-switching-hierarchy"
sCtl17	Verify that with plant level authority (LocSta=T) remote control requests are rejected with AddCause "Blocked-by-switching-hierarchy"
sCtl18	Verify that on CmdBlk.stVal is set the control requests are rejected with AddCause "Blocked-by-command" (IEC 61850-7-2:2010, Table 54)
sCtl19	Verify that when the blkEna is set the control requests are terminated/rejected with AddCause "Time-limit-over"
sCtl20	Verify that when parameters are changed after the select respond, the operate request is rejected with AddCause "Parameter-change-in-execution" (IEC 61850-7-2:2010, Table 54)
sCtl21	Verify that when tap changer has reached the limit (EndPosR or EndPosL in YLTC) control requests are rejected with AddCause "Step-limit" (IEC 61850-7-2:2010, Table 54)
sCtl22	Verify that with insufficient access authority control requests are rejected with AddCause "No-access-authority" (IEC 61850-7-2:2010, Table 54)
sCtl23	Verify that when a APC control action end position has overshoot the command terminates with AddCause "Ended-with-overshoot" (IEC 61850-7-2:2010, Table 47)
sCtl24	Verify that when a APC control action is aborted due to deviation between the command value and the measured value the control terminates with AddCause "Abortion-due-to-deviation" (IEC 61850-7-2:2010, Table 47)
sCtl25	Verify that a cancel request is successful when the control object is in the unselected state (IEC 61850-7-2:2010, Table 47)
sCtl26	Verify that when the control object is in the WaitForExecution state the cancel or SelectWithValue request is rejected with AddCause "Command-already-in-execution" (IEC 61850-7-2:2010,Table 54)
sCtl27	Verify that the SelectWithValue request on a SBOns control object is rejected with Addcause "Unknown" (IEC 61850-7-2:2010, Table 54)
sCtl28	Verify that the DUT can control an object with maximum name length for IED and Logical Device (IEC 61850-7-2:2010,22.2)

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

a) Direct control with normal security (DOns),

b) SBO control with normal security (SBOns),

c) Direct control with enhanced security (DOes),

d) SBO control with enhanced security (SBOes).

6.2.4.13.3 Control model specific test cases

The test cases listed in Table 17, Table 18, Table 19 and Table 20 shall apply.

Table 17 – DOns test cases

Test case	Test case description
sDOns1	Send a correct Operate request
sDOns2	Send an Operate request, resulting in “Test not ok”
sDOns3	Send an TimeActivatedOperate request, resulting in respond-
sDOns4	Send a correct TimeActivatedOperate request Verify the TimeActivatedOperateTermination+
sDOns5	Send a TimeActivatedOperate request, Verify that each of these paths will return the device to the Ready state and verify the TimeActivatedOperateTermination-: – Force a “Test not ok” – Send a correct Cancel request

Table 18 – SBOns test cases

Test case	Test case description
sSBOns1	Send a correct Select request Send a correct Operate request
sSBOns2	Send a correct Select request Verify that each of these paths will return the device to the Unselected state: – Send a correct Cancel request – Wait for timeout – Association lost – Send a Release request – Send an Operate request resulting in “Test not ok”
sSBOns3	Send a correct Select request – Send an incorrect TimeActivatedOperate request resulting in respond-
sSBOns4	Send a correct Select request Send a correct TimeActivatedOperate request, thereby making sure the device will generate a 'test Ok'. Verify the TimeActivatedOperateTermination+
sSBOns5	Send a correct Select request Send a correct TimeActivatedOperate request. Verify that each of these paths will return the device to Ready state and the TimeActivatedOperateTermination-: – Force a test “Test not ok” – Send a correct Cancel request
sSBOns6	Send a correct Select request resulting in respond- Verify that each of the device returns to the Unselected state:
sSBOns7	Send a correct Select request Verify that sending multiple Operate Many requests will return the device to Ready state Verify that sending a Cancel request will return the device to the Unselected state

Table 19 – DOes test cases

Test case	Test case description
sDOes1	Send a correct Operate request Verify that each of these paths will return the device to the Ready state and verify the CommandTermination: – force the equipment simulator to move to the requested new state – force the equipment simulator to keep the old state (AddCause: Time-limit-over or Invalid-position) – force the equipment simulator to move to the 'between' state (AddCause: Invalid-position)
sDOes2	Send an Operate request, thereby making sure the device will generate a 'Test not Ok'.
sDOes3	Send a TimeActivated Operate request, resulting in respond-
sDOes4	Send a correct TimeActivated Operate request Verify the TimeActivatedOperateTermination+ Verify that each of these paths will return the device to the Ready state and verify the CommandTermination: – force the equipment simulator to move to the requested new state – force the equipment simulator to keep the old state (AddCause: Time-limit-over) – force the equipment simulator to move to the 'between' state (AddCause: Invalid-position)
sDOes5	Send a correct TimeActivated Operate request Verify the TimeActivatedOperateTermination+ Verify that each of these paths will return the device to the Ready state and verify the TimeActivatedOperateTermination: – Force a “Test not ok” – Send a correct Cancel request

Table 20 – SBOes test cases

Test case	Test case description
sSBOes1	Send a correct SelectWithValue and Operate request Verify that each of these paths will return the device to the Unselected state Verify the command termination: – force the equipment simulator to move to the requested new state – force the equipment simulator to keep the old state (AddCause: Time-limit-over or Invalid-position) – force the equipment simulator to move to the 'between' state (AddCause: Invalid-position) –
sSBOes2	Send a correct SelectWithValue request Verify that each of these paths will return the device to the Unselected state: – Send a correct Cancel request – Client waits for select timeout – Send a Release request – Send an Operate request resulting in “Test not ok”
sSBOes3	Send a correct SelectWithValue and TimeActivatedOperate request, resulting in respond-
sSBOes4	Send a correct SelectWithValue request Send a correct TimeActivatedOperate Once request Verify the TimeActivatedOperateTermination+ Verify that each of these paths will return the device to the Unselected state and verify the CommandTermination: – force the equipment simulator to move to the requested new state – force the equipment simulator to keep the old state (AddCause:Time-limit-over or Invalid-position) – force the equipment simulator to move to the 'between' state (AddCause: Invalid-position)
sSBOes5	Send a correct SelectWithValue request Send a correct TimeActivatedOperate request Verify that each of these paths will return the device to the Ready state: – Force a test “Test not ok” – Send a correct Cancel request
sSBOes6	Select device using SelectWithValue with improper access rights. Access should be denied (IEC 61850-7-2:2010,20.2.2) or send an incorrect SelectWithValue request
sSBOes7	Send a correct SelectWithValue request Verify that sending multiple Operate Many requests will return the device to Ready state Verify that sending a Cancel request will return the device to the Unselected state
sSBOes8	Verify that the Operate or Cancel request with different control parameters than the SelectWithValue is rejected with AddCause: Inconsistent-parameters

6.2.4.14 Time and time synchronisation model

6.2.4.14.1 General

The time and time synchronization test cases defined for a server device are as follows.

6.2.4.14.2 Positive test cases

The test cases listed in Table 21 shall apply.

Table 21 – Time positive test cases

Test case	Test case description
sTm1	Verify that the DUT supports and executes the SCSM time synchronisation
sTm2	Check report/logging timestamp accuracy matches the documented timestamp quality of the server
sTm3	Verify that when the device supports time zones and daylight saving the time stamp of events and disturbance files are UTC time
sTm4	Verify the time management settings in logical node LTIM
sTm5	Verify the time master supervision in logical node LTMS

6.2.4.14.3 Negative test cases

The test case listed in Table 22 shall apply.

Table 22 – Time negative test cases

Test case	Test case description
sTmN1	Verify that when time synchronisation communication lost is detected after a time period specified by the test facility.
sTmN2	On synchronisation error, deviation beyond time stamp tolerance should be detected

6.2.5 Test cases to test a client device

6.2.5.1 General

This part of the IEC 61400-25-5 specifies abstract test cases for testing the compliance of a IEC 61400-25 client. The abstract test cases shall be used for the definition of test procedures to run in tests.

The difference to the specifications given in the IEC 61850-10 is the wind power information model and the wind power specific mappings. The specific IEC 61400-25-2 data classes are not tested. The IEC 61400-25-4 mapping particularities are not described in the IEC 61400-25-5 abstract level.

The SCSM specific test procedures shall be provided by test facilities agreed upon by the market participants.

6.2.5.2 Test system architecture to test a client device

In order to be able to perform a client device test, a minimum test set-up is necessary. The test architecture contains (see Figure 5):

– DUT with optional HMI;
– multi server simulator to respond to TPAA messages from the DUT;
– test master to start/stop test cases, start/stop the analyse and archive test results;
– time master;
– engineering tool to configure the DUT;
– a protocol analyser to store all the network traffic for each test case.

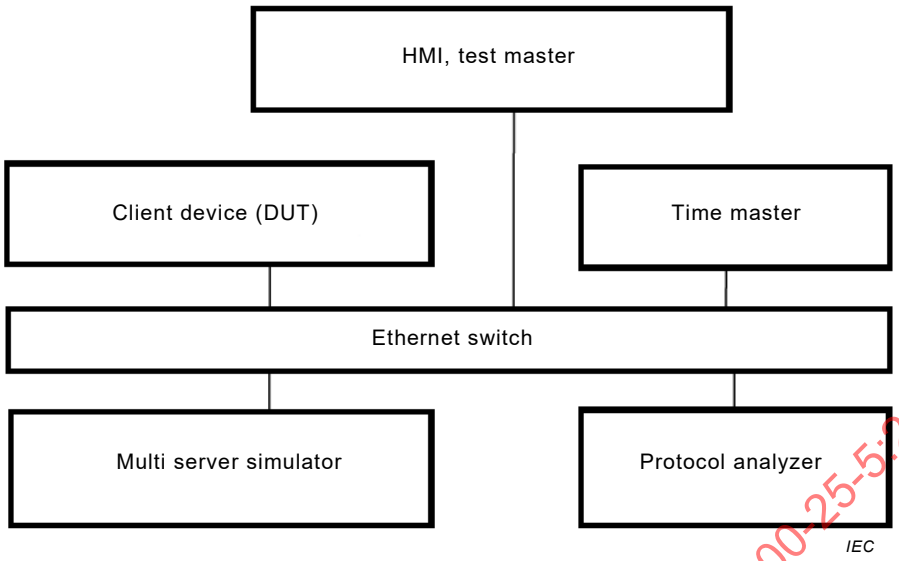


Figure 5 – Test system architecture to test a client device

The test system shall include documentation regarding test system hardware and test system software.

6.2.5.3 Documentation and version control test procedure overview

The test case listed in Table 23 shall apply.

Table 23 – Client documentation test case

Test case	Test case description
cDoc1	Check if the major/minor software version in the PICS documentation and the DUT do match (IEC 61850-4)
cDoc2	Check if the major/minor software version manufacturer PIXIT documentation and software version of the DUT do match (IEC 61850-4). PIXIT shall indicate the required information as requested in the test cases
cDoc3	Check if the major/minor software version manufacturer MICS documentation and software version of the DUT do match (IEC 61850-4). MICS shall indicate which CDCs and/or CDC parts are supported by the DUT, for example arrays
cDoc4	Check if the major/minor software version in the TICS documentation and the software version of the DUT do match (IEC 61850-4). TICS shall indicate the supported technical issues.

6.2.5.4 Data model test cases

The test case listed in Table 24 shall apply.

Table 24 – Client data model test case

Test case	Test case description
cMdl1	Verify that the client can handle the maximum name length according to IEC 61400-25-2 and SCSM expands objects like SDOs correctly (PIXIT)
cMdl2	Verify that DUT supports the following naming conventions for the supported control blocks a) unbuffered report control block – not indexed b) unbuffered report control block – indexed c) buffered report control blocks d) Log control block
cMdl3	Verify that DUT can read and process the mandatory and optional attributes from the CDCs in IEC 61400-25 unless stated otherwise in the MICS

6.2.5.5 Mapping of ACSI models and services test cases

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

– Application association (cAss);
– Server, Logical device, Logical node, Data, and Data Attribute model (cSrv);
– Data set model (cDs);
– Unbuffered report control model (cRp);
– Buffered report control model (cBr);
– Log control model (cLog);
– Control model (cCtl);
– Time and time synchronisation model (cTm).

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 61850-7-2:2010, Annex A. The test result interpretation (passed/failed) depends on the declared capabilities.

6.2.5.6 Application association model

6.2.5.6.1 Positive test case

The test cases listed in Table 25 shall apply.

Table 25 – Association positive test cases

Test case	Test case description
cAss1	Associate and force the DUT to release or abort a TPAA association (IEC 61850-7-2:2010,8.3)
cAss2	Force the DUT to associate with maximum number of servers simultaneously (PIXIT)
cAss3	Verify that the DUT restores the association after the association of one server is lost and that this has no effect on the other active associations of the other servers

6.2.5.6.2 Negative test case

The test cases listed in Table 26 shall apply.

Table 26 – Association negative test cases

Test case	Test case description
cAssN1	Associate and server responds with negative answer due to AccessPointReference.
cAssN2	Associate and server responds with negative answer due to AuthenticationParameter.
cAssN3	Associate and server releases TPAA association (IEC 61850-7-2:2010,8.3). DUT should try to re-establish the association after the configured period (PIXIT).
cAssN4	Associate and server-abort TPAA association (IEC 61850-7-2:2010,8.3). DUT should try to re-establish the association after the configured period (PIXIT).
cAssN5	Associate and server denies TPAA association (IEC 61850-7-2:2010,8.3) DUT should try to re-establish the association after the configured period (PIXIT).
cAssN6	Disconnect the communication interface between server and the Ethernet switch such that the link between DUT and the Ethernet switch stays active. 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.
cAssN7	Interrupt and restore the power supply, the DUT shall establish the configured associations when ready (PIXIT).

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

6.2.5.7.1 Positive test cases

The test cases listed in Table 27 shall apply.

Table 27 – Server positive test cases

Test case	Test case description
cSrv1	If the DUT implements Autodescription (See Note 1), force the DUT to start the autodescription and check that the DUT requests a GetServerDirectory (LOGICAL-DEVICE) to all the logical devices of the configured servers (See Note 2) (IEC 61850-7-2:2010,7.2.2)
cSrv2	If DUT implements Autodescription, for each GetServerDirectory (LOGICAL-DEVICE) response, check that the DUT issues a GetLogicalDeviceDirectory request (IEC 61850-7-2:2010,9.2.1)
cSrv3	If DUT "implements Autodescription", for each GetLogicalDeviceDirectory response issue, check that the DUT issues a GetLogicalNodeDirectory(DATA) request (IEC 61850-7-2:2010,10.2.2)
cSrv4	If the DUT "implements Autodescription", for a subset of the GetLogicalNodeDirectory(DATA) response, check that the DUT issues at least one of the following services: – GetDataDirectory request and check response (IEC 61850-7-2:2010,11.4.4), – GetDataDefinition request and check response (IEC 61850-7-2:2010,11.4.5).
cSrv5	Verify that after startup, the DUT is able to update the process values of the configured servers (PIXIT).
cSrv6	Request a SetDataValues of the different basic types (with e.g. FC=CF) and check the services (IEC 61400-25-3).
cSrv7	Request a GetDataValues and check if the DUT updates its model
cSrv8	Request GetAllDataValues for the required functional constraint and check if the DUT updates its model (IEC 61850-7-2:2010,10.2.3).
cSrv9	Verify that the DUT is able to set/reset blkEna (IEC 61850-7-3:2010,6.2.6)
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 DUT is configured to communicated with. The DUT at least needs to know the parameters to establish an association with them.	

6.2.5.7.2 Negative test cases

The test cases listed in Table 28 shall apply.

Table 28 – Server negative test cases

Test case	Test case description
cSrvN1	If the DUT implements Autodescription, force the SUT to start the autodescription and check that the DUT still communicates with other servers when it requests the following services with negative response: a) GetServerDirectory(LOGICAL-DEVICE), b) GetLogicalDeviceDirectory, c) GetLogicalNodeDirectory(DATA), d) GetDataDirectory, e) GetDataDefinition.
cSrvN2	Check that the DUT is able to communicate with other connected servers after a request for GetAllDataValues fails in the following circumstances: a) The response is negative. b) The response comes with mismatching data objects.
cSrvN3	Check that the DUT is able to communicate with other connected servers after a request for GetDataValues fails in the following circumstances: a) The response is negative. b) The response comes with mismatching data objects. c) The value is out of the valid range for this data.
cSrvN4	Check that the DUT is able to communicate with other connected servers after a request for SetDataValues fails in the following circumstances: a) The response is negative. b) One of the data values is read-only.
cSrvN5	If the DUT 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 DUT and check the behaviour described in the PIXIT.
cSrvN6	If the DUT 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 DUT and check the behaviour described in the PIXIT.

6.2.5.8 DataSet model

6.2.5.8.1 Positive test cases

The test cases listed in Table 29 shall apply.

Table 29 – Data set positive test cases

Test case	Test case description
cDs1	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogicalNodeDirectory(DATASET) of the Logical Nodes of the configured servers (IEC 61850-7-2:2010,10.2.2)
cDs2	If the DUT implements Autodescription, force it to start autodescription and check it requests a GetDataSetDirectory of all the DataSets of the server (IEC 61850-7-2:2010,13.3.6)
cDs3	Check that the DUT can request a GetDataSetValues and handle the respond (IEC 61850-7-2:2010,13.3.2)
cDs4	Check that the DUT can request a SetDataSetValues and handle the respond (IEC 61850-7-2:2010, 13.3.3)
cDs5	Verify that the DUT checks the pre-configured datasets in the SCD file. If any deviation is detected the DUT behaves as specified in the PIXIT
cDs6	If the DUT creates persistent / non-persistent datasets dynamically after starting up check that the DUT sends the CreateDataSet services according to configuration. PIXIT (IEC 61850-7-2:2010,13.3.4)
cDs7	Request a DeleteDataSet service and check that the DUT sends the request properly and is able to process the response of the server (IEC 61850-7-2:2010,13.3.5)
cDs8	Verify that a persistent data set can be handled with the maximum name length for data set and a data set member (IEC 61850-7-2:2010, 22.2)
cDs9	Verify that a non-persistent data set can be handled with the maximum name length for data set and a data set member (IEC 61850-7-2:2010, 22.2)

6.2.5.8.2 Negative test cases

The test cases listed in Table 30 shall apply.

Table 30 – Data set negative test cases

Test case	Test case description
cDsN1	If the DUT implements Autodescription, force the DUT to start the Autodescription and check that the DUT still communicates with other servers when it request the following services with negative response: a) GetLogicalNodeDirectory (DATA-SET), b) GetDataSetDirectory.
cDsN2	Check that the DUT still communicates with other servers properly when it requests a GetDataSetValue to one of them and the following situations happen: a) the response is negative, b) the response comes with more/less elements than expected, c) the response comes with reordered elements of different types, d) the response comes with reordered elements of the same type.
cDsN3	Check that the DUT still communicates with other servers properly when it requests a SetDataSetValue to one of them and the response is negative.
cDsN4	If the DUT creates persistent/non-persistent datasets dynamically after starting up check that the DUT still communicates with other servers when it requests a CreateDataSet with negative response
cDsN5	If the DUT configures the datasets dynamically after starting up check that the DUT still communicates with other servers when it requests a DeleteDataSet with negative response

6.2.5.9 Substitution model – Test cases

The test cases listed in Table 31 shall apply.

Table 31 – Substitution test cases

Test case	Test case description
cSub1	Verify that the DUT can enable substitution, enter a substituted value and disable substitution
cSub2	Verify that the DUT can display the source “substituted” for substituted values
cSub3	Verify that the DUT can display the source “substituted” for values substituted by another client
cSub4	Verify that the DUT can handle the maximum name length for substitution values (IEC 61850-7-2:2010,22.2)

6.2.5.10 Unbuffered reporting model

6.2.5.10.1 Positive test cases

The test cases listed in Table 32 shall apply.

Table 32 – Unbuffered reporting positive test cases

Test case	Test case description
cRp1	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogicalNodeDirectory(URCB) of the logical nodes declared in the PIXIT of all configured servers
cRp2	If the DUT configures the server’s Unbuffered ReportControlBlock parameters after startup using SetURCBValues, check that the SetURCBValues are sent with the configured values (IEC 61850-7-2:2010,17.2.5.4)
cRp3	Verify that the DUT is able to process the reports with different optional fields: Force the DUT to configure/enable a URCB with useful optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name and/or data-reference (IEC 61850-7-2:2010,17.2.2.4), force/trigger a report and check that the DUT is able to process the reports and updates its database.
cRp4	Verify that the DUT is able to process the reports with different trigger conditions (IEC 61850-7-2:2010,17.2.2.4): Configure and enable a URCB with all supported optional fields and check that the reports are transmitted according to the following (supported) trigger conditions: a) on integrity b) on update (dupd) c) on update with integrity d) on data change (dchg) e) on data change and quality change (dchg, qchg) f) on data change and quality change with integrity period (dchg, qchg)
cRp5	Verify that the DUT is able to process segmented reports
cRp6	Verify that the DUT can change the (pre-) configured Buffer Time (IEC 61850-7-2:2010,17.2.2.9)
cRp7	Verify that the DUT can force a General interrogation (IEC 61850-7-2:2010,17.2.2.13)
cRp8	Verify that after startup the DUT configures and enables the URCB’s as specified in the SCD file
cRp9	Verify that the DUT can handle reporting of complex structured data (for example WYE and DEL data objects)
cRp10	Verify that the DUT can handle reporting of basic data (for example stVal and quality)
cRp11	Verify that the DUT can handle a URCB, RptID and DatSet with maximum name length (IEC 61850-7-2:2010,22.2)
cRp12	Verify that the DUT can change the dataset elements of a dynamic dataset previously used in a URCB resulting in a ConfRev increment by the server
cRp13	Verify that the DUT configures another indexed URCB when another DUT has reserved the indexed URCB before

6.2.5.10.2 Negative test cases

The test cases listed in Table 33 shall apply.

Table 33 – Unbuffered reporting negative test cases

Test case	Test case description
cRpN1	If the DUT implements Autodescription, force the DUT to start the Autodescription and check that the DUT still communicates with other servers when it requests GetLogicalNodeDirectory (URCB) with negative response.
cRpN2	Check that the DUT still works properly when it requests a GetURCBValues when the response is negative.
cRpN3	Check that the DUT still works properly when it requests a SetURCBValues when the response is negative.
cRpN4	Check that the DUT still works properly when it requests a SetURCBValues and the URCB is reserved (Resv=TRUE, PIXIT).
cRpN5	Report with not supported OptFlds. Check that the DUT does not collapse if it receives a Report with a non-configured or non-supported OptFlds.
cRpN6	Report with not supported TrgOps. Check that the DUT does not collapse if it receives a Report with a non-configured or non-supported Trigger Option.
cRpN7	Mismatching reports: a) Report with unknown DataSet b) Report with unknown RptId c) Report with incorrect references of the Data d) Report with incorrect types in the Data Check the behaviour described in the PIXIT.
cRpN8	Verify that the DUT detects a change in the ConfRev attribute (Configuration revision, IEC 61850-7-2:2010,14.2.2.7) of the Report Control Block. When the DUT does not perform the ConfRev check it should check the dataset elements. The means of detection needs to be specified in the PIXIT.

6.2.5.11 Buffered reporting model

6.2.5.11.1 Positive test cases

The test cases listed in Table 34 shall apply.

Table 34 – Buffered reporting positive test cases

Test case	Test case description
cBr1	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogicalNodeDirectory(BRCB) of the logical nodes declared in the PIXIT of all configured servers
cBr2	If the DUT configures the server's Buffered ReportControlBlock parameters after startup using SetBRCBValues, check that the GetBRCBValues/SetBRCBValues are sent with the configured values (IEC 61850-7-2:2010,17.2.3.4)
cBr3	Verify that the DUT is able to process the reports with different optional fields: Force the DUT to configure/enable a BRCB with the useful optional fields combinations: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, entryID and conf-version, force/trigger a report and check that the DUT is able to process the reports and updates its database (IEC 61850-7-2:2010,17.2.2.8)
cBr4	Verify that the DUT is able to process the reports with different trigger conditions (IEC 61850-7-2:2010,17.2.2.11) Configure and enable a BRCB with all useful optional fields: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow, entryID and conf-revision and check that the reports are transmitted according to the following (supported) trigger conditions: a) on integrity b) on update (dupd) c) on update with integrity d) on data change (dchg) e) on data and quality change (dchg, qch) f) on data and quality change with integrity period (dchg, qchg)
cBr5	Verify that the DUT is able to process segmented reports
cBr6	Verify that the DUT can change the (pre-) configured Buffer Time (IEC 61850-7-2:2010,17.2.2.9)
cBr7	Verify that the DUT can force a General interrogation (IEC 61850-7-2:2010,17.2.2.13)
cBr8	Verify that after startup the DUT configures and enables the BRCBs as configured in the SCD file (and actually used).
cBr9	Verify that the DUT can handle reporting of complex structured data (for example WYE and DEL data objects)
cBr10	Verify that the DUT can handle reporting of basic data (for example stVal and quality)
cBr11	Verify that the DUT can handle a BRCB, RptID and DatSet with maximum name length (IEC 61850-7-2:2010,22.2)
cBr12	Verify that the DUT can change the dataset elements of a dynamic dataset previously used in a BRCB resulting in a ConfRev increment by the server
cBr13	Verify that the DUT configures another indexed BRCB when another client has reserved the indexed BRCB before.
cBr14	Verify that the DUT is able to process reports buffered during an lost association a) without bufferoverflow (PIXIT) b) with bufferoverflow
cBr15	Verify that the DUT is able to request specific buffered reports after restoring a lost association by setting the EntryID
cBr16	Verify that the DUT is able to purge buffered reports
cBr17	Verify that the DUT first sets the ResvTms attribute if this attribute is available and has value 0

6.2.5.11.2 Negative test cases

The test cases listed in Table 35 shall apply.

Table 35 – Buffered reporting negative test cases

Test case	Test case description
cBrN1	If the DUT implements Autodescription, force the DUT to start the Autodescription and check that the DUT still communicates with other servers when it requests GetLogicalNodeDirectory (BRCB) with negative response.
cBrN2	Check that the DUT still works properly when it requests a GetBRCBValues when the response is negative.
cBrN3	Check that the DUT still works properly when it requests a SetBRCBValues when the response is negative.
cBrN4	Check that the DUT still works properly when it requests a SetBRCBValues and the BRCB is used by or pre-assigned to another DUT (PIXIT).
cBrN5	Report with not supported OptFlds. Check that the DUT does not collapse if it receives a Report with a non-configured or non-supported OptFlds.
cBrN6	Report with not supported TrgOps. Check that the DUT does not collapse if it receives a Report with a non-configured or non-supported Trigger Option.
cBrN7	Mismatching reports: a) Report with unknown DataSet. b) Report with unknown RptID c) Report with incorrect references of the Data (when data references are enabled) d) Report with incorrect types in the Data Check the behaviour described in the PIXIT.
cBrN8	Verify that the DUT detects a change in the ConfRev attribute (Configuration revision, IEC 61850-7-2:2010,17.2.2.7) of the Report Control Block. When the DUT does not perform the ConfRev check it should check the dataset elements. The means of detection needs to be specified in the PIXIT.
cBrN9	Verify that the DUT can handle a severe buffer overflow with SetBRBValues(EntryID) response-

6.2.5.12 Log model

6.2.5.12.1 Positive test cases

The test cases listed in Table 36 shall apply.

Table 36 – Log positive test cases

Test case	Test case description
cLog1	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogicalNodeDirectory (LOG) of all the logical nodes of all configured servers
cLog2	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogicalNodeDirectory(LCB) of all the logical nodes of all configured servers
cLog3	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLogStatusValues of all the LOGs found with the GetLogicalNodeDirectory(LCB) services
cLog4	If the DUT implements Autodescription, force it to start Autodescription and check if it requests a GetLCBValues of all the LCBs found with the GetLogicalNodeDirectory(LCB) services (IEC 61850-7-2:2010,17.3.2.5)
cLog5	If the DUT configures the server's LogControlBlock parameters after startup using SetLCBValues, check that the GetLCBValues/SetLCBValues are sent with the configured values (IEC 61850-7-2:2010,17.3.2.6)
cLog6	Force the DUT to enable the Logging of at least one LOG of the server and check that the DUT sent the request correctly
cLog7	Force the DUT to QueryLogByTime and check that the DUT updates its database with the Log entries received (IEC 61850-7-2:2010,17.3.5)
cLog8	Verify that the DUT can handle a LCB and DatSet with maximum name length (IEC 61850-7-2:2010,22.2)

6.2.5.12.2 Negative test cases

The test cases listed in Table 37 shall apply.

Table 37 – Log negative test cases

Test case	Test case description
cLogN1	If the DUT implements Autodescription, force the DUT to start the Autodescription and check that the DUT still communicates with other servers when it requests GetLogicalNodeDirectory (LCB) and GetLogicalNodeDirectory (LOG) with negative response.
cLogN2	Check that the DUT still works properly when it requests a GetLCBValues/GetLogStatusValues when the response is negative.
cLogN3	Check that the DUT still works properly when it requests a SetLCBValues when the response is negative.

6.2.5.13 Control model

6.2.5.13.1 General

Testing of the control models has been divided in a list of general test cases and a list of test cases for the specific control models. The general test cases are as follows.

6.2.5.13.2 Positive test cases

The test cases listed in Table 38 shall apply.

Table 38 – Control model positive test cases

Test case	Test case description
cCtl1	Check if the DUT is able to set the TEST field in the SelectWithValue and Operate requests (PIXIT).
cCtl2	Check if the DUT is able to set the CHECK (Synchro-Check or Interlock-Check bits) in the commands (PIXIT) for the supported control models.
cCtl3	Check if the DUT is able to change control model using online services (PIXIT).
cCtl4	Verify the values of originator category and identification and the control number values (PIXIT).

6.2.5.13.3 Negative test cases

The test cases listed in Table 39 shall apply.

Table 39 – Control model negative test cases

Test case	Test case description
cCtlN1	Check if the DUT reacts in a proper way when its detects a control model mismatch (PIXIT): a) Server status-only – DUT expects controllable b) Server SBO – DUT expects direct operate c) Server direct operate – DUT expects

6.2.5.13.4 Control model specific test cases

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

a) SBO control with enhanced security (SBOes),
b) SBO control with normal security (SBOns),
c) Direct control with enhanced security (DOes),
d) Direct control with normal security(DOns),

The test cases listed in Table 40, Table 41, Table 42 and Table 43 shall apply.

Table 40 – SBOes test cases

Test case	Test case description
cSBOes1	SelectWithValue [test not ok] resp-: Select device using SelectWithValue resulting in test not ok. Check that the DUT indicates an error.
cSBOes2	SelectWithValue [test ok] resp+ and OperReq[test ok] resp+ of selected object Select device using correct SelectWithValue. Perform a correct Operate request. Check that the DUT indicates no error after receiving the command termination+
cSBOes3	SelectWithValue [test ok] resp+ and OperReq[test not ok] resp- of selected object. Perform a SelectWithValues and Operate request. The Operate results in test not ok. Check that the DUT realizes the operation failed.
cSBOes4	SelectWithValue [test ok] resp+ and CancelReq of selected object. Perform a correct Cancel request. Check that the DUT indicates no error.
cSBOes5	SelectWithValue [test ok] resp+ and TimOperReq[test ok] resp+ of selected object Perform a correct TimOperate request. Check that the DUT realizes the operation succeeded after the WaitForActionTime and detects the CommandTermination with the result of the order.
cSBOes6	SelectWithValue [test ok] resp+ and TimOperReq[test ok] resp- of selected object Perform a SelectWithValue and TimOperate request. The TimeOperate results in test not ok. Check that the DUT realizes the operation failed.

Table 41 – SBOns test cases

Test case	Test case description
cSBOns1	SelectReq[test not ok] resp-: DUT requests Select resulting in Test not ok. Check that the DUT realizes the select failed (PIXIT).
cSBOns2	SelectReq[test ok] resp+ and OperReq[test ok] resp+ of selected object. Select a controllable object using Select. Perform a correct Operate request. Check that the DUT does not generate an error.
cSBOns3	SelectReq[test ok] resp+ and OperReq[test not ok] resp- of selected object. Perform a correct Operate request resulting in Test not ok. Check that the DUT realizes the operation failed.
cSBOns4	SelectReq[test ok] resp+ and CancelReq of selected object. Perform a correct cancel request.
cSBOns5	SelectReq[test ok] resp+ and TimOperReq[test ok] resp+ of selected object. Perform a correct TimOperate request. Check that the DUT realizes the operation succeeded after the WaitForActionTime.
cSBOns6	SelectReq[test ok] resp+ and TimOperReq[test not ok] resp- of selected object. Perform a correct TimOperate request resulting in test not ok. Check that the DUT realizes the operation failed.

Table 42 – DOes test cases

Test case	Test case description
cDOes1	OperReq[test ok] resp+: Send a correct Operate request. a) Check that the DUT notice the operation ended positively when it receives the CommandTermination+. b) Check that the DUT notice the operation ended negatively when it receives the CommandTermination- (PIXIT)
cDOes2	OperReq[test not ok] resp-: Send an Operate request, thereby making sure the device will generate a 'test not Ok'. Check that the DUT realizes the operation failed (PIXIT)
cDOes3	TimOperReq[test not ok] resp-: Send a TimeActivated Operate request, thereby making sure the device will generate a 'test not Ok'. Check that the DUT realizes the operation failed.
cDOes4	TimOperReq[test ok] resp+: Send a correct TimeActivated Operate request. a) Check that the DUT realizes the operation request succeeded. b) Check that the DUT notice the operation ended positively when it receives the CommandTermination+. c) Check that the DUT notice the operation ended negatively when it receives the CommandTermination-.

Table 43 – DOns test cases

Test case	Test case description
cDOns1	OperReq[test ok] resp+ Perform a correct Operate request. Check that the DUT does not generate an error.
cDOns2	OperReq[test not ok] resp- DUT requests Oper resulting in Test not ok. Check that the DUT realizes the operation failed.
cDOns3	TimOperReq[test not ok] resp- DUT requests TimOper resulting in Test not ok. Check that the DUT realizes the time operation failed.
cDOns4	TimOperReq[test ok] + TimerExpired[test ok] resp+ 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’ and that the DUT realizes the operation succeeded.
cDOns5	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 DUT realizes the operation failed.

6.2.5.14 Time and time synchronisation model

6.2.5.14.1 General

The time and time synchronization test cases defined for a client device are as specified in the following text.

6.2.5.14.2 Positive test cases

The test cases listed in Table 44 shall apply.

Table 44 – Time positive test cases

Test case	Test case description
cTm1	Verify that the DUT supports and executes the SCSM time synchronisation. Change the time in the time server and verify that the DUT uses the new time.
cTm2	Check that report/logging timestamp accuracy matches the documented timestamp quality.

6.2.5.14.3 Negative test cases

The test case listed in Table 45 shall apply.

Table 45 – Time negative test cases

Test case	Test case description
cTmN1	Verify that a lost time synchronisation is detected after a specified period and the timestamp quality invalid is set.
cTmN2	Verify that the DUT handles the time stamp quality coming from the time server.

6.2.6 Acceptance criteria

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

– specific design characteristics to be validated,

– checkpoints identified for anomalous conditions.

There are 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 compliance to the compliance 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-compliance with respect to (at least one of) the compliance 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 test case is passed when the DUT behaves as specified in IEC 61400-25 (all parts) and the PIXIT, the test cases are failed when the DUT behaves different as specified in IEC 61400-25 (all parts) and PIXIT. When not specified in IEC 61400-25 (all parts) 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

IEC 61400-25 (all parts) does not specify any specific performance requirements for applications operating in IEC 61400-25 (all parts) environment, but a series of essential metrics are identified. Based on this fact, Clause 7 defines the essential metrics identified within devices such that the documented product claims supporting those requirements can be compared across vendors.

7.2 Communication latency – Transfer time test introduction

The communications transfer time requirements are 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 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 IEC 61400-25 (all parts) services are used to deliver the process values. IEC 61400-25 (all parts) defines two mechanisms: Reporting and Control, whose transfer time can be tested.

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;

– control output latency.

A test system (see Figure 6) 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.

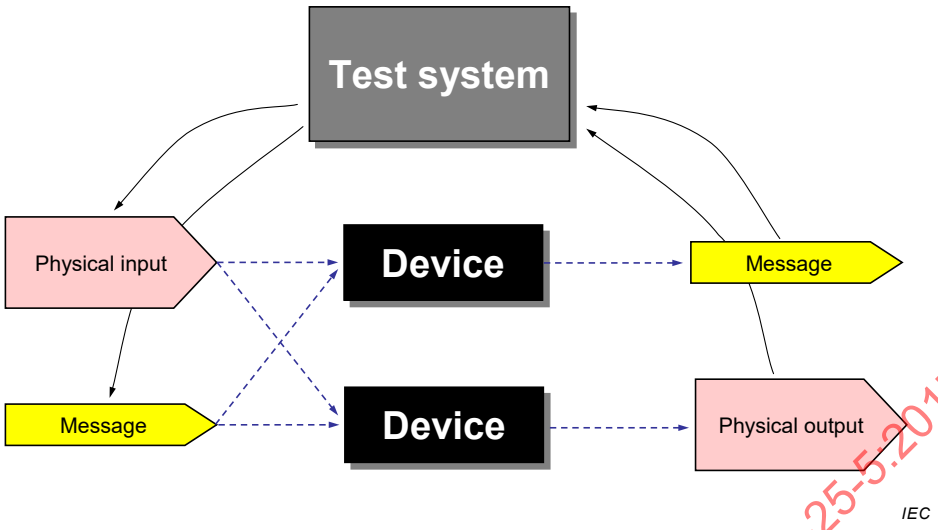


Figure 6 – Performance testing (black box principle)

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.

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.

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

7.3.2.1 General

The time synchronisation test requires a test system (see Figure 7) 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.

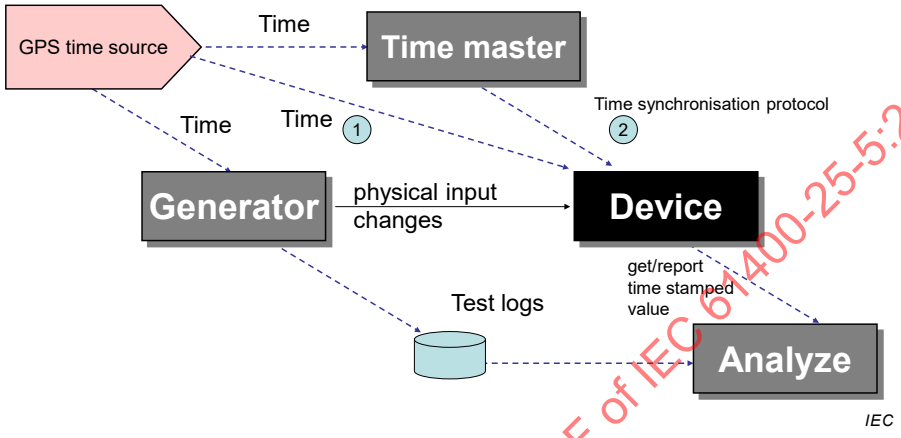


Figure 7 – Time synchronisation and accuracy test setup

7.3.2.2 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 time master as indicated with (1) on Figure 7. 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.

7.3.2.3 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.

Annex A
(informative)

Examples of test procedure template

A.1 Example 1

sBr1	GetLogicalNodeDirectory(BRCB) and GetBRCBValues	☐ Passed ☐ Failed ☐ Inconclusive
IEC 61400-25-3, xx IEC 61400-25-4, yy		
Expected result DUT sends GetLogicalNodeDirectory(BRCB) Response+ DUT sends GetBRCBValues Response+		
Test description For each logical node Client requests GetLogicalNodeDirectory(BRCB) For each BRCB Client requests GetBRCBValues()		
Comment		

A.2 Example 2

sRp1	GetLogicalNodeDirectory(URCB) and GetURCBValues	☐ Passed ☐ Failed ☐ Inconclusive
IEC 61400-25-3, xx IEC 61400-25-4, yy		
Expected result DUT sends GetLogicalNodeDirectory(URCB) Response+ DUT sends GetURCBValues Response+		
Test description For each logical node Client requests GetLogicalNodeDirectory(URCB) For each BRCB Client requests GetURCBValues()		
Comment		

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SYSTÈMES DE GÉNÉRATION D'ÉNERGIE ÉOLIENNE –

Partie 25-5: Communications pour la surveillance et la commande des centrales éoliennes – Essai de conformité

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61400-25-5 a été établie par le comité d'études 88 de l'IEC: Systèmes de génération d'énergie éolienne.

Cette deuxième édition annule et remplace la première édition parue en 2006. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- harmonisation avec la structure et les cas d'essai de l'IEC 61850-10:2012;
- l'utilisation de SCL dans le processus d'essai de conformité est hors du domaine d'application de la présente édition, mais sera envisagée pour la troisième édition;

- réduction du chevauchement entre les normes et simplification par augmentation des références à la série de normes IEC 61850;
- tous les cas d'essai qui emploient des fichiers SCL ne font toujours pas partie du présent document, les spécifications SCL applicables au domaine de l'énergie éolienne étant toujours en attente de publication.

La présente version bilingue (2020-10) correspond à la version anglaise monolingue publiée en 2017-09.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

Une liste de toutes les parties de la série IEC 61400, publiées sous le titre général *Systèmes de génération d'énergie éolienne*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

L'IEC 61400-25 (toutes les parties) concerne essentiellement les communications entre les composants des centrales éoliennes tels que les éoliennes et des acteurs tels que les systèmes SCADA. La communication interne entre les composants des centrales éoliennes ne relève pas du domaine d'application de l'IEC 61400-25 (toutes les parties).

L'IEC 61400-25 (toutes les parties) est conçue pour un environnement de communication fondé sur un modèle client-serveur. Trois domaines sont définis et sont modélisés séparément pour assurer l'extensibilité des systèmes mis en œuvre:

a) les modèles d'information de centrale éolienne;

b) le modèle d'échange d'information; et

c) le mapping de ces deux modèles pour un profil de communication normalisé.

Le modèle d'information de centrale éolienne et le modèle d'échange d'information, pris en compte ensemble, constituent une interface entre le client et le serveur. Dans cette combinaison, le modèle d'information de centrale éolienne sert de trame pour interpréter les données accessibles de la centrale éolienne. Le modèle d'information de centrale éolienne est utilisé par le serveur pour fournir au client une vue uniforme, orientée composant, des données de la centrale éolienne. Le modèle d'échange d'information reflète toutes les fonctions actives du serveur. L'IEC 61400-25 (toutes les parties) permet de connecter entre eux une combinaison hétérogène de clients et de serveurs qui proviennent de différents fabricants et fournisseurs.

Comme le montre la Figure 1, l'IEC 61400-25 (toutes les parties) définit un serveur qui présente les aspects suivants:

– les informations fournies par un composant de centrale éolienne, par exemple la "vitesse du rotor de l'éolienne" ou la "production d'électricité totale durant un intervalle de temps donné", sont modélisées et rendues accessibles. Les informations modélisées dans le document sont définies dans l'IEC 61400-25-2;

– les services pour échanger les valeurs des informations modélisées, définies dans l'IEC 61400-25-3;

– le mapping pour un profil de communication, qui fournit une pile de protocoles pour transporter les valeurs échangées qui proviennent des informations modélisées (IEC 61400-25-4).

L'IEC 61400-25 (toutes les parties) se contente de définir comment modéliser les informations, l'échange d'information et le mapping pour des protocoles de communication spécifiques. L'IEC 61400-25 (toutes les parties) s'abstient de définir comment et où mettre en œuvre l'interface de communication, l'interface du programme applicatif et les recommandations de mise en œuvre. Toutefois, l'objectif de l'IEC 61400-25 (toutes les parties) est de permettre l'accès aux informations associées à chacun des composants de la centrale éolienne (tel qu'une éolienne) à travers un dispositif logique correspondant.

Le présent document s'adresse aux fabricants de dispositifs ou de systèmes et/ou de composants système ainsi qu'aux développeurs/fournisseurs des systèmes d'essai.

NOTE Les abréviations employées dans l'IEC 61400-25-5 sont récapitulées aux Articles 3 et 4 ou peuvent figurer dans d'autres parties de la série de normes IEC 61400-25 en rapport avec les essais de conformité.

SYSTÈMES DE GÉNÉRATION D'ÉNERGIE ÉOLIENNE –

Partie 25-5: Communications pour la surveillance et la commande des centrales éoliennes – Essai de conformité

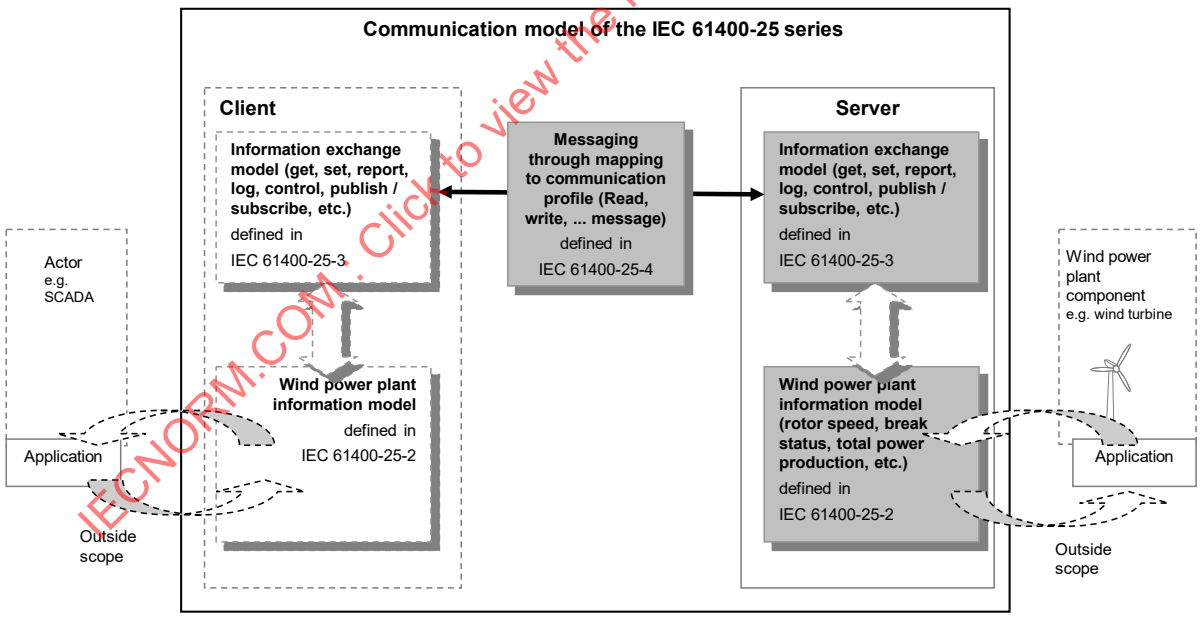
1 Domaine d'application

La présente partie de l'IEC 61400-25 spécifie les techniques normalisées destinées à soumettre à l'essai la conformité des mises en œuvre ainsi que des techniques de mesure spécifiques à appliquer lors de l'établissement des paramètres de performance. L'utilisation de ces techniques permet aux utilisateurs d'acheter en toute connaissance de cause des systèmes faciles à intégrer, qui fonctionnent correctement et prennent en charge les applications prévues.

La présente partie de l'IEC 61400-25 définit:

- les méthodes et les cas d'essai abstraits pour les essais de conformité des dispositifs serveur et client utilisés dans les centrales éoliennes;
- les mesurages à réaliser dans lesdits dispositifs conformément aux exigences relatives à la communication spécifiées dans l'IEC 61400-25 (toutes les parties).

NOTE Le rôle des installations d'essais dans le cadre des essais de conformité et de la certification des résultats ne relève pas du domaine d'application de l'IEC 61400-25-5.



Anglais	Français
Communication model of the IEC 61400-25 series	Modèle de communication de la série IEC 61400-25
Actor e.g. SCADA	Acteur ex. SCADA
Outside scope	En dehors du domaine d'application
Information exchange model (get, set, report, log, control, publish / subscribe, etc.) defined IEC 61400-25-3	Modèle d'échange d'information (get, set, report, log, control, publish / subscribe, etc.) défini dans l'IEC 61400-25-3
Wind power plant information model defined in IEC 61400-25-2	Modèle d'information de la centrale éolienne défini dans l'IEC 61400-25-2
Messaging through mapping to communication profile (Read, write, … message) defined in IEC 61400-25-4	Messagerie par le biais du mapping pour le profil de communication (message read, write,…) définie dans l'IEC 61400-25-4
Server	Serveur
Wind power plant information model (rotor speed, break status, total power production, etc.) defined in IEC 61400-25-2	Modèle d'information de la centrale éolienne (vitesse du rotor, statut de rupture, production totale d'électricité, etc.) défini dans l'IEC 61400-25-2
Wind power plant component e.g. wind turbine	Composant de la centrale éolienne ex. éolienne

Figure 1 – Modèle de communication conceptuel de la série de normes IEC 61400-25

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 61400-25 (toutes les parties), *Eoliennes – Partie 25: Communications pour la surveillance et la commande des centrales éoliennes*

IEC 61400-25-1:2006, *Wind turbines – Part 25-1: Communications for monitoring and control of wind power plants – Overall description of principles and models* (disponible en anglais seulement)

IEC 61400-25-2:2015, *Eoliennes – Partie 25-2: Communications pour la surveillance et la commande des centrales éoliennes – Modèles d'information*

IEC 61400-25-3:2015, *Eoliennes – Partie 25-3: Communications pour la surveillance et la commande des centrales éoliennes – Modèles d'échange d'information*

IEC 61400-25-4:2016, *Systèmes de génération d'énergie éolienne – Partie 25-4: Communications pour la surveillance et la commande des centrales éoliennes – Mapping pour les profils de communication*

IEC 61850-4:2011, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 4: Gestion du système et gestion de projet*

IEC 61850-6:2009, *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs* (disponible en anglais seulement)

IEC 61850-7-1:2011, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 7-1: Structure de communication de base – Principes et modèles*

IEC 61850-7-2:2010, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)* (disponible en anglais seulement)

IEC 61850-7-3:2010, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 7-3: Structure de communication de base – Classes de données communes*

IEC 61850-7-4:2010, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 7-4: Structure de communication de base – Classes de nœuds logiques et classes d'objets de données compatibles*

IEC 61850-10:2012, *Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 10: Essais de conformité*

ISO/IEC 9646 (toutes les parties), *Technologies de l'information – Interconnexion de systèmes ouverts – Cadre général et méthodologie des tests de conformité*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 61400-25-1 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
essai de réception en usine
FAT
essais fonctionnels, convenus avec le client, du système automatisé de poste fabriqué spécifiquement ou de ses composants utilisant l'ensemble de paramètres pour l'application prévue

Note 1 à l'article: L'essai de réception en usine (FAT) doit être réalisé dans l'usine du fabricant ou dans autre lieu convenu, au moyen d'un équipement d'essai simulant le procédé.

Note 2 à l'article: L'abréviation "FAT" est dérivée du terme anglais développé correspondant "factory acceptance test".

3.2
point d'arrêt
point, défini dans le document approprié, au-delà duquel une activité ne doit pas se poursuivre sans l'accord de la personne à l'origine (ou initiateur) de l'essai de conformité

Note 1 à l'article: L'installation d'essai doit fournir une notification écrite à la personne à l'origine de l'essai à un moment convenu préalable au point d'arrêt.

Note 2 à l'article: La personne à l'origine de l'essai ou son mandataire est tenu(e) de vérifier le point d'arrêt et d'agréer le déroulement de l'activité.

3.3
interopérabilité
capacité d'au moins deux dispositifs provenant du même fournisseur (ou de fournisseurs différents) à échanger des informations et à utiliser celles-ci à des fins de coopération correcte

Note 1 à l'article: Un ensemble de valeurs défini correspond aux quantités ou valeurs d'un autre ensemble.

3.4
déclaration de conformité de mise en œuvre du modèle
MICS
déclaration qui donne des détails sur les éléments du modèle d'objet de données normalisé pris en charge par le système ou le dispositif

Note 1 à l'article: L'abréviation "MICS" est dérivée du terme anglais développé correspondant "model implementation compliance statement".

3.5
essai négatif
essai visant à vérifier la réponse correcte d'un dispositif ou d'un système lorsqu'il est soumis:

– à des informations et des services, conformes à l'IEC 61400-25 (toutes les parties), qui ne sont pas mis en œuvre dans le dispositif ou le système soumis à l'essai;
– à des informations et des services, non conformes à l'IEC 61400-25 (toutes les parties), envoyés au dispositif ou au système soumis à l'essai

3.6
déclaration de conformité de mise en œuvre du protocole
PICS
déclaration qui contient le récapitulatif des capacités de communication du système ou du dispositif devant être soumis à l'essai

Note 1 à l'article: L'abréviation "PICS" est dérivée du terme anglais développé correspondant "protocol implementation compliance statement".

3.7
informations complémentaires de mise en œuvre du protocole destinées aux essais
PIXIT
déclaration qui contient des informations spécifiques au système ou au dispositif devant être soumis à l'essai et qui ne relèvent pas du domaine d'application de l'IEC 61400-25 (toutes les parties)

Note 1 à l'article: Les PIXIT ne font pas l'objet d'une normalisation.

Note 2 à l'article: L'abréviation "PIXIT" est dérivée du terme anglais développé correspondant "protocol implementation extra information for testing".

3.8
essai individuel de série
essai réalisé par le fabricant afin de garantir l'exploitation et la sécurité du dispositif

3.9
essai de réception sur site
SAT
vérification de chaque donnée et point de contrôle ainsi que du fonctionnement correct au sein de la centrale éolienne et de son environnement d'exploitation dans la totalité de l'installation au moyen de l'ensemble de paramètres final

Note 1 à l'article: Le SAT est la condition préalable à la mise en service de la centrale éolienne.

Note 2 à l'article: L'abréviation "SAT" est dérivée du terme anglais développé correspondant "site acceptance test".

3.10
essai système
vérification du comportement correct des composants de la centrale éolienne ainsi que de l'ensemble de la centrale dans des conditions d'applications diverses

Note 1 à l'article: L'essai système marque le stade final du développement d'un composant système d'une centrale éolienne.

3.11
essai du système
validation du comportement correct des IED et du système d'automatisation de système électrique (PUAS) global dans des conditions d'application spécifiques

Note 1 à l'article: L'essai du système constitue le stade final du développement des IED en tant que composants d'une famille de produits de système d'automatisation de système électrique (PUAS).

3.12
équipement d'essai
ensemble des outils et des instruments simulant et vérifiant les entrées/sorties de l'environnement d'exploitation de la centrale éolienne, tels que l'éolienne, l'équipement de distribution, les transformateurs, les centres de contrôle réseau ou les unités de télécommunication connectées, d'une part, et les liens de communication entre les composants du système de la centrale éolienne, d'autre part

3.13
installation d'essai
organisation capable de fournir un équipement d'essai approprié et du personnel formé pour la réalisation des essais de conformité

Note 1 à l'article: Il convient que la gestion des essais de conformité et des informations qui en découlent s'inscrive dans le cadre d'un système qualité.

3.14
déclaration de conformité relative aux questions techniques
TICS
déclaration qui contient des informations spécifiques aux questions techniques de mise en œuvre détectées après la publication de la norme

Note 1 à l'article: La TICS ne fait pas l'objet d'une normalisation.

Note 2 à l'article: L'abréviation "TICS" est dérivée du terme anglais développé correspondant "technical issues compliance statement".

3.15
essai de type
vérification du comportement correct des IED (composants du système) de la centrale éolienne au moyen du logiciel du système soumis à l'essai dans les conditions d'essai correspondant aux données techniques

Note 1 à l'article: L'essai de type marque le stade final du développement matériel et constitue la condition préalable au lancement de la production. Cet essai doit être réalisé avec des composants système qui ont été fabriqués dans le cycle de production normal.

3.16
point d'observation
point, défini dans le document approprié, auquel un contrôle portant sur une activité est effectué

Note 1 à l'article: L'activité peut être réalisée sans l'approbation de l'initiateur de l'essai de conformité. L'installation d'essai fournit à l'initiateur une note écrite à un moment convenu préalable au point d'observation. L'initiateur ou son représentant a le droit, mais n'est pas tenu, de vérifier le point d'observation.

4 Abréviations

ACSI	Abstract Communication Service Interface (interface abstraite des services de communication)
BRCB	Buffered Report Control Block (bloc de commande de rapport mis en mémoire tampon)
CDC	Classe de Données Communes
DUT	Device Under Test (dispositif soumis à l'essai)
FAT	Factory acceptance test (Essai de réception en usine)
GI	General Interrogation (interrogation générale)
IHM	Interface Homme Machine
ICD	IED capability subscription (abonnement aux capacités des IED)
IED	Intelligent Electronic Device (dispositif électronique intelligent)
IID	Instantiated IED Description (description des IED instanciés)
IP	Inter-networking protocol internet Protocol (protocole Internet de protocole d'interconnexion de réseaux)
LCB	Log Control Block (bloc de commande de journal)
LD	Logical Device (dispositif logique)
LN	Logical Node (nœud logique)
MICS	Model Implementation Compliance Statement (déclaration de conformité de mise en œuvre du modèle)
PICS	Protocol Implementation Compliance Statement (déclaration de conformité de mise en œuvre du protocole)
PIXIT	Protocol Implementation eXtra Information for Testing (informations complémentaires de mise en œuvre du protocole destinées aux essais)
PUAS	Power Utility Automation System (système d'automatisation de système électrique)
RCB	Report Control Block (bloc de commande de rapport)
RTU	Remote Terminal Unit (unité terminale distante)
SAT	site acceptance test (Essai de réception sur site)
SCADA	Supervisory Control And Data Acquisition (commande, surveillance et acquisition de données)
SCSM	Specific Communication Service Mapping (mapping des services de communication spécifiques)
SGCB	Setting Group Control Block (bloc de contrôle de groupe de réglage)
SoE	Sequence-of-Events (séquence des événements)
SUT	System Under Test (système soumis à l'essai)
TICS	Technical Issues Compliance Statement (déclaration de conformité relative aux questions techniques)
TPAA	Two Party Application Association (association d'applications en deux parties)
TUT	Tool Under Test (outil soumis à l'essai)
URCB	Unbuffered Report Control Block (bloc de commande de rapport non mis en mémoire tampon)
UTC	Coordinated Universal Time (temps universel coordonné)
WPP	Wind Power Plant (centrale éolienne)

5 Présentation des essais de conformité

5.1 Généralités

Le développement et la production d'un dispositif, puis l'exploitation correcte d'un système complet conçu conformément aux besoins spécifiques d'un client impliquent de nombreuses étapes. Des étapes d'essai appropriées font partie de ce processus.

De nombreux essais internes qui ont lieu pendant le développement d'un dispositif ou d'un composant système débouchent sur un essai de type (essai au niveau de l'unité) réalisé au moins par le fournisseur et, si les normes applicables l'exigent, par un organisme d'essai indépendant. Dans le cadre de la présente partie de l'IEC 61400-25 (toutes les parties), le terme "essai de type" se limite au comportement fonctionnel du dispositif et exclut la communication.

Des essais individuels de série continus dans la chaîne de production sont nécessaires pour assurer une qualité constante des dispositifs fournis conformément aux procédures qualité du producteur.

Un essai de conformité correspond à l'essai de type dans le domaine de la communication et, étant donné que la communication établit un système, il correspond également à l'essai système de base des composants système intégrés. En tant que norme relative aux communications mondiales, l'IEC 61400-25 (toutes les parties) inclut des essais de conformité normalisés qui visent à garantir que tous les fournisseurs satisfont aux exigences applicables.

Les essais de type et les essais de conformité ne garantissent pas totalement que l'ensemble des exigences fonctionnelles et de performance sont respectées. Toutefois, lorsqu'ils sont réalisés correctement, ces essais réduisent significativement le risque de problèmes liés aux coûts survenant pendant l'intégration du système dans l'usine et sur site.

Les essais de conformité ne remplacent pas les essais système spécifiques au projet tels que le FAT et le SAT. Le FAT et le SAT s'appuient sur les exigences des clients relatives à un système de centrale éolienne dédié. Ils sont effectués par l'intégrateur du système, généralement en présence du client. Ces essais augmentent le niveau de confiance selon lequel tous les problèmes potentiels du système ont été identifiés et résolus. Ces essais établissent que le système de centrale éolienne fourni fonctionne comme spécifié.

5.2 Procédures d'essai de conformité

En général, il convient que les essais de conformité du comportement de communication d'un composant système portent sur les exigences fonctionnelles et les exigences de performance des applications types prises en charge par ces dispositifs dans une centrale éolienne.

Les essais de conformité démontrent la capacité du dispositif soumis à l'essai (DUT) à fonctionner avec d'autres systèmes ou composants système de manière spécifiée, conformément à l'IEC 61400-25 (toutes les parties).

Les essais de conformité nécessitent la prise en compte des questions suivantes:

– le problème lié à tous les essais concerne l'exhaustivité des essais. Le nombre de toutes les situations possibles peut être très élevé. Il peut être possible de couvrir tous les cas d'exploitation normaux, mais cela peut ne pas s'appliquer à tous les cas d'échec;
– il est impossible de soumettre à l'essai toutes les configurations système en utilisant des composants système qui proviennent de différents fournisseurs à l'échelle mondiale. Par conséquent, il convient d'utiliser une architecture d'essai normalisée équipée de simulateurs de dispositifs. L'utilisation d'une telle architecture d'essai implique un accord relatif à sa configuration et aux procédures d'essai appliquées afin d'obtenir des résultats compatibles;
– une norme sur la communication ne normalise pas les fonctions de l'équipement de communication. Par conséquent, les modes d'échec des fonctions ne relèvent pas du domaine d'application de la présente partie de l'IEC 61400-25 (toutes les parties). Cependant, l'existence des fonctions distribuées et l'impact de la réponse fonctionnelle dans les dispositifs sur le flux de données créent une certaine interdépendance;
– selon les définitions données dans l'IEC 61400-25 (toutes les parties), certaines propriétés du dispositif peuvent être démontrées au moyen d'informations et de documents fournis avec le DUT aux fins des essais de conformité plutôt qu'au moyen de l'essai de conformité proprement dit.

L'essai de conformité établit le bon fonctionnement de la communication du DUT conformément à l'IEC 61400-25 (toutes les parties). L'IEC 61400-25 (toutes les parties) concerne essentiellement l'interopérabilité au moyen d'objets de données, de fonctions et de modèles de dispositifs, y compris les services au niveau de l'application ou au-dessus (ACSI).

Etant donné que l'IEC 61400-25 (toutes les parties) ne définit aucune nouvelle pile de communication, la conformité avec l'ensemble des sept couches ISO/OSI peut être démontrée par un document attestant que le logiciel de la pile de communication compatible avec les spécifications correspondantes est implémenté et peut avoir fait l'objet d'un essai préalable et d'une certification éventuelle. Dans l'essai de conformité normalisé, seule l'application conforme à l'ACSI peut être soumise à l'essai.

5.3 Assurance qualité et essais

5.3.1 Généralités

Afin d'assurer la qualité au cours d'essais de conformité, un système d'assurance qualité doit être en place. Cela doit être clairement démontré par l'installation d'essai et cela s'applique également au système d'assurance qualité de tout sous-traitant.

En général, la surveillance de la qualité a pour objet de surveiller et vérifier l'état des composants pendant toutes les phases des essais de conformité. A cet effet, des contrôles sont effectués, fondés sur des points d'arrêt et des points d'observation indiqués par l'initiateur ou son représentant dans l'essai et dans le plan de contrôle fourni par l'installation d'essai. Ces contrôles sont liés au processus et fournissent des informations et un niveau de confiance relatifs à la qualité des essais. La surveillance de la qualité réduit les risques d'échec pendant le FAT et le SAT.

5.3.2 Plan qualité

5.3.2.1 Plan qualité pour les essais de conformité

L'installation d'essai fournit, à des fins d'évaluation, un plan qualité pour l'essai de conformité.

Le plan doit décrire toutes les mesures relatives au domaine d'application et/ou aux aspects de l'organisation, du temps, des informations et de la qualité. Un seul plan est attribué à l'installation d'essai et à ses sous-traitants.

Il est proposé que le plan qualité de l'essai de conformité contienne les éléments suivants:

– une description complète et détaillée des méthodes de travail. Cette description permet d'assurer que toutes les activités vérifiables satisfont à l'ensemble des exigences et conditions applicables spécifiées dans le domaine d'application pendant la durée autorisée;
– une description détaillée de toutes les tâches à réaliser, y compris les références au calendrier, une présentation du personnel, des matériaux et des méthodes de travail impliqués ainsi que des méthodes et procédures concernées;
– une description détaillée de l'organisation, y compris les affectations, les tâches et les responsabilités du personnel mentionné au cours des différentes étapes des programmes d'essais. La description doit inclure tous les essais, les contrôles, toutes les recherches et tous les audits pendant les différentes étapes des essais ainsi que les dates auxquelles ils auront lieu. Ces descriptions seront incluses dans le plan d'essai et de contrôle;
– une méthode de traitement des écarts, des changements et des modifications pendant toutes les étapes de l'essai;
– une procédure signée et une description de la documentation à fournir.

5.3.2.2 Plan d'essai et de contrôle

Le plan qualité de l'essai de conformité doit contenir un plan d'essai et de contrôle. Dans ce plan, l'installation d'essai spécifie, pour toutes les phases des essais:

– les éléments contrôlés, soumis à l'essai et enregistrés;
– l'objectif des contrôles et des essais;
– les procédures et normes selon lesquelles les contrôles, essais et enregistrements sont effectués;
– les résultats attendus des contrôles et des essais;
– l'identification des personnes chargées des contrôles, essais et enregistrements.

L'installation d'essai est responsable de l'exécution correcte et dans les délais de toutes les activités mentionnées dans le plan d'essai et de contrôle.

L'installation d'essai doit fournir une proposition de points d'arrêt, d'observation et de revue dans le plan d'essai et de contrôle.

Plusieurs méthodes permettent d'élaborer un point d'arrêt ou d'observation. L'initiateur de l'essai de conformité ou son représentant peut être présent lors de l'exécution d'un essai ou d'un contrôle. Il est également possible d'examiner les documents qualité associés, par exemple les listes de contrôle, les documents de vérification et de validation. Le point d'arrêt ou d'observation peut avoir lieu sur le site de l'installation d'essai pendant l'exécution d'un essai, ou un contrôle peut être effectué sur le site de l'initiateur, auquel cas l'installation d'essai doit fournir tous les documents pertinents à l'initiateur.

Tous les points d'arrêt et d'observation sont annoncés par l'installation d'essai au moins à une date/heure prédéfinie avant leur réalisation. Une période d'au moins une semaine est recommandée, selon la durée exigée pour organiser les déplacements et la disponibilité des ressources nécessaires.

5.3.2.3 Audits demandés par l'initiateur

L'initiateur d'un essai de conformité a le droit de mener des audits sur le système qualité de l'installation d'essai et de ses sous-traitants. L'installation d'essai doit coopérer et fournir un accès à tous les sites concernés par l'essai de conformité. Le droit de l'initiateur à vérifier la qualité de l'essai de conformité ne dégage pas l'installation d'essai de ses responsabilités.

Les contrôles et essais mis en œuvre par l'initiateur d'un essai de conformité doivent être possibles à des dates/heures faisant l'objet d'un accord commun sur les sites, bureaux et usines de l'installation d'essai et de tous les sous-traitants et parties tierces concernés.

5.4 Essais

5.4.1 Généralités

Les essais de conformité doivent être adaptés à chaque dispositif soumis à l'essai en fonction des capacités identifiées dans les PICS, PIXIT et MICS remises par le fournisseur. Lorsque les dispositifs sont soumis à l'essai, les éléments suivants doivent être fournis:

– un dispositif prêt pour les essais;
– une déclaration de conformité de mise en œuvre du protocole (PICS);
– des informations complémentaires de mise en œuvre du protocole destinées aux essais (PIXIT);
– une déclaration de conformité de mise en œuvre du modèle (MICS); une déclaration de conformité relative aux questions techniques (TICS);
– des manuels d'instruction qui décrivent l'installation et l'exploitation du dispositif.

Les exigences des essais de conformité se divisent en deux catégories:

- les exigences de conformité statiques (définissent les exigences que la mise en œuvre doit respecter);
- les exigences de conformité dynamiques (définissent les exigences posées par le protocole utilisé pour une mise en œuvre donnée).

Les exigences de conformité statiques et dynamiques doivent être définies dans une déclaration de conformité de mise en œuvre du protocole ou PICS. La PICS a trois objectifs:

a) sélectionner l'ensemble d'essais approprié;

b) assurer la réalisation des essais appropriés à une déclaration de conformité;

c) fournir la base de la revue de conformité statique.

Une PICS normalisée doit être fournie.

La PICS concrète doit être telle que définie pour les SCSM.

Une déclaration de conformité de mise en œuvre du modèle ou MICS doit être fournie et décrire les éléments du modèle d'objet de données normalisé pris en charge par le système ou dispositif. La MICS est mise en œuvre dans l'ICD du fichier IID conformément à l'IEC 61850-6.

Une déclaration de conformité relative aux questions techniques (TICS) doit être fournie et décrire les questions techniques mises en œuvre après la publication de la norme.

Outre la PICS, des informations complémentaires de mise en œuvre du protocole destinées aux essais (PIXIT) doivent être fournies.

Le processus d'évaluation de la conformité est représenté à la Figure 2.

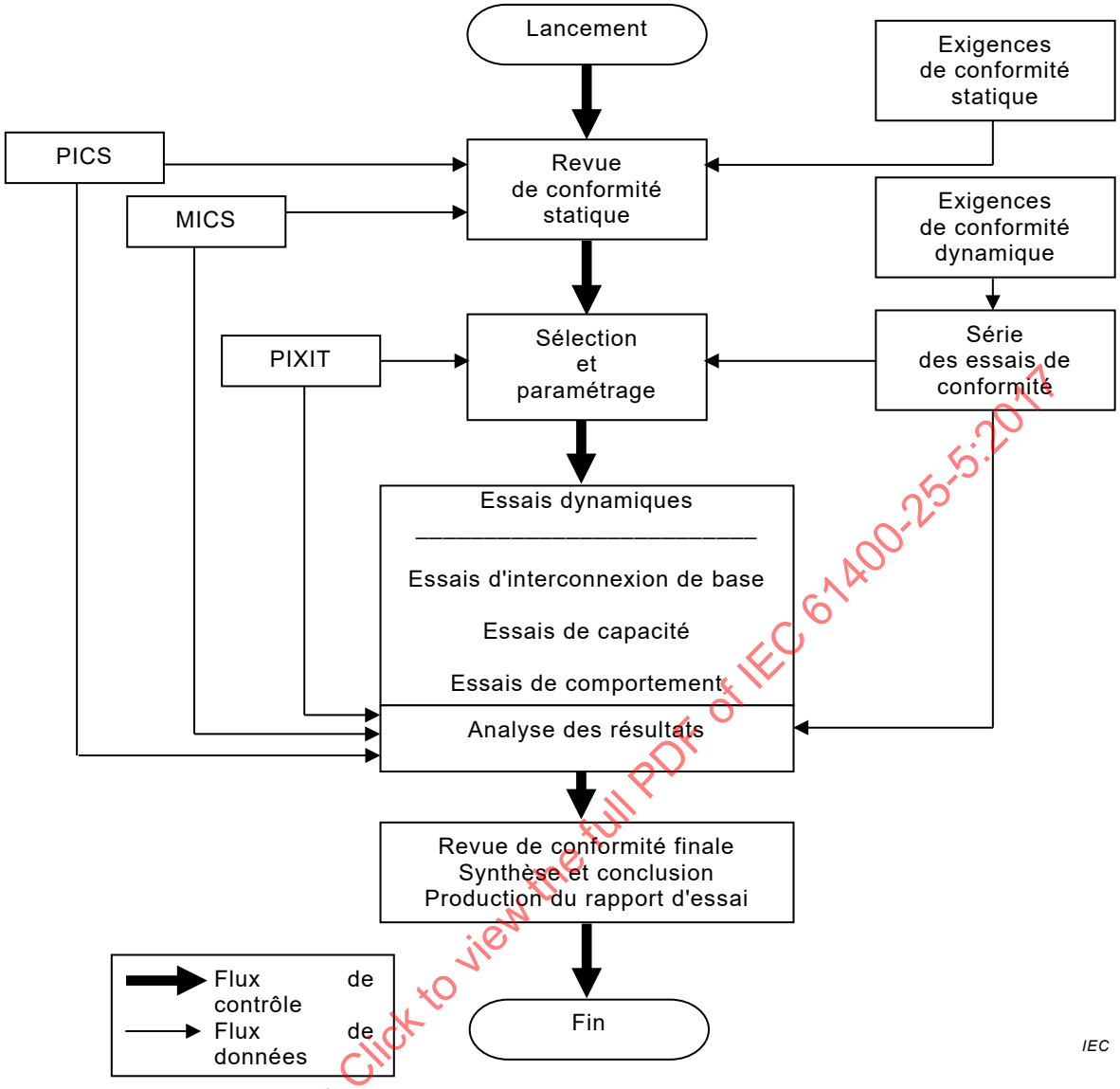


Figure 2 – Processus d'évaluation de la conformité conceptuel

5.4.2 Essais des dispositifs

Un essai de conformité doit être réalisé entre un dispositif unique et un dispositif pour essai.

Les essais de conformité spécifiques au dispositif englobent les essais positifs et négatifs des éléments suivants, selon le cas:

– le contrôle de la documentation et de la version du dispositif;
– l'essai du fichier de configuration du dispositif par rapport au modèle d'objet du dispositif (IEC 61400-25-2);
– l'essai de l'implémentation de la pile de communication par rapport au SCSM applicable (IEC 61400-25-4);
– l'essai des services ACSI implémentés par rapport à la définition de l'ACSI (IEC 61400-25-3);
– l'essai des extensions spécifiques au dispositif conformément aux règles définies par l'IEC 61400-25 (toutes les parties) en général.

5.5 Documentation du rapport d'essai de conformité

Un rapport d'essai de conformité doit comporter les informations suivantes:

– une liste des références de tous les documents qui décrivent ou spécifient tout essai qualificatif réalisé. Ces documents peuvent inclure les procédures normales d'essai et d'exploitation du fournisseur ainsi que les normes locales, nationales et internationales. Les normes internationales doivent être indiquées par numéro de document, date, article et paragraphe. Les références à d'autres documents doivent inclure une adresse source complète et une identification de document. Un résumé complet et inscrit dans un contexte précis ou un extrait du document peuvent être inclus par souci de commodité;
– une liste de tout équipement d'essai spécialisé ou des programmes informatiques utilisés pour la réalisation des essais de conformité;
– le nom et l'adresse du fournisseur;
– le nom et l'adresse de l'initiateur de l'essai de conformité (s'il diffère du nom du fournisseur);
– le nom du dispositif soumis à l'essai;
– toutes les versions (matériel, micrologiciel, etc.) du dispositif soumis à l'essai;
– le nom et l'adresse de l'installation d'essai;
– la date d'émission du rapport d'essai;
– le nom et la signature du contrôleur;
– un numéro de référence unique;
– une liste des éléments soumis à l'essai afin de vérifier la conformité;
– les commentaires et problèmes identifiés;
– pour chaque élément soumis à l'essai, les aspects suivants doivent être documentés:
  - la description de l'élément soumis à l'essai en indiquant l'objectif de l'essai, la procédure d'essai et le résultat attendu;
  - une référence à l'article et au paragraphe concernés de la série IEC 61400-25 (toutes les parties);
  - un identifiant unique pour chaque élément soumis à l'essai;
  - le résultat de l'essai: accepté, refusé, non concluant, non applicable;
  - la comparaison du résultat de l'essai au résultat attendu.

Les modifications du dispositif apportées en un point quelconque de l'essai, notamment celles qui visent à corriger un défaut de l'essai, doivent être entièrement décrites. Les conséquences et exigences relatives au nouvel essai d'un dispositif, si nécessaire, doivent être spécifiées dans les plans d'essai et les rapports d'essai correspondants.

La documentation de l'essai de conformité doit être remise à l'initiateur.

6 Essais de conformité liés au dispositif

6.1 Méthode d'essai

Les essais de communication nécessitent au moins deux dispositifs communiquant entre eux. Il n'est pas possible de réaliser des essais d'interopérabilité exhaustifs de tous les produits existants. Par conséquent, le concept de l'essai doit inclure des dispositifs pour essai, des configurations d'essai et des scénarios d'essai.

Il convient que le comportement dynamique soit soumis à l'essai correctement au moyen de cas d'essai bien définis.

Une attention particulière doit être accordée aux équipements de communication tels que les coupleurs en étoile, les commutateurs, etc., qui doivent prendre en charge toutes les caractéristiques exigées par l'IEC 61400-25 (toutes les parties), mais sans introduire d'éventualités ou de restrictions supplémentaires. L'impact de la méthode de communication (client-serveur, FTP/IP, etc.) utilisée par le dispositif soumis à l'essai doit être correctement pris en compte dans les procédures d'essai. La vérification des applications fonctionnelles ne fait pas partie d'un essai de conformité, même si des outils avancés peuvent fournir une telle analyse.

6.2 Procédures d'essai de conformité

6.2.1 Généralités

Le 6.2 décrit les exigences relatives aux procédures d'essai, la structure de l'essai, les cas d'essai abstraits (ce qui doit être soumis à l'essai). Le format et deux exemples de procédures d'essai (mode opératoire à suivre pour les essais) sont donnés à l'Annexe A.

6.2.2 Exigences relatives aux procédures d'essai

Les exigences relatives aux procédures d'essai sont les suivantes:

– les cas d'essai abstraits décrivent les éléments qui doivent être soumis à l'essai; les procédures d'essai décrivent le mode opératoire qui doit être suivi par un ingénieur responsable des essais ou un système d'essai;

– les cas d'essai comprennent une référence à un ou plusieurs paragraphes applicables dans le ou les documents référencés;

– les résultats d'essai doivent être reproductibles dans le même laboratoire d'essai ainsi que dans d'autres laboratoires;

– des essais automatisés qui impliquent une intervention humaine minimale, autant que raisonnablement possible;

– les essais doivent porter plus spécifiquement sur des situations qui ne peuvent pas être facilement soumises à l'essai durant, par exemple, un essai de réception en usine ou sur site, et prévenir des risques d'interopérabilité, tels que:

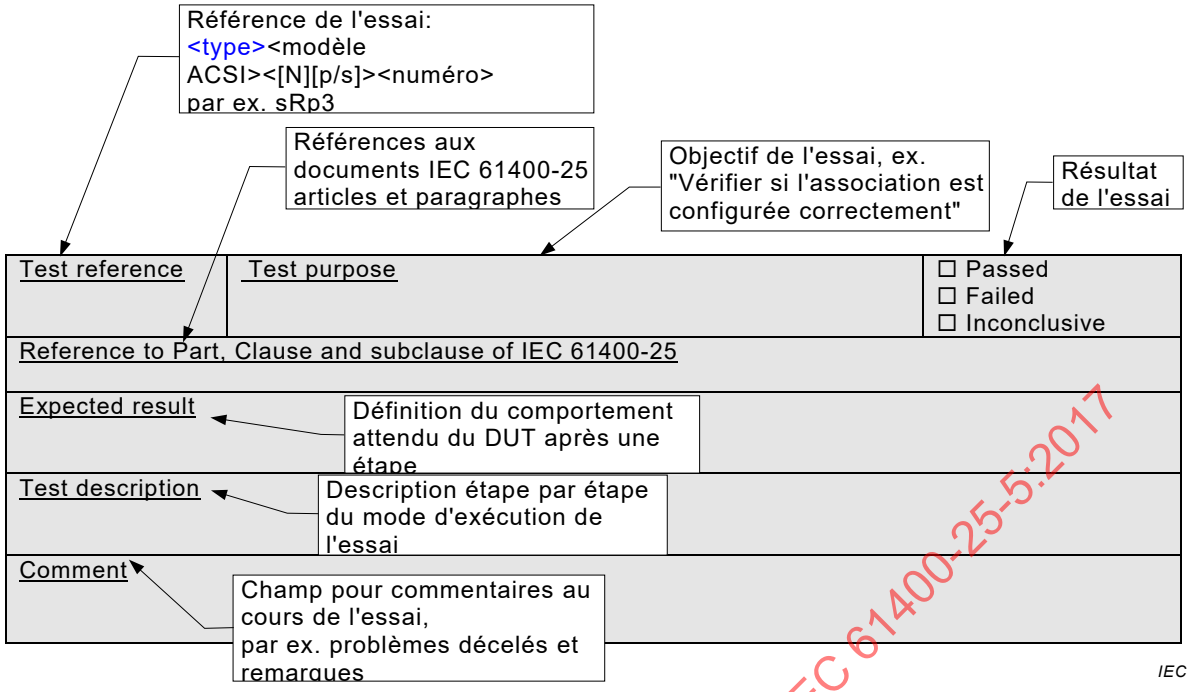
  - le mode de contrôle du dispositif en cas de paquets différés, perdus, doubles et défectueux;
  - les risques liés à la configuration, l'implémentation, l'exploitation;
  - des noms, paramètres, options ou types de données incohérents;
  - le dépassement de certaines limites, plages ou temporisations;
  - des situations provoquées pour soumettre à l'essai des réponses négatives;
  - la vérification de tous les chemins des machines à états (commande); et
  - des opérations de commande provoquées simultanément, provenant de clients multiples;

– les essais de l'ACSI sont axés sur la couche application (mapping);

– le dispositif soumis à l'essai (DUT) est considéré comme une boîte noire. L'interface entrée-sortie et l'interface de communication sont utilisées aux fins de l'essai;

– l'essai porte sur les versions, le modèle de données et le fichier de configuration, ainsi que sur l'utilisation de la terminologie de la série ISO/IEC 9646 applicable.

Les procédures d'essai doivent être conformes au modèle représenté à la Figure 3. Dans ce format, le document relatif aux procédures d'essai peut également faire office de rapport d'essai. L'Annexe A donne quelques exemples de procédures d'essai.



Anglais	Français
Test reference	Référence de l'essai
Test purpose	Objectif de l'essai
Reference to Part, Clause and subclause of IEC 61400-25	Référence à la partie, à l'article et au paragraphe de l'IEC 61400-5
Passed	Accepté
Failed	Refusé
Inconclusive	Non concluant
Expected result	Résultat attendu
Test description	Description de l'essai
Comment	Commentaire

Figure 3 – Format de la procédure d'essai

6.2.3 Structure de l'essai

Les cas d'essai du serveur sont structurés comme suit:

– la documentation et le contrôle de version (IEC 61400-25-5);
– le modèle de données (IEC 61400-25-2);
– le mapping des modèles et services ACSI (IEC 61400-25-3);
– tous les cas d'essai sont hérités de l'IEC 61850-10:2012, s'ils sont applicables dans le cadre de l'IEC 61400-25 (toutes les parties).

6.2.4 Cas d'essai pour un dispositif serveur

6.2.4.1 Généralités

La présente partie de l'IEC 61400-25 spécifie l'architecture des systèmes d'essai et des cas d'essai abstraits pour un dispositif serveur. Les cas d'essai abstraits doivent être utilisés pour la définition de procédures d'essai à mettre en place au cours des essais.

Les procédures d'essai spécifiques au SCSM doivent être fournies par des installations d'essai définies par les acteurs du marché.

6.2.4.2 Architecture du système d'essai pour un dispositif serveur

Afin de pouvoir réaliser un essai sur le dispositif, une configuration d'essai minimale est nécessaire. L'architecture d'essai comprend (voir Figure 4):

– le DUT;
– un simulateur client pour initier et générer des messages TPAA ainsi que pour enregistrer et traiter les informations qui en découlent;
– une matrice pour la synchronisation temporelle (la matrice de synchronisation temporelle);
– un logiciel outil d'ingénierie pour configurer le DUT;
– un analyseur de protocole/réseau pour surveiller et stocker l'ensemble du trafic du réseau pour chaque cas d'essai;
– un générateur de signal pour provoquer des événements binaires et analogiques, commandé par la matrice d'essai ou l'ingénieur responsable de l'essai.

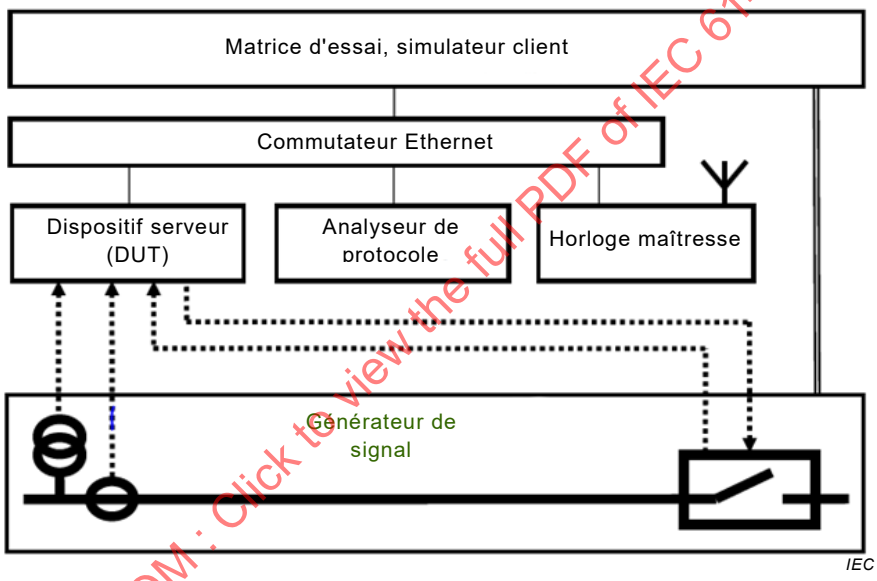


Figure 4 – Architecture du système d'essai pour un dispositif serveur

Le système d'essai doit inclure une documentation relative au matériel du système d'essai et au logiciel du système d'essai.

6.2.4.3 Présentation de la procédure d'essai relative au contrôle de la documentation et de la version

Les cas d'essais répertoriés dans le Tableau 1 doivent s'appliquer.

Tableau 1 – Cas d'essai de la documentation serveur

Cas d'essai	Description du cas d'essai
sDoc1	Vérifier si la version logicielle principale/secondaire de la documentation PICS concorde avec celle du DUT (IEC 61850-4). La PICS doit contenir la déclaration de conformité ACSI selon l'IEC 61400-25-3.
sDoc2	Vérifier si la documentation PIXIT du fabricant de la version logicielle principale/secondaire concorde avec la version logicielle du DUT (IEC 61850-4). Les PIXIT doivent indiquer les informations exigées comme demandé dans les cas d'essai.
sDoc3	Vérifier si la documentation MICS du fabricant de la version logicielle principale/secondaire concorde avec la version logicielle du DUT (IEC 61850-4). La MICS doit indiquer la sémantique de tous les nœuds logiques, objets de données, attributs de données et énumérations non normalisés.
sDoc4	Vérifier si la documentation TICS du fabricant de la version logicielle principale/secondaire concorde avec la version logicielle du DUT (IEC 61850-4). La TICS doit indiquer les questions techniques mises en œuvre.

6.2.4.4 Cas d'essai du modèle de données

Les cas d'essais répertoriés dans le Tableau 2 doivent s'appliquer.

Tableau 2 – Cas d'essai du modèle de données serveur

Cas d'essai	Description du cas d'essai
sMdl1	Vérifier la présence d'objets obligatoires pour chaque LN. Accepté lorsque tous les objets/attributs sont présents.
sMdl2	Vérifier la présence des objets corrects dont la présence est soumise à condition pour chaque LN. Accepté lorsque tous les objets/attributs sont présents.
sMdl3	Vérifier l'absence des objets erronés dont la présence est soumise à condition. Accepté lorsque ces objets/attributs sont absents.
sMdl4	Vérifier le mapping du modèle de données selon le SCSM applicable en ce qui concerne la longueur du nom et l'expansion de l'objet. Accepté lorsque le mapping est conforme au SCSM applicable.
sMdl5	Vérifier le mapping du modèle de données selon le SCSM applicable en ce qui concerne l'organisation des composants fonctionnels. Accepté lorsque le mapping est conforme au SCSM applicable.
sMdl6	Vérifier le mapping du modèle de données selon le SCSM applicable en ce qui concerne le nommage des blocs de commande et des journaux. Accepté lorsque le mapping est conforme au SCSM applicable.
sMdl7	Vérifier le type de données de tous les objets pour chaque LN. Accepté lorsque le type de données de tous les objets/attributs concorde avec l'IEC 61400-25-2, l'IEC 61400-25-3 et le SCSM applicable.
sMdl8	Vérifier que les valeurs des attributs de données du dispositif se situent dans la plage spécifiée (effort permanent tout au long de l'essai de conformité). Accepté lorsque toutes les valeurs se situent dans la plage.
sMdl9	Vérifier si les extensions du modèle de données spécifiques au fabricant sont mises en œuvre conformément aux règles d'extension de l'IEC 61400-25-2 (uniquement lorsque des extensions sont mises en œuvre). Accepté lorsque toutes les extensions sont mises en œuvre conformément aux règles spécifiées.
sMdl10	Vérifier si l'ordre des attributs de données dans les types d'objets de données concorde avec l'IEC 61400-25-2. Accepté lorsque tous les attributs sont dans l'ordre correspondant.
sMdl11	Vérifier la longueur maximale du nom du dispositif logique, du nœud logique, des ensembles de données et des blocs de commande selon l'IEC 61850-7-2:2010, 22.2, et le SCSM applicable.
sMdl12	Vérifier que les règles pour l'instanciation d'objets de données multiples sont respectées (IEC 61850-7-1, IEC 61850-7-4).
sMdl13	Vérifier que l'espace de nom du dispositif logique fait référence à l'IEC 61400-25-2:2015.
sMdl14	Vérifier l'utilisation correcte des espaces de noms pour les applications non relatives à une centrale éolienne.

6.2.4.5 Mapping des cas d'essai des modèles et services ACSI

Les éléments soumis à l'essai doivent être regroupés dans des tableaux. Les tableaux doivent refléter les modèles de services applicables spécifiés dans l'IEC 61850-7-2:2010, Figure 3:

– association d'applications (sAss);
– serveur, dispositif logique, nœud logique, données et modèle d'attribut de données (sSrv);
– modèle d'ensemble de données (sDs);
– modèle de commande de rapport non mis en mémoire tampon (sRp);
– modèle de commande de rapport mis en mémoire tampon (sBr);
– modèle de commande de journal (sLog);
– modèle de commande (sCtl);
– modèle de synchronisation temporelle (sTm).

Les cas d'essai sont définis pour chaque modèle et service ACSI dans les catégories suivantes:

- positif = vérification des conditions normales, entraînant généralement "response+";
- négatif = vérification des conditions anormales, entraînant généralement "response-".

Un cas d'essai est obligatoire lorsque le modèle ACSI et le service ACSI applicables sont pris en charge par le DUT. Cette prise en charge est spécifiée dans la PICS conformément à l'IEC 61850-7-2:2010, Annexe A. L'interprétation du résultat de l'essai (accepté/refusé) dépend des capacités déclarées de l'IED, par exemple dans le fichier ICD, ainsi que du résultat de l'essai.

6.2.4.6 Association d'applications

6.2.4.6.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 3 doivent s'appliquer.

Tableau 3 – Cas d'essai positifs d'association

Cas d'essai	Description du cas d'essai
sAss1	Effectuer l'association et libérer une association TPAA (IEC 61850-7-2:2010, 8.3).
sAss2	Effectuer l'association et interrompre une association TPAA côté client (IEC 61850-7-2:2010, 8.3).
sAss3	Effectuer l'association au nombre maximal de clients simultanément (PIXIT).

6.2.4.6.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 4 doivent s'appliquer.

Tableau 4 – Cas d'essai négatifs d'association

Cas d'essai	Description du cas d'essai
sAssN1	Vérifier qu'avec des paramètres d'authentification incorrects et une authentification activée au niveau du serveur, l'association échoue, et qu'avec une authentification désactivée, le serveur effectue l'association (IEC 61850-7-2:2010, 8.3).
sAssN2	Vérifier qu'avec des paramètres d'association incorrects au niveau du serveur ou du client, l'association échoue (IEC 61850-7-2:2010, 8.3, PIXIT).
sAssN3	Configurer maximum+1 associations; vérifier que le dernier associé est refusé.
sAssN4	Déconnecter l'interface de communication; le DUT doit détecter une liaison perdue dans un délai spécifié.

Cas d'essai	Description du cas d'essai
sAssN5	Interrompre et restaurer l'alimentation; le DUT doit accepter une demande d'association lorsqu'il est prêt.
sAssN6	Vérifier la réutilisation des ressources d'association abandonnées.

6.2.4.7 Serveur, dispositif logique, nœud logique et modèle de données

6.2.4.7.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 5 doivent s'appliquer.

Tableau 5 – Cas d'essai positifs de serveur

Cas d'essai	Description du cas d'essai
sSrv1	Demander GetServerDirectory(LOGICAL-DEVICE) et vérifier la réponse (IEC 61850-7-2:2010, 7.2.2)
sSrv2	Pour chaque réponse GetServerDirectory(LOGICAL-DEVICE), effectuer une demande GetLogicalDeviceDirectory et vérifier la réponse (IEC 61850-7-2:2010, 9.2.1)
sSrv3	Pour chaque réponse GetLogicalDeviceDirectory, effectuer une demande GetLogicalNodeDirectory(DATA) et vérifier la réponse (IEC 61850-7-2:2010, 10.2.2)
sSrv4	Pour chaque réponse GetLogicalNodeDirectory(DATA), effectuer – une demande GetDataDirectory et vérifier la réponse (IEC 61850-7-2:2010, 11.4.4) – une demande GetDataDefinition et vérifier la réponse (IEC 61850-7-2:2010, 11.4.5) – une demande GetDataValues et vérifier la réponse (IEC 61850-7-2:2010, 11.4.2)
sSrv5	Effectuer une demande GetDataValues avec le nombre maximal de valeurs de données et vérifier la réponse
sSrv6	Pour chaque objet DATA activé en écriture, effectuer une demande SetDataValues et vérifier la réponse (IEC 61850-7-2:2010, 11.4.3)
sSrv7	Effectuer une demande SetDataValues avec le nombre maximal de valeurs de données et vérifier la réponse
sSrv8	Demander GetAllDataValues pour chaque contrainte fonctionnelle et vérifier la réponse (IEC 61850-7-2:2010, 10.2.3)
sSrv9	Evaluer la sémantique des mesures analogiques sélectionnées (V/A): – vérifier la valeur analogique (contrôle de vraisemblance, pas de précision); – vérifier les bits de qualité, provoquer des situations pour définir des bits de qualité spécifiques; – vérifier la valeur et la qualité de l'horodatage (UTC) (contrôle de vraisemblance, pas de précision); – vérifier l'échelle, la plage et les unités, modifier un réglage et vérifier la valeur obtenue; – vérifier la zone morte, modifier la zone morte et vérifier le résultat; – vérifier les indications de limite.
sSrv10	Evaluer la sémantique des points d'état sélectionnés: – vérifier la valeur d'état; – vérifier les bits de qualité, provoquer des situations pour définir des bits de qualité spécifiques; – vérifier la valeur et la qualité de l'horodatage (UTC) (contrôle de vraisemblance, pas de précision);
sSrv11	Vérifier que lorsque blkEna est défini sur true par un opérateur, le bit de qualité "oldData and operatorblocked" est défini par le serveur et les données de processus ne sont plus mises à jour; la qualité "oldData" est définie par une fonction automatique (interne) et les données de processus ne sont plus mises à jour (IEC 61850-7-3:2010, 6.2.6).

Cas d'essai	Description du cas d'essai
sSrv12	Vérifier les valeurs de Mod/Beh: "off", "test", "blocked" – Lorsque Mod/Beh vaut "off", les données de processus ne sont pas mises à jour, Mod et Beh sont mis à jour, la qualité est définie sur "invalid". – Lorsque Mod/Beh vaut "test" ou "test-blocked", la qualité des données de processus "test" est définie. – Lorsque Mod/Beh vaut "blocked", la qualité des données de processus "operatorBlocked" est définie. – (IEC 61850-7-4:2010, Annexe A)
sSrv13	Vérifier la hiérarchie des dispositifs logiques: – il convient que LLN0.GrRef fasse référence à un dispositif logique valide; – la référence ne doit pas entraîner de boucle de hiérarchie; – une valeur de Beh à un niveau supérieur influence correctement les niveaux inférieurs (c'est-à-dire que comme LD, Beh influence le comportement de LN en fonction de LN Mod).

6.2.4.7.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 6 doivent s'appliquer.

Tableau 6 – Cas d'essai négatifs de serveur

Cas d'essai	Description du cas d'essai
sSrvN1	Demander les services de données suivants avec des paramètres erronés (objet inconnu, noms de cas incohérents, dispositif logique erroné ou nœud logique erroné) et vérifier l'erreur de service "response-" – ServerDirectory(LOGICAL-DEVICE) (IEC 61850-7-2:2010, 7.2.2) – GetLogicalDeviceDirectory (IEC 61850-7-2:2010, 9.2.1) – GetLogicalNodeDirectory(DATA) (IEC 61850-7-2:2010, 10.2.2) – GetAllDataValues (IEC 61850-7-2:2010, 10.2.3) – GetDataValues (IEC 61850-7-2:2010, 11.4.2) – SetDataValues (IEC 61850-7-2:2010, 11.4.3) – GetDataDirectory (IEC 61850-7-2:2010, 11.4.4) – GetDataDefinition (IEC 61850-7-2:2010, 11.4.5)
sSrvN2	Demander SetDataValues des données ENUMERATED avec une valeur hors plage et vérifier l'erreur de service "response-" (IEC 61850-7-2:2010, 11.4.3).
sSrvN3	Demander SetDataValues avec un type de données incohérent (par exemple int-float) et vérifier l'erreur de service "response-" (IEC 61850-7-2:2010, 11.4.3).
sSrvN4	Demander SetDataValues pour des valeurs de données en lecture seule et vérifier l'erreur de service "response-" (IEC 61850-7-2:2010, 11.4.3).

6.2.4.8 Modèle d'ensemble de données

6.2.4.8.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 7 doivent s'appliquer.

Tableau 7 – Cas d'essai positifs d'ensemble de données

Cas d'essai	Description du cas d'essai
sDs1	Demander GetLogicalNodeDirectory(LOGICAL-DEVICE) et vérifier la réponse (IEC 61850-7-2:2010, 10.2.2). Pour chaque réponse, effectuer: – une demande GetDataSetValues et vérifier la réponse (IEC 61850-7-2:2010, 13.3.2); – une demande GetDataSetDirectory et vérifier la réponse (IEC 61850-7-2:2010, 13.3.6).
sDs2	Demander CreateDataSet persistant avec un membre et avec le nombre maximal de membres possible, vérifier la réponse (IEC 61850-7-2:2010, 13.3.4) et vérifier que l'ensemble de données non persistant est visible pour un autre client.
sDs3	Demander CreateDataSet non persistant avec un membre et avec le nombre maximal de membres possible, vérifier la réponse (IEC 61850-7-2:2010, 13.3.4) et vérifier que l'ensemble de données persistant n'est pas visible pour un autre client.
sDs4	Créer et supprimer un ensemble de données persistant, recréer l'ensemble de données avec le même nom et une valeur de données supplémentaire/un membre reclassé et vérifier les membres.
sDs5	Créer et supprimer un ensemble de données non persistant, recréer l'ensemble de données avec le même nom et une valeur de données supplémentaire/un membre reclassé et vérifier les membres.
sDs6	Créer un ensemble de données non persistant, libérer/interrompre l'association, effectuer l'association à nouveau et vérifier que l'ensemble de données a été supprimé (IEC 61850-7-2:2010, 13.1).
sDs7	Créer un ensemble de données non persistant, libérer/interrompre l'association, effectuer l'association à nouveau et vérifier que l'ensemble de données est toujours présent (IEC 61850-7-2:2010, 13.1).
sDs8	Créer et supprimer un ensemble de données persistant et vérifier que chaque ensemble de données peut être créé normalement: répéter une fois le processus de création et de suppression.
sDs9	Créer et supprimer un ensemble de données non persistant et vérifier que chaque ensemble de données peut être créé normalement: répéter une fois le processus de création et de suppression.
sDs10	Vérifier SetDataSetValues/GetDataSetValues avec GetDataValues et SetDataValues.
sDs11	Vérifier que le nombre maximal d'ensembles de données persistants avec le nombre maximal de membres peut être créé pour chaque nombre maximal de clients spécifié, comme spécifié.
sDs12	Vérifier que le nombre maximal d'ensembles de données non persistants avec le nombre maximal de membres peut être créé pour chaque nombre maximal de clients spécifié, comme spécifié.
sDs13	Vérifier qu'un ensemble de données non persistant peut être créé avec la longueur maximale de nom pour l'ensemble de données et un membre de l'ensemble de données (IEC 61850-7-2:2010, 22.2).
sDs14	Vérifier qu'un ensemble de données persistant peut être créé avec la longueur maximale de nom pour l'ensemble de données et un membre de l'ensemble de données (IEC 61850-7-2:2010,22.2).

6.2.4.8.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 8 doivent s'appliquer.

Tableau 8 – Cas d'essai négatifs d'ensemble de données

Cas d'essai	Description du cas d'essai
sDsN1	Demander les services d'ensemble de données suivants avec des paramètres erronés (objet inconnu, noms de cas incohérents, dispositif logique erroné ou nœud logique erroné) et vérifier l'erreur de service "response-" – GetDataSetValues (IEC 61850-7-2:2010, 13.3.2) – SetDataSetValues (IEC 61850-7-2:2010, 13.3.3) – CreateDataSet (IEC 61850-7-2:2010, 13.3.4) – DeleteDataSet (IEC 61850-7-2:2010, 13.3.5) – GetDataSetDirectory (IEC 61850-7-2:2010, 13.3.6)
sDsN2	Créer un ensemble de données persistant avec le même nom deux fois et vérifier l'erreur de service "response-"
sDsN3	Créer un ensemble de données non persistant avec le même nom deux fois et vérifier l'erreur de service "response-"
sDsN4	Continuer à créer des ensembles de données non persistants jusqu'à qu'une erreur de service "response-" correcte soit renvoyée
sDsN5	Continuer à créer des ensembles de données non persistants jusqu'à qu'une erreur de service "response-" correcte soit renvoyée
sDsN6	Créer un ensemble de données persistant avec des membres inconnus et vérifier l'erreur de service "response-"
sDsN7	Créer un ensemble de données non persistant avec des membres inconnus et vérifier l'erreur de service "response-"
sDsN8	Supprimer un ensemble de données (prédéfini) impossible à supprimer et vérifier l'erreur de service "response-"
sDsN9	Supprimer un ensemble de données persistant deux fois et vérifier l'erreur de service "response-"
sDsN10	Supprimer un ensemble de données non persistant deux fois et vérifier l'erreur de service "response-"
sDsN11	Supprimer un ensemble de données persistant référencé par classe de commande (rapport) et vérifier l'erreur de service "response-" (IEC 61850-7-2:2010, 13.1)
sDsN12	Supprimer un ensemble de données non persistant référencé par classe de commande (rapport) et vérifier l'erreur de service "response-" (IEC 61850-7-2:2010, 13.1)
sDsN13	Demander SetDataSetValues avec un ensemble de données avec un ou plusieurs membres en lecture seule et vérifier l'erreur de service "response-"

6.2.4.9 Modèle de substitution – Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 9 doivent s'appliquer.

Tableau 9 – Cas d'essai positifs de substitution

Cas d'essai	Description du cas d'essai
sSub1	Désactiver subEna et définir subVal, subMag, subCMag, subQ, subID et vérifier que les valeurs substituées ne sont pas transmises lorsque subEna est désactivé et sont transmises lorsque subEna est activé (IEC 61850-7-3:2010, Tableau 64)
sSub2	Vérifier qu'en cas d'échec de l'association, les valeurs substituées doivent rester inchangées.
sSub3	Vérifier que le réglage de subVal, subMag, subCMag, subQ et subID est admis, que les valeurs substituées sont transmises et que Quality.Source est défini sur Substituted lorsque subEna est activé.

6.2.4.10 Modèle de reporting non mis en mémoire tampon

6.2.4.10.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 10 doivent s'appliquer.

Tableau 10 – Cas d'essai positifs de reporting non mis en mémoire tampon

Cas d'essai	Description du cas d'essai
sRpt1	Demander GetLogicalNodeDirectory(URCB) et vérifier la réponse Demander GetURCBValues de tous les URCB avec réponse
sRpt2	Vérifier le reporting des champs facultatifs d'un URCB Configurer/activer un URCB avec toutes les combinaisons de champs facultatifs: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name et/ou data-reference (IEC 61850-7-2:2010, 17.2.3.2.2.1), provoquer/déclencher un rapport et vérifier que le rapport contient les champs facultatifs activés
sRpt3	Vérifier les conditions de déclenchement d'un URCB Configurer et activer un URCB avec les champs facultatifs: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow et entryID, puis vérifier que les rapports sont transmis conformément aux conditions de déclenchement (prises en charge) suivantes: • en cas d'intégrité; • en cas de mise à jour (dupd); • en cas de mise à jour avec intégrité; • en cas de modification de données (dchg); • en cas de modification de données et de qualité; • en cas de modification de données et de qualité avec période d'intégrité. Vérifier la validité du ReasonCode (IEC 61850-7-2:2010,17.2.3.2.2.9) Vérifier que si davantage de conditions de déclenchement sont possibles, un seul rapport est généré, de préférence (IEC 61850-7-2:2010,17.2.3.2.3.2) Vérifier que les rapports sont envoyés uniquement lorsque RptEna est défini sur True (IEC 61850-7-2:2010, 17.2.2.5); lorsque le reporting est désactivé, il convient qu'aucun rapport ne soit transmis
sRpt4	Interrogation générale (IEC 61850-7-2:2010,17.2.2.13) Le paramétrage de l'attribut GI d'un URCB doit lancer le processus general-interrogation (interrogation générale). Un rapport avec les valeurs de données actuelles sera envoyé. Après lancement de general-interrogation, l'attribut GI est réinitialisé sur False.
sRpt5	Segmentation des rapports Vérifier que si un long rapport ne s'intègre pas dans un message, le rapport est divisé en sous-rapports. Activer les champs facultatifs sequence-number et report-time-stamp et vérifier la validité de: (IEC 61850-7-2:2010, 17.2.3.2.2.5) – SeqNum (non modifié) – SubSeqNum (0 pour premier rapport, incrementing, roll-over) – MoreSeqmentsFollow – TimeOfEntry (non modifié, car SeqNum n'est pas modifié) (IEC 61850-7-2:2010,17.2.3.2.2.9) Vérifier qu'une mise à jour d'une valeur de données pendant l'envoi d'un rapport segmenté causé par un déclenchement "integrity" ou "general-interrogation" peut être interrompue par un rapport, en modifiant l'une des valeurs de données avec un nouveau numéro de séquence (IEC 61850-7-2:2010, 17.2.3.2.3.5) Une nouvelle demande pour general-interrogation doit arrêter l'envoi des segments restants du rapport GI encore en cours. Un nouveau rapport GI doit commencer avec un nouveau numéro de séquence et le numéro de sous-séquence doit être 0 (IEC 61850-7-2:2010, 17.2.3.2.3.4)

Cas d'essai	Description du cas d'essai
sRpt6	Révision de configuration (IEC 61850-7-2:2010, 17.2.2.7) Vérifier que ConfRev représente un décompte du nombre de fois où la configuration de l'ensemble de données référencé par DatSet a été modifiée. Modifications décomptées: • suppression d'un membre du data-set (ensemble de données) • reclassement des membres du data-set Vérifier qu'après un redémarrage du serveur, la valeur de ConfRev est restaurée à sa valeur d'origine de la configuration locale de base OU la valeur est conservée à partir de la configuration antérieure au redémarrage (PIXIT) Vérifier que le serveur incrémente ConfRev dans le cas où les ensembles de données varient en raison du traitement des services ACSI Il convient que ConfRev ne soit jamais égal à 0 (zéro) dans le cas où DatSet n'est pas nul.
sRpt7	Vérifier qu'après un redémarrage du serveur, la valeur de ConRev est restaurée à sa valeur d'origine de la configuration locale de base OU la valeur est conservée à partir de la configuration antérieure au redémarrage (PIXIT).
sRpt8	Buffer Time (IEC 61850-7-2:2010,17.2.2.9) Vérifier que, dans le cas où une seconde notification interne du même membre d'un DATA-SET s'est produite avant l'expiration de BufTm, le serveur: (IEC 61850-7-2:2010, 17.2.2.9) • doit, pour les informations d'état, se comporter comme si BufTm avait expiré et envoyer immédiatement le rapport, relancer le temporisateur avec la valeur BufTm et traiter la seconde notification; ou • peut, pour des informations analogiques, se comporter comme si BufTm avait expiré et transmettre immédiatement le rapport pour transmission, relancer le temporisateur avec la valeur BufTm et traiter la seconde notification; ou • peut, pour des informations analogiques, remplacer la valeur actuelle dans le rapport en attente par la nouvelle. Configurer "Buffer Time" sur 1 000 ms et forcer une modification de valeur de données de membres "dataset" multiples dans le "buffer time" (temps de mémoire tampon). Il convient que le serveur n'envoie pas plus d'un rapport par "buffer time" avec toutes les modifications des valeurs de données depuis le dernier rapport. Vérifier que la valeur 0 pour "buffer time" indique que l'attribut "buffer time" n'est pas utilisé. (IEC 61850-7-2:2010, 17.2.2.9) Vérifier que la valeur "BufTm" peut contenir au moins la valeur 3 600 0000 (= 1 h en ms)
sRpt9	Vérifier que le DUT peut envoyer des rapports avec des objets de données
sRpt10	Vérifier que le DUT peut envoyer des rapports avec des attributs de données
sRpt11	Vérifier que le DUT peut envoyer tout événement mis en mémoire tampon avant le rapport d'intégrité
sRpt12	Vérifier que lorsque la valeur de LLN0 Behavior est Off ou On/Blocked, il convient que plus aucun rapport de modification de données/de qualité ne soit transmis pour les valeurs de processus dans ce dispositif logique (IEC 61850-7-4:2010, Annexe A)
sRpt13	Vérifier que le serveur définit URCB Owner sur une valeur différente de NULL lorsque l'URCB est configuré par un client et que la valeur est réinitialisée à NULL lorsqu'un client libère l'URCB
sRpt14	Vérifier que le DUT peut traiter un URCB avec la longueur maximale de nom pour RptID et Dataset. (IEC 61850-7-2:2010, 22.2)

6.2.4.10.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 11 doivent s'appliquer.

Tableau 11 – Cas d'essai négatifs de reporting non mis en mémoire tampon

Cas d'essai	Description du cas d'essai
sRpN1	Demander GetURCBValues avec des paramètres erronés et vérifier les erreurs de service "response-" (IEC 61850-7-2:2010,17.2.5.3)
sRpN2	Configurer le reporting avec l'option de déclenchement GI (pas dchg, qchg, dupd, integrity). Lorsque cette option est activée, seuls les rapports GI sont transmis. Il convient qu'aucun rapport ne soit envoyé lors de la génération des événements (IEC 61850-7-2:2010, 17.2.5.3)
sRpN3	Le paramétrage de la période d'intégrité (integrity period) sur 0 avec TrgOps = integrity aura pour résultat l'envoi d'aucun rapport d'intégrité (IEC 61850-7-2:2010, 17.2.2.12)
sRpN4	Configuration incorrecte d'un URCB: configurer lorsqu'activé, configurer ConfRev et SqNum et configurer avec ensemble de données inconnu
sRpN5	Utilisation exclusive d'URCB et association perdue Configurer un URCB et définir l'attribut Resv, puis l'activer. Vérifier qu'un autre client ne peut pas définir d'attribut de cet URCB (IEC 61850-7-2:2010, 17.2.4.5)
sRpN6	Configurer des options URCB non prises en charge (PIXIT) Configurer des conditions de déclenchement non prises en charge, des champs facultatifs et des paramètres liés
sRpN7	Vérifier qu'un autre client ne peut pas configurer un URCB préattribué
sRpN8	Vérifier que lorsque TrgOps – GI n'est pas défini, la demande de définition de GI sur true doit échouer

6.2.4.11 Modèle de reporting mis en mémoire tampon

6.2.4.11.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 12 doivent s'appliquer.

Tableau 12 – Cas d'essai positifs de reporting mis en mémoire tampon

Cas d'essai	Description du cas d'essai
sBr1	Demander GetLogicalNodeDirectory(BRCB) et vérifier la réponse Demander GetBRCBValues de tous les BRCB avec réponse
sBr2	Vérifier le reporting des champs facultatifs d'un BRCB Configurer/activer un BRCB avec toutes les combinaisons de champs facultatifs: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow et/ou entryID (IEC 61850-7-2:2010, 17.2.3.2.2.1), provoquer/déclencher un rapport et vérifier que le rapport contient les champs facultatifs activés

Cas d'essai	Description du cas d'essai
sBr3	Vérifier les conditions de déclenchement d'un BRCB Configurer et activer un BRCB avec les champs facultatifs: sequence-number, report-time-stamp, reason-for-inclusion, data-set-name, data-reference, buffer-overflow et entryID, puis vérifier que les rapports sont transmis conformément aux conditions de déclenchement (prises en charge) suivantes: • en cas d'intégrité; • en cas de mise à jour (dupd); • en cas de mise à jour avec intégrité; • en cas de modification de données (dchg); • en cas de modification de données et de qualité; • en cas de modification de données et de qualité avec période d'intégrité. Vérifier la validité du ReasonCode (IEC 61850-7-2:2010, 17.2.3.2.2.9) Vérifier que si davantage de conditions de déclenchement sont possibles, un seul rapport est généré, de préférence (IEC 61850-7-2:2010, 17.2.3.2.3.2) Vérifier que les rapports sont envoyés uniquement lorsque RptEna est défini sur True (IEC 61850-7-2:2010, 17.2.2.5); lorsque le reporting est désactivé, il convient qu'aucun rapport ne soit transmis.
sBr4	Interrogation générale (IEC 61850-7-2:2010,17.2.2.13) Le paramétrage de l'attribut GI d'un BRCB doit lancer le processus general-interrogation. Un rapport avec les valeurs de données actuelles sera envoyé. Après lancement de general-interrogation, l'attribut GI est réinitialisé sur False.
sBr5	Segmentation des rapports Vérifier que si un long rapport ne s'intègre pas dans un message, le rapport est divisé en sous-rapports. Activer les champs facultatifs sequence-number et report-time-stamp et vérifier la validité de: (IEC 61850-7-2:2010, 17.2.3.2.2.5) – SqNum (non modifié) – SubSqNum (0 pour premier rapport, incrementing, roll-over) – MoreSeqmentsFollow – TimeOfEntry (non modifié car SqNum n'est pas modifié) (IEC 61850-7-2:2010, 17.2.3.2.2.9) Vérifier qu'une mise à jour d'une valeur de données pendant l'envoi d'un rapport segmenté causé par un déclenchement "integrity" ou "general-interrogation" peut être interrompue par un rapport, en modifiant l'une des valeurs de données avec un nouveau numéro de séquence (IEC 61850-7-2:2010, 17.2.3.2.3.5) Une nouvelle demande pour general-interrogation doit arrêter l'envoi des segments restants du rapport GI encore en cours. Un nouveau rapport GI doit commencer avec un nouveau numéro de séquence et le numéro de sous-séquence doit être 0 (IEC 61850-7-2:2010, 17.2.3.2.3.4) Vérifier que lorsque OptFlds=sequence-number n'est PAS défini, SubSqNum et SqNum ne sont pas présents dans les sous-rapports (17.2.3.2.2.4, 17.2.3.2.2.5)
sBr6	Révision de configuration (IEC 61850-7-2:2010, 17.2.2.7) Vérifier que ConfRev représente un décompte du nombre de fois où la configuration de l'ensemble de données référencé par DatSet a été modifiée. Modifications décomptées: • suppression d'un membre du data-set (ensemble de données) • reclassement des membres du data-set Vérifier qu'après un redémarrage du serveur, la valeur de ConfRev est restaurée à sa valeur d'origine de la configuration locale de base OU la valeur est conservée à partir de la configuration antérieure au redémarrage (PICS) Vérifier que le serveur incrémente ConfRev dans le cas où les ensembles de données varient en raison du traitement des services ACSI Il convient que ConfRev ne soit jamais égal à 0 (zéro) dans le cas où DatSet n'est pas nul
sBr7	Vérifier qu'après un redémarrage du serveur, la valeur de ConRev est restaurée à sa valeur d'origine de la configuration locale de base OU la valeur est conservée à partir de la configuration antérieure au redémarrage (PIXIT)

Cas d'essai	Description du cas d'essai
sBr8	Buffer Time (IEC 61850-7-2:2010, 17.2.2.9) Vérifier que, dans le cas où une seconde notification interne du même membre d'un DATA-SET s'est produite avant l'expiration de BufTm, le serveur: (IEC 61850-7-2:2010, 17.2.2.9) • doit, pour les informations d'état, se comporter comme si BufTm avait expiré et envoyer immédiatement le rapport, relancer le temporisateur avec la valeur BufTm et traiter la seconde notification; ou • peut, pour des informations analogiques, se comporter comme si BufTm avait expiré et transmettre immédiatement le rapport pour transmission, relancer le temporisateur avec la valeur BufTm et traiter la seconde notification; ou • peut, pour des informations analogiques, remplacer la valeur actuelle dans le rapport en attente par la nouvelle. Configurer "Buffer Time" sur 1 000 ms et forcer une modification de valeur de données de membres "dataset" multiples dans le "buffer time". Il convient que le serveur n'envoie pas plus d'un rapport par "buffer time" avec toutes les modifications des valeurs de données depuis le dernier rapport. Vérifier que la valeur 0 pour "buffer time" indique que l'attribut "buffer time" n'est pas utilisé (IEC 61850-7-2:2010, 17.2.2.9) Vérifier que la valeur "BufTm" peut contenir au moins la valeur 3 600 0000 (= 1 h en ms)
sBr9	Vérifier que le DUT peut envoyer des rapports avec des objets de données
sBr10	Vérifier que le DUT peut envoyer des rapports avec des attributs de données
sBr11	Vérifier que tous les événements mis en mémoire tampon doivent être envoyés avant que les rapports d'intégrité puissent être envoyés (IEC 61850-7-2:2010, 17.2.3.2.3.3)
sBr12	Vérifier que tous les événements mis en mémoire tampon doivent être envoyés avant que le rapport GI puisse être envoyé (IEC 61850-7-2:2010, 17.2.3.2.3.4)
sBr13	Vérifier que le serveur définit BRCB Owner sur une valeur différente de NULL lorsque le BRCB est configuré par un client et que la valeur est réinitialisée à NULL lorsqu'un client libère le BRCB. En cas de BRCB préattribué, le serveur réinitialise le propriétaire à l'adresse client préattribuée.
sBr14	Vérifier que le DUT peut traiter un BRCB avec la longueur maximale de nom pour RptID et DatSet (IEC 61850-7-2:2010, 22.2)
sBr20	Machine à états de reporting mis en mémoire tampon (BRCB) (IEC 61850-7-2:2010, 17.2.2.5, Figure 24) – Vérifier que les événements sont mis en mémoire tampon après la libération de l'association – Vérifier que le reporting est désactivé après la perte de l'association – Vérifier que les rapports non reçus tant que non associés sont maintenant reçus dans l'ordre correct (SOE) (IEC 61850-7-2:2010, 17.2.1, IEC 61850-7-2:2010, 17.2.2.5) – Procéder de même, mais définir PurgeBuf sur True avant d'activer le reporting. Il convient d'envoyer les rapports mis en mémoire tampon non stockés (IEC 61850-7-2:2010, 17.2.2.14) – Vérifier qu'après modification de DatSet, la mémoire tampon du rapport est purgée (IEC 61850-7-2:2010, 17.2.2.5) Provoquer un dépassement de mémoire tampon; il convient que le champ facultatif "buffer overflow" soit défini dans le premier rapport qui est envoyé avec les événements qui se sont produits après le dépassement (IEC 61850-7-2:2010, 17 2.3.2.2.8)
sBr21	Reporting mis en mémoire tampon (BRCB); événements de mise en mémoire tampon (IEC 61850-7-2:2010, 17.2.3.2.3.6) Vérifier que lorsque l'association est à nouveau disponible et que le client a défini EntryID et activé le BRCB, le BRCB doit commencer à envoyer les rapports d'événements mis en mémoire tampon. Le BRCB doit utiliser les numéros de séquence et de sous-séquence de manière à empêcher toute discontinuité.
sBr22	Vérifier que les rapports d'intégrité sont mis en mémoire tampon

Cas d'essai	Description du cas d'essai
sBr23	Vérifier le comportement satisfaisant de ResvTms • A ResvTms = –1, le BRCB peut être utilisé par le client configuré • A ResvTms = 0, un client peut réserver le BRCB en inscrivant une valeur et configurer le BRCB • A la perte de l'association, le BRCB réservé est libéré après le nombre ResvTms de secondes (ResvTms défini sur zéro) A la perte de l'association, aucun des autres clients ne peut réserver le BRCB dans le délai ResvTms, sauf celui qui l'avait réservé à l'origine (le client restaure l'association)
sBr24	Vérifier que pour définir ResvTms, une demande SetBRCBValues doit: • générer une réponse négative si la valeur ResvTms du BRCB est –1; • générer une réponse négative si la valeur ResvTms du BRCB est différente de zéro et si la demande SetBRCBValues est émise par un autre client pour lequel le BRCB n'est pas réservé; • générer une réponse négative si la valeur ResvTms à définir est négative.
sBr25	Vérifier qu'une modification de l'un des paramètres BRCB suivants purge la mémoire tampon: RptID, BufTm, TrgOps, IntgPd, DatSet. Il convient qu'une modification de OptFlds ne purge pas la mémoire tampon (IEC 61850-7-2:2010, 17.2.2.5)
sBr26	Vérifier qu'après avoir défini un EntryID non valide, nul ou non existant, le DUT envoie tous les rapports dans la mémoire tampon
sBr27	Vérifier que lorsque l'état du BRCB est RptEna=FALSE, GetBRCBValues doit renvoyer la valeur EntryID qui représente la dernière entrée (la plus récente) à avoir été mise en mémoire tampon. Lorsque RptEna=TRUE: la valeur EntryID renvoyée dans une réponse GetBRCBValues doit être l'EntryID du dernier EntryID formaté et mis en file d'attente pour transmission.
sBr28	Vérifier que seul le dernier rapport GI mis en mémoire tampon est transmis après une resynchronisation.

6.2.4.11.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 13 doivent s'appliquer.

Tableau 13 – Cas d'essai négatifs de reporting mis en mémoire tampon

Cas d'essai	Description du cas d'essai
sBrN1	Demander GetBRCBValues avec des paramètres erronés et vérifier les erreurs de service "response-" (IEC 61850-7-2:2010, 17.2.3.3.2)
sBrN2	Configurer le reporting avec l'option de déclenchement GI (pas dchg, qchg, dupd, integrity). Lorsque cette option est activée, seuls les rapports GI sont transmis. Il convient qu'aucun rapport ne soit envoyé lors de la génération des événements (IEC 61850-7-2:2010, 17.2.3.2.2.4)
sBrN3	Le paramétrage de la période d'intégrité (integrity period) sur 0 avec TrgOps = integrity aura pour résultat l'envoi d'aucun rapport d'intégrité (IEC 61850-7-2:2010, 17.2.2.11)
sBrN4	Configuration incorrecte d'un BRCB: configurer lorsqu'activé, configurer ConfRev et SqNum et configurer avec ensemble de données inconnu
sBrN5	Utilisation exclusive de BRCB et association perdue Configurer un BRCB et l'activer. Vérifier qu'un autre client ne peut pas définir de valeur d'attribut dans ce BRCB (IEC 61850-7-2:2010, 17.2.1)
sBrN6	Configurer des options BRCB non prises en charge (PIXIT) Configurer des conditions de déclenchement non prises en charge, des champs facultatifs et des paramètres liés
sBrN7	Vérifier qu'un autre client ne peut pas configurer un BRCB préattribué
sBrN8	Vérifier que lorsque TrgOps – GI n'est pas défini, le dispositif n'envoie pas de rapports avec le motif GI

6.2.4.12 Modèle de journal

6.2.4.12.1 Cas d'essai positifs

Les cas d'essais répertoriés dans le Tableau 14 doivent s'appliquer.

Tableau 14 – Cas d'essai positifs de journal

Cas d'essai	Description du cas d'essai
sLog1	Demander GetLogicalNodeDirectory(LOG) et vérifier "response+"
sLog2	Demander GetLogicalNodeDirectory(LCB) et vérifier "response+"
sLog3	Demander GetLCBValues avec contrainte fonctionnelle LG de tous les LCB avec réponse
sLog4	Demander SetLCBValues avec contrainte fonctionnelle LG lorsque LCB est désactivé
sLog5	Vérifier que la journalisation est indépendante d'un ensemble limité d'associations d'applications externes ou d'autres transactions de communication
sLog6	Configurer et activer la journalisation et vérifier que les conditions de déclenchement de journalisation suivantes placent une entrée correcte dans le journal avec les membres corrects de l'ensemble de données – en cas d'intégrité; – en cas de mise à jour (dupd); – en cas de mise à jour avec intégrité; – en cas de modification de données (dchg); – en cas de modification de qualité (qchg); – en cas de modification de données et de qualité; – en cas de modification de données et de qualité avec période d'intégrité.
sLog7	Demander QueryLogByTime et vérifier "response+"
sLog8	Demander QueryLogByEntry et vérifier "response+"
sLog9	Demander GetLogStatusValues et vérifier "response+", vérifier que les entrées avec réponses indiquent l'entrée ID/time la plus ancienne/la plus récente dans le journal
sLog10	Vérifier que les données sont consignées comme défini dans les paramètres du nœud logique GLOG. Le motif correspondant doit être "application-trigger"
sLog11	Vérifier que le serveur peut traiter un LCB et un LOG avec la longueur maximale de nom pour LCBRef, LogRef et DatSet (IEC 61850-7-2:2010, 22.2)
sLog12	Vérifier que les entrées de journal sont volatiles et qu'elles ne sont pas perdues après réinitialisation et perte d'alimentation

6.2.4.12.2 Cas d'essai négatifs

Les cas d'essais répertoriés dans le Tableau 15 doivent s'appliquer.

Tableau 15 – Cas d'essai négatifs de journal

Cas d'essai	Description du cas d'essai
sLogN1	Demander les services de journal suivants avec des paramètres erronés (entrées en dehors de la plage ou Dataset, LCB ou Log inexistant) et vérifier l'erreur de service "response-" – GetLCBValues (IEC 61850-7-2:2010, 17.3.2.5) – SetLCBValues (IEC 61850-7-2:2010, 17.3.2.6) – QueryLogByTime (IEC 61850-7-2:2010, 17.3.5.2) – QueryLogAfter (IEC 61850-7-2:2010, 17.3.5.3) – GetLogStatusValues (IEC 61850-7-2:2010, 17.3.5.4)
sLogN2	Demander SetLCBValues avec contrainte fonctionnelle LG lorsque LCB est activé et vérifier l'erreur de service "response-"

6.2.4.13 Modèles de commande

6.2.4.13.1 Généralités

L'essai qui porte sur les modèles de commande a été divisé en un essai général et en une liste de cas d'essai pour les modèles de commande spécifiques. Les cas d'essai généraux sont les suivants.

6.2.4.13.2 Cas d'essai généraux pour les modèles de commande

Les cas d'essais répertoriés dans le Tableau 16 doivent s'appliquer.

Tableau 16 – Cas d'essai des modèles de commande

Cas d'essai	Description du cas d'essai
sCtl1	Forcer et vérifier chaque chemin de la machine à états de commande pour plusieurs objets de commande avec modèles de commande • direct with normal security (directe avec sécurité normale) (IEC 61850-7-2:2010, 20.2.1) • SBO-control with normal security (commande SBO avec sécurité normale) (IEC 61850-7-2:2010, 20.2.2) • direct with enhanced security (directe avec sécurité renforcée) (IEC 61850-7-2:2010, 20.3.2) • SBO-control with enhanced security (commande SBO avec sécurité renforcée) (IEC 61850-7-2:2010, 20.3.3) Comparer les cas d'essais décrits pour chaque modèle de commande
sCtl2	Modifier le modèle de commande en utilisant les services en ligne et vérifier que l'objet de commande répond conformément au nouveau modèle de commande
sCtl3	"Time Operate" un deuxième objet de commande de sécurité renforcée avant le temps d'activation pour le premier objet de commande (PIXIT)
sCtl4	Vérifier que la valeur de l'attribut stSeld est définie/réinitialisée comme spécifié dans les machines à états
sCtl5	Vérifier le fanion "test" dans selectwithvalue/operate et que Beh = test (IEC 61850-7-4:2010, Annexe A, Tableau A.1) • Lorsque le LN Beh est "on", les demandes de commande sont rejetées avec AddCause "Blocked-by-mode" • Lorsque le LN Beh est "test/blocked", les demandes de commande sont acceptées • Lorsque le LN Beh est "test", les demandes de commande sont acceptées
sCtl6	Sélectionner tous les objets de commande SBO et les annuler dans l'ordre inverse. Dans le cas où une action de commande est bloquée parce qu'une autre commande est déjà en cours d'exécution, AddCause doit être "1-of-n-control"

Cas d'essai	Description du cas d'essai
sCtl7	Vérifier que les vérifications spécifiées sont effectuées dans des conditions de verrouillage ou de contrôle de synchronisme et que la commande est exécutée en conséquence (IEC 61850-7-2:2010, 20.5.2.7) • Lorsque le contrôle de verrouillage échoue avec AddCause "Blocked-by-interlocking" • Lorsque le contrôle de verrouillage réussit • Lorsque le contrôle de synchronisme échoue avec AddCause "Blocked-by-synchrocheck" • Lorsque le contrôle de synchronisme réussit
sCtl8	Activer (sans sélectionner) un objet de commande SBO et vérifier que la demande est rejetée avec AddCause "Object-not-selected" (IEC 61850-7-2:2010, Tableau 54)
sCtl9	Sélectionner le même objet de commande deux fois, vérifier que la deuxième demande "select" est rejetée avec AddCause "Object-already-selected" (IEC 61850-7-2:2010, Tableau 54) et que l'objet reste à l'état "selected" (Operate.req est accepté)
sCtl10	La valeur de commande "Operate" est identique à la valeur d'état réelle (On-On ou Off-Off), et vérifier que la demande de commande est rejetée avec AddCause "Position-reached" (IEC 61850-7-2:2010, Tableau 54, PIXIT)
sCtl11	Sélectionner le même objet de commande à partir de 2 clients différents. Vérifier que les demandes de commande du deuxième client sont rejetées avec AddCause "Locked-by-other-client" (IEC 61850-7-2:2010, Tableau 54)
sCtl12	Sélectionner/activer un objet de commande inconnu et vérifier que les demandes de commandes sont rejetées avec AddCause "unknown" (IEC 61850-7-2:2010, Tableau 54)
sCtl13	Vérifier que la demande Select sur un objet de commande "direct operate" est rejetée avec AddCause "Unknown" (IEC 61850-7-2:2010, Tableau 54)
sCtl14	Activer le même objet de commande direct deux fois à partir de 2 clients (IEC 61850-7-2:2010, Tableau 54, PIXIT) et vérifier que la dernière demande de commande est rejetée avec AddCause "Command-already-in-execution"
sCtl15	Vérifier que la demande SBOes Operate ou Cancel avec des paramètres de commande différents de SelectWithValue est rejetée avec AddCause: "Inconsistent-parameters"
sCtl16	Vérifier que lorsque Loc est défini, les demandes de commande à distance sont rejetées avec AddCause "Blocked-by-switching-hierarchy"
sCtl17	Vérifier qu'en cas de droits au niveau de la centrale (LocSta=T), les demandes de commande à distance sont rejetées avec AddCause "Blocked-by-switching-hierarchy"
sCtl18	Vérifier que lorsque CmdBlk.stVal est défini, les demandes de commande sont rejetées avec AddCause "Blocked-by-command" (IEC 61850-7-2:2010, Tableau 54)
sCtl19	Vérifier que lorsque blkEna est défini, les demandes de commande sont interrompues/rejetées avec AddCause "Time-limit-over"
sCtl20	Vérifier que lorsque les paramètres sont modifiés après la réponse "select", la demande "operate" est rejetée avec AddCause "Parameter-change-in-execution" (IEC 61850-7-2:2010, Tableau 54)
sCtl21	Vérifier que lorsque le changeur de prise a atteint la limite (EndPosR ou EndPosL dans YLTC), les demandes de commande sont rejetées avec AddCause "Step-limit" (IEC 61850-7-2:2010, Tableau 54)
sCtl22	Vérifier que les demandes de commande avec des droits d'accès insuffisants sont rejetées avec AddCause "No-access-authority" (IEC 61850-7-2:2010, Tableau 54)
sCtl23	Vérifier que lorsque la position finale d'une action de commande APC est en dépassement, la commande s'arrête avec AddCause "Ended-with-overshoot" (IEC 61850-7-2:2010, Tableau 47)
sCtl24	Vérifier que lorsqu'une action de commande APC est interrompue en raison d'un écart entre la valeur de commande et la valeur mesurée, la commande s'arrête avec AddCause "Abortion-due-to-deviation" (IEC 61850-7-2:2010, Tableau 47)
sCtl25	Vérifier qu'une demande "cancel" a abouti lorsque l'objet de commande est à l'état "unselected" (IEC 61850-7-2:2010, Tableau 47)
sCtl26	Vérifier que lorsque l'objet de commande est à l'état WaitForExecution, la demande "cancel" ou "SelectWithValue" est rejetée avec AddCause "Command-already-in-execution" (IEC 61850-7-2:2010, Tableau 54)
sCtl27	Vérifier que la demande SelectWithValue sur un objet de commande SBOns est rejetée avec Addcause "Unknown" (IEC 61850-7-2:2010, Tableau 54)
sCtl28	Vérifier que le DUT peut contrôler un objet avec la longueur maximale de nom pour IED et Logical Device (IEC 61850-7-2:2010,22.2)

L'essai qui porte sur les modèles de commande spécifiques a été divisé en quatre modèles de commande possibles pouvant être implémentés:

a) commande directe avec sécurité normale (DOns);

b) commande SBO avec sécurité normale (SBOns);

c) commande directe avec sécurité renforcée (DOes);

d) commande SBO avec sécurité renforcée (SBOes).

6.2.4.13.3 Cas d'essai spécifiques pour les modèles de commande

Les cas d'essais répertoriés dans le Tableau 17, le Tableau 18, le Tableau 19 et le Tableau 20 doivent s'appliquer.

Tableau 17 – Cas d'essai DOns

Cas d'essai	Description du cas d'essai
sDOns1	Envoyer une demande "Operate" correcte
sDOns2	Envoyer une demande "Operate" entraînant "Test not ok"
sDOns3	Envoyer une demande "TimeActivatedOperate" entraînant "respond-"
sDOns4	Envoyer une demande "TimeActivatedOperate" correcte Vérifier "TimeActivatedOperateTermination+"
sDOns5	Envoyer une demande "TimeActivatedOperate" Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Ready" et vérifier "TimeActivatedOperateTermination-": – provoquer "Test not ok" – envoyer une demande "Cancel" correcte

Tableau 18 – Cas d'essai SBOns

Cas d'essai	Description du cas d'essai
sSBOns1	Envoyer une demande "Select" correcte Envoyer une demande "Operate" correcte
sSBOns2	Envoyer une demande "Select" correcte Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Unselected": – envoyer une demande "Cancel" correcte – attendre la temporisation – association perdue – envoyer une demande "Release" – envoyer une demande "Operate" entraînant "Test not ok"
sSBOns3	Envoyer une demande "Select" correcte – Envoyer une demande "TimeActivatedOperate" incorrecte entraînant "respond-"
sSBOns4	Envoyer une demande "Select" correcte Envoyer une demande "TimeActivatedOperate" correcte, ce qui permet de garantir que le dispositif générera "test Ok" Vérifier "TimeActivatedOperateTermination+"

Cas d'essai	Description du cas d'essai
sSBOns5	Envoyer une demande "Select" correcte Envoyer une demande "TimeActivatedOperate" correcte Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Ready" et vérifier "TimeActivatedOperateTermination-": – provoquer un essai "Test not ok" – envoyer une demande "Cancel" correcte
sSBOns6	Envoyer une demande "Select" correcte entraînant "respond-" Vérifier que chaque dispositif repasse à l'état "Unselected"
sSBOns7	Envoyer une demande "Select" correcte Vérifier que l'envoi de demandes "Operate Many" multiples fera repasser le dispositif à l'état "Ready" Vérifier que l'envoi d'une demande "Cancel" fera repasser le dispositif à l'état "Unselected"

Tableau 19 – Cas d'essai DOes

Cas d'essai	Description du cas d'essai
sDOes1	Envoyer une demande "Operate" correcte Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Ready" et vérifier "CommandTermination": – forcer le passage du simulateur d'équipement au nouvel état demandé – forcer le maintien de l'ancien état du simulateur d'équipement (AddCause: Time-limit-over ou Invalid-position) – forcer le passage du simulateur d'équipement à l'état "between" (AddCause: Invalid-position)
sDOes2	Envoyer une demande "Operate", ce qui permet de garantir que le dispositif générera "Test not Ok"
sDOes3	Envoyer une demande "TimeActivated Operate"entraînant "respond-"
sDOes4	Envoyer une demande "TimeActivated Operate" correcte Vérifier "TimeActivatedOperateTermination+" Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Ready" et vérifier "CommandTermination": – forcer le passage du simulateur d'équipement au nouvel état demandé – forcer le maintien de l'ancien état du simulateur d'équipement (AddCause: Time-limit-over) – forcer le passage du simulateur d'équipement à l'état "between" (AddCause: Invalid-position)
sDOes5	Envoyer une demande "TimeActivated Operate" correcte Vérifier "TimeActivatedOperateTermination+" Vérifier que chacun de ces chemins fera repasser le dispositif à l'état "Ready" et vérifier "TimeActivatedOperateTermination": – provoquer "Test not ok" – Envoyer une demande "Cancel" correcte