

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Communication networks and systems for power utility automation –
Part 10: Conformance testing**

**Réseaux et systèmes de communication pour l'automatisation des systèmes
électriques –
Partie 10: Essais de conformité**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2012 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Communication networks and systems for power utility automation –
Part 10: Conformance testing**

**Réseaux et systèmes de communication pour l'automatisation des systèmes
électriques –
Partie 10: Essais de conformité**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.200

ISBN 978-2-83220-557-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	12
5 Introduction to conformance testing	13
5.1 General	13
5.2 Conformance test procedures.....	14
5.3 Quality assurance and testing	14
5.3.1 General	14
5.3.2 Quality plan	15
5.4 Testing	16
5.4.1 General	16
5.4.2 Use of SCL files.....	17
5.4.3 Device testing.....	17
5.5 Documentation of conformance test report	18
6 Device related conformance testing	19
6.1 Test methodology.....	19
6.2 Conformance test procedures.....	19
6.2.1 General	19
6.2.2 Test procedure requirements	19
6.2.3 Test structure	20
6.2.4 Test cases to test a server device	20
6.2.5 Test cases to test a client device	44
6.2.6 Test cases to test sampled values device	60
6.2.7 Acceptance criteria	65
7 Tool related conformance testing	65
7.1 General guidelines	65
7.1.1 Test methodology	65
7.1.2 Test system architecture.....	66
7.2 Conformance test procedures.....	66
7.2.1 General	66
7.2.2 Test procedure requirements	66
7.2.3 Test structure	66
7.2.4 Test cases to test an IED configurator tool	66
7.2.5 Test cases to test a system configurator tool	68
7.2.6 Acceptance criteria	73
8 Performance tests	73
8.1 General	73
8.2 Communications latency.....	74
8.2.1 Application domain	74
8.2.2 Methodology.....	74
8.2.3 GOOSE performance test	75
8.3 Time synchronisation and accuracy.....	75

8.3.1	Application domain	79
8.3.2	Methodology.....	79
8.3.3	Testing criteria	80
8.3.4	Performance.....	81
9	Additional tests.....	81
Annex A (informative) Examples of test procedure template.....		82
Bibliography.....		83
Figure 1 – Conceptual conformance assessment process		17
Figure 2 – Test procedure format.....		20
Figure 3 – Test system architecture to test a server device		21
Figure 4 – Test system architecture to test a client device		44
Figure 5 – Test system architecture to test a sampled values publishing device.....		60
Figure 6 – Test system architecture to test a sampled values subscribing device.....		61
Figure 7 – Test system architecture to test a configurator tool		66
Figure 8 – Performance testing (black box principle).....		75
Figure 9 – Measure round trip time using GOOSE ping-pong method.....		76
Figure 10 – Time synchronisation and accuracy test setup.....		80
Table 1 – Server documentation test cases.....		21
Table 2 – Server configuration test cases		22
Table 3 – Server data model test cases		22
Table 4 – Association positive test cases		23
Table 5 – Association negative test cases.....		24
Table 6 – Server positive test cases		24
Table 7 – Server negative test cases		25
Table 8 – Data set positive test cases.....		26
Table 9 – Date set negative test cases		27
Table 10 – Service tracking test cases		28
Table 11 – Substitution positive test cases		28
Table 12 – Setting group positive test cases		29
Table 13 – Setting group negative test cases.....		29
Table 14 – Unbuffered reporting positive test cases.....		30
Table 15 – Unbuffered reporting negative test cases		31
Table 16 – Buffered reporting positive test cases.....		32
Table 17 – Buffered reporting negative test cases.....		34
Table 18 – Log positive test cases		35
Table 19 – Log negative test cases.....		35
Table 20 – GOOSE publish positive test cases		36
Table 21 – GOOSE subscribe positive test cases		37
Table 22 – GOOSE management positive test cases		37
Table 23 – GOOSE publish negative test cases		37
Table 24 – GOOSE subscribe negative test cases		38
Table 25 – GOOSE management negative test cases		38

Table 26 – Control test cases	38
Table 27 – SBOes test cases	40
Table 28 – DOns test cases	41
Table 29 – SBOs test cases	41
Table 30 – DOes test cases	42
Table 31 – Time positive test cases	42
Table 32 – Time negative test cases	43
Table 33 – File transfer positive test cases	43
Table 34 – File transfer negative test cases	43
Table 35 – Network redundancy test cases	44
Table 36 – Client documentation test cases	45
Table 37 – Client configuration test cases	45
Table 38 – Client data model test cases	45
Table 39 – Association positive test cases	46
Table 40 – Association negative test cases	47
Table 41 – Server positive test cases	47
Table 42 – Server negative test cases	48
Table 43 – Data set positive test cases	48
Table 44 – Data set negative test cases	49
Table 45 – Service tracking test cases	50
Table 46 – Substitution test cases	50
Table 47 – Setting group positive test cases	51
Table 48 – Setting group negative test cases	51
Table 49 – Unbuffered reporting positive test cases	52
Table 50 – Unbuffered reporting negative test cases	53
Table 51 – Buffered reporting positive test cases	53
Table 52 – Buffered reporting negative test cases	55
Table 53 – Log positive test cases	55
Table 54 – Log negative test cases	56
Table 55 – GOOSE control block test cases	56
Table 56 – Control general test cases	56
Table 57 – SBOes test cases	57
Table 58 – DOns test cases	57
Table 59 – SBOs test cases	58
Table 60 – DOes test cases	58
Table 61 – Time positive test cases	59
Table 62 – Time negative test cases	59
Table 63 – File transfer positive test cases	59
Table 64 – File transfer negative test cases	59
Table 65 – Sampled values documentation test cases	61
Table 66 – Sampled values configuration test cases	62
Table 67 – Sampled values datamodel test cases	62
Table 68 – Sampled value control block test cases	63

Table 69 – Send SV message publish test cases	64
Table 70 – Send SV message subscribe positive test cases	64
Table 71 – Send SV message subscribe negative test cases	65
Table 72 – ICD test cases	67
Table 73 – ICD export test cases	67
Table 74 – SCD Import test cases	67
Table 75 – IED configurator data model test cases	68
Table 76 – IID export test cases	68
Table 77 – Negative IID export test case	68
Table 78 – System configurator documentation test case	68
Table 79 – ICD / IID import test cases	69
Table 80 – ICD / IID negative test case	69
Table 81 – Communication engineering test cases	70
Table 82 – Communication engineering negative test case	70
Table 83 – Data flow test cases	70
Table 84 – Data flow negative test cases	70
Table 85 – Substation section handling test cases	71
Table 86 – SCD modification test cases	71
Table 87 – SCD export test cases	72
Table 88 – SCD import test cases	72
Table 89 – SED file handling test cases	73
Table 90 – GOOSE performance test cases	78

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**COMMUNICATION NETWORKS AND SYSTEMS
FOR POWER UTILITY AUTOMATION –****Part 10: Conformance testing**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC 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 61850-10 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

This second edition cancels and replaces the first edition published in 2005. It constitutes a technical revision.

The major technical changes with regard to the previous edition are as follows:

- server device conformance test procedures have been updated;
- client device conformance test procedures have been added;
- sampled values device conformance test procedures have been added;
- (engineering) tool related conformance test procedures have been added;
- GOOSE performance test procedures have been added.

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

FDIS	Report on voting
57/1284/FDIS	57/1303/RVD

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

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

A list of all parts of IEC 61850 series, under the general title *Communication networks and systems for power utility automation*, can be found on the IEC website.

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

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

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

INTRODUCTION

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

This part of IEC 61850 defines:

- the methods and abstract test cases for conformance testing of client, server and sampled values devices used in power utility automation systems, and
- the methods and abstract test cases for conformance testing of engineering tools used in power utility automation systems, and
- the metrics to be measured within devices according to the requirements defined in IEC 61850-5.

The intended readers are IEC 61850 developers, test engineers and test system developers.

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

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

NOTE 2 Abbreviations used in IEC 61850-10 are listed in Clause 4 or may be found in other parts of IEC 61850 that are relevant for conformance testing.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 10: Conformance testing

1 Scope

This part of IEC 61850 specifies standard techniques for testing of conformance of client, server and sampled value devices and engineering tools, as well as specific measurement techniques to be applied when declaring performance parameters. The use of these techniques will enhance the ability of the system integrator to integrate IEDs easily, operate IEDs correctly, and support the applications as intended.

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-2, *Communication networks and systems for power utility automation – Part 2: Glossary*

IEC 61850-3, *Communication networks and systems for power utility automation – Part 3: General requirements*

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

IEC 61850-5:2003, *Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and devices models*

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 61850-7-4:2011, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2:2011, *Communication networks and systems for power utility automation – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC 62439-3:2012, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High Availability Seamless Redundancy (HSR)*

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

ISO 9001 (all parts), *Quality management systems*

ISO 9506 (all parts), *Industrial automation systems – Manufacturing Message Specification*

IEEE 1588:2008, *Standard for a precision clock synchronization protocol for networked measurement and control systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61850-2 and the following apply.

3.1

factory acceptance test

FAT

customer-agreed functional tests of the specifically manufactured power utility automation system or its parts using the parameter set for the planned application as specified in a specific customer specification

Note 1 to entry: The FAT will be carried out in the factory of the manufacturer or other agreed-upon location by the use of process simulating test equipment.

3.2

hold point

point, defined in the appropriate document beyond which an activity shall not proceed without the approval of the initiator of the conformance test

Note 1 to entry: The test facility shall provide a written notice to the initiator at an agreed time prior to the hold point. The initiator or his representative is obligated to verify the hold point and approve the proceeding of the activity.

3.3

interoperability

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

Set of values having defined correspondence with the quantities or values of another set

3.4

model implementation conformance 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 system or a device when subjected to:

- IEC 61850 series conformant information and services which are not implemented in the system or device under test;
- non IEC 61850 series conformant information and services sent to the system or device under test

3.6**protocol implementation conformance statement****PICS**

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 regarding the communication capabilities of the system or device to be tested and which are outside the scope of the IEC 61850 series. The PIXIT is not subject to standardisation.

3.8**routine test**

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

3.9**site acceptance test****SAT**

verification of each data and control point and the correct functionality within the PUAS and between the PUAS and its operating environment at the whole installed plant by use of the final parameter set as specified in a specific customer specification

Note 1 to entry: The SAT is the precondition for the power utility automation system (PUAS) being put into operation.

3.10**SCL implementation conformance statement****SICS**

statement with the summary of the capabilities of the SCL engineering tool

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 PUAS such as switchgear, transformers, network control centres or connected telecommunication units on the one side, and the serial links between the IEDs of the PUAS on the other

3.13**test facility**

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

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

3.14

technical issues conformance statement TICS

statement with device specific information regarding the implemented technical issues detected after publication of the standard. The TICS is not subject to standardisation.

3.15

type test

verification of correct behaviour of the IEDs of the PUAS 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 is carried out with IEDs, 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 conformance test. The test facility provides a written notice to the initiator at an agreed time prior to the witness point. The initiator or his representative has the right, but is not obligated, to verify the witness point.

4 Abbreviated terms

ACSI	abstract communication service interface
BRCB	buffered report control block
CDC	common data class
DUT	device under test
FAT	factory acceptance test
GI	general interrogation
GoCB	GOOSE control block
GOOSE	generic object oriented substation events
HMI	human machine interface
HSR	high availability seamless ring
ICD	IED capability description
IED	intelligent electronic device
IID	instantiated IED description
IP	internet protocol
LCB	log control block
LD	logical device
LN	logical node
MICS	model implementation conformance statement
MMS	manufacturing message specification (ISO 9506 series)
MSVCB	multicast sampled value control block
PICS	protocol implementation conformance statement
PIXIT	protocol implementation extra information for testing
PPS	pulse per second

PRP	parallel redundancy protocol
PUAS	power utility automation system
SAT	site acceptance test
SAV	sampled analogue values (IEC 61850-9-2)
SCD	substation configuration description
SCL	substation configuration language
SCSM	specific communication service mapping
SGCB	setting group control block
SICS	SCL implementation conformance statement
SNTP	simple network time protocol
SSD	system specification description
SV	sampled values
SVCB	sampled values control block
TCP	transport control protocol
TICS	technical issues conformance statement
TPAA	two party application association
TUT	tool under test
URCB	unbuffered report control block
USVCB	unicast sampled values control block
UTC	coordinated universal time
XML	extensible markup language

5 Introduction to conformance testing

5.1 General

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

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

Many internal tests during the development of a device (or a system kit) result in a type test (unit level test) performed at least by the provider and – if required by applicable standards – by an independent test authority. In the context of this standard, the term type test is restricted to the functional behaviour of the device.

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

A conformance test is the type test for communication and – since communication establishes a system – the system related test of the incorporated IEDs. As a global communications standard, the IEC 61850 series includes standardised conformance tests to ensure that all suppliers comply with applicable requirements.

Type tests and conformance tests do not completely guarantee that all functional and performance requirements are met. However, when properly performed, such tests

significantly reduce the risk of costly problems occurring during system integration in the factory and on-site.

Conformance testing does not replace project specific system related tests such as the FAT and SAT. The FAT and SAT are based on specific customer requirements for a dedicated power utility automation system and are done by the system integrator and normally witnessed by the customer. These tests increase the confidence level that all potential problems in the system have been identified and solved. These tests establish that the delivered power utility automation system is performing as specified.

5.2 Conformance test procedures

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

Conformance testing demonstrates the capability of the DUT to operate with other IEDs in a specified way according to the IEC 61850 series.

Conformance testing requires consideration of the following issues:

- The problem of all testing is the completeness of the tests. The number of all possible situations can be very large. It may be possible to cover all normal operating cases, but this may not be true for all failure cases.
- It is impossible to test all system configurations using IEDs from different world-wide suppliers. Therefore, a standardized test architecture with device simulators should be used. The use of such a test architecture implies agreement about its configuration and the test procedures applied in order to achieve compatible and reproducible results.
- A communication standard does not standardise the functions of the communicating equipment. Therefore, the failure modes of the functions are outside the scope of this part of the IEC 61850 series. But both, the existence of distributed functions and the impact of function response in devices on the data flow create some interdependence.
- Depending on the definition range of the standard, some properties of the device may be proven by information and documents provided with the DUT for the conformance testing instead of the conformance test itself.

The conformance test establishes that the communication of the DUT works according the IEC 61850 series. The IEC 61850 series is focussed on interoperability using data, function and device models including all services above or at the application level (ACSI). In addition, performance classes are addressed.

Since the IEC 61850 series defines no new communication stacks, the conformance to all seven ISO/OSI layers may be proven by documentation that communication stack software compliant with the corresponding specifications is implemented and may have been pre-tested and optionally certified. In the standard conformance test, only the application according to ACSI can be tested.

5.3 Quality assurance and testing

5.3.1 General

In order to ensure the quality during conformance testing, a quality assurance system has to be in place. This shall be clearly demonstrated by the test facility. This applies to the quality systems of all sub-suppliers.

In general, quality surveillance is used to monitor and verify the status of components during all phases of the conformance tests. For this purpose, inspections are carried out based on hold and witness points that are indicated by the initiator or its representative in the test and

the inspection plan that is supplied by the test facility. These inspections are process-related and will provide information and confidence on the quality of the tests. Quality surveillance will reduce the risks of failure during the FAT and SAT.

5.3.2 Quality plan

5.3.2.1 Conformance test quality plan

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

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

The conformance test quality plan shall also contain the following:

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

5.3.2.2 Test and inspection plan

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

- what will be inspected, tested and registered;
- the purpose of the inspections and tests;
- the procedures and standards to which inspections, tests and registrations will be performed;
- the expected results of the inspections and tests;
- by whom the inspections, tests and registrations will be performed.

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

The test facility shall provide a proposal for so-called hold, witness and review points in the test and inspection plan.

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

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

5.3.2.3 Audits requested by initiator

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

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

5.4 Testing

5.4.1 General

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

- device ready for testing;
- protocol implementation conformance statement (PICS). A standard PICS, also known as PICS proforma shall be supplied (see IEC 61850-7-2, Annex A);
- protocol implementation extra information for testing (PIXIT) statement;
- model implementation conformance statement (MICS);
- technical issues conformance statement (TICS);
- instruction manuals detailing the installation and operation of the device.

The requirements for conformance testing fall into two categories:

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

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

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

A standard PICS shall be supplied.

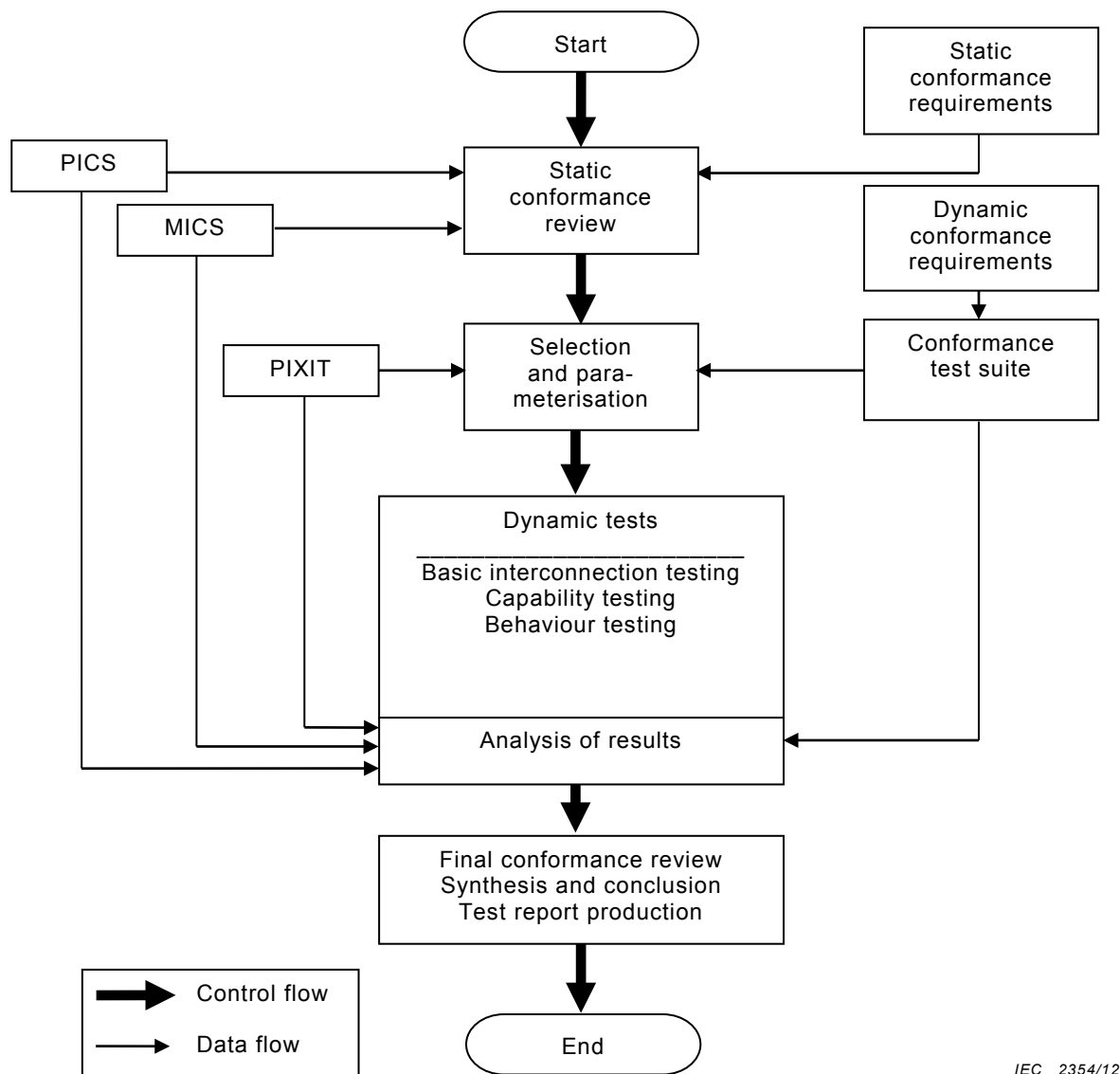
Concrete PICS shall be as defined for the SCSMs.

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

A technical issues conformance statement or TICS shall be provided detailing the implemented technical issues detected after publication of the standard.

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

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



IEC 2354/12

Figure 1 – Conceptual conformance assessment process

5.4.2 Use of SCL files

The DUT shall be delivered with an ICD file.

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

5.4.3 Device testing

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

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

- inspection of the documentation and version control of the device (IEC 61850-4);
- test of device configuration file against standardised syntax (schema) (IEC 61850-6);
- test of device configuration file against the device related object model (IEC 61850-7-4, IEC 61850-7-3);
- test of communication stack implementation against applicable SCSM (IEC 61850-8-1, IEC 61850-9-2);
- test of implemented ACSI services against ACSI definition (IEC 61850-7-2);
- test of device specific extensions according to rules given by the IEC 61850 series in general.

5.5 Documentation of conformance test report

A conformance test report shall include the following information:

- A reference list of all documents that describe or specify any qualifying tests that have been performed. These documents may include the vendor's standard operating and testing procedures, and local, national and international standards. International standards shall be cited by document number, date, clause and subclauses. References to other documents shall include a complete source address and document identification. A complete and contextually accurate summary or extract of the document may be included for convenience.
- A list of any specialised test equipment or computer programs used for performing the conformance tests.
- Name and address of the vendor.
- Name and address of the initiator of the conformance test (if different from vendor name).
- Name of the tested device.
- All of the variants (hardware, firmware, etc.) of the tested device.
- Name and address of the test facility.
- Date of issue of the test report.
- Name and signature of the tester.
- Unique reference number.
- A list of test items performed to verify conformance.
- Comments and problems found.
- For each test item, the following subjects shall be documented:
 - description of the test item with the objective of the test, the procedure how to perform the test and the expected result;
 - reference to the IEC 61850 series part, clause and subclause;
 - unique identifier per test item;
 - test result: passed, failed, inconclusive, not applicable or <empty> = not tested;
 - comparison of the test result to the expected result.

Changes or alterations to the device made at any point in the test, particularly those made to correct a test deficiency, shall be completely described. The consequences and requirements of re-testing of a server device – if required – shall be specified in corresponding test plans and test reports.

Conformance test documentation shall be supplied to the initiator.

6 Device related conformance testing

6.1 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.

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

Special attention shall be given to communication equipment such as star-couplers, switches, etc. which shall support all requested features of the standard but not introduce additional contingencies and limitations. The impact of the communication method (client-server, GOOSE, SV, etc.) used by the DUT shall be considered properly in the test procedures. Verification of functional applications (use of GOOSE messages) is not part of a conformance test even if advanced tools may offer such analysis.

6.2 Conformance test procedures

6.2.1 General

This subclause describes the test procedure requirements, test structure, the abstract test cases (what is to be tested). The format and a few examples of detailed test procedures (how to perform the test) 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 detailed 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 2. With this format, the test procedures document can also be used as test report. A few test procedure examples are depicted in Annex A.

<u>Test reference</u>	<u>Test purpose</u>	<u>References to the IEC 61850 documents Clause and Subclause</u>	<u>Test result</u>
Test reference: <type><ACSI-model><[N][p/s]><number> e.g. sRp3		Test purpose, e.g. test if association is set up correctly	
		☐ Passed ☐ Failed ☐ Inconclusive	
<u>Ref. Part Clause and Subclause of IEC 61850</u>			
<u>Expected result</u>		Definition of the expected behavior of the DUT after a step	
<u>Test description</u>		Step by step description of how to perform the test	
<u>Comment</u>		Area for comments during testing, e.g. found problems and remarks	

IEC 2355/12

Figure 2 – Test procedure format

6.2.3 Test structure

The test cases are structured as follows:

- documentation and version control (IEC 61850-4);
- configuration file (IEC 61850-6);
- data model (IEC 61850-7-3 and IEC 61850-7-4);
- mapping of ACSI models and services (IEC 61850-7-2 and applicable SCSM).

6.2.4 Test cases to test a server device

6.2.4.1 General

This part of the IEC 61850 series specifies the test system architecture and abstract test cases for server devices. The abstract test cases shall be used for the definition of test procedures to run in tests.

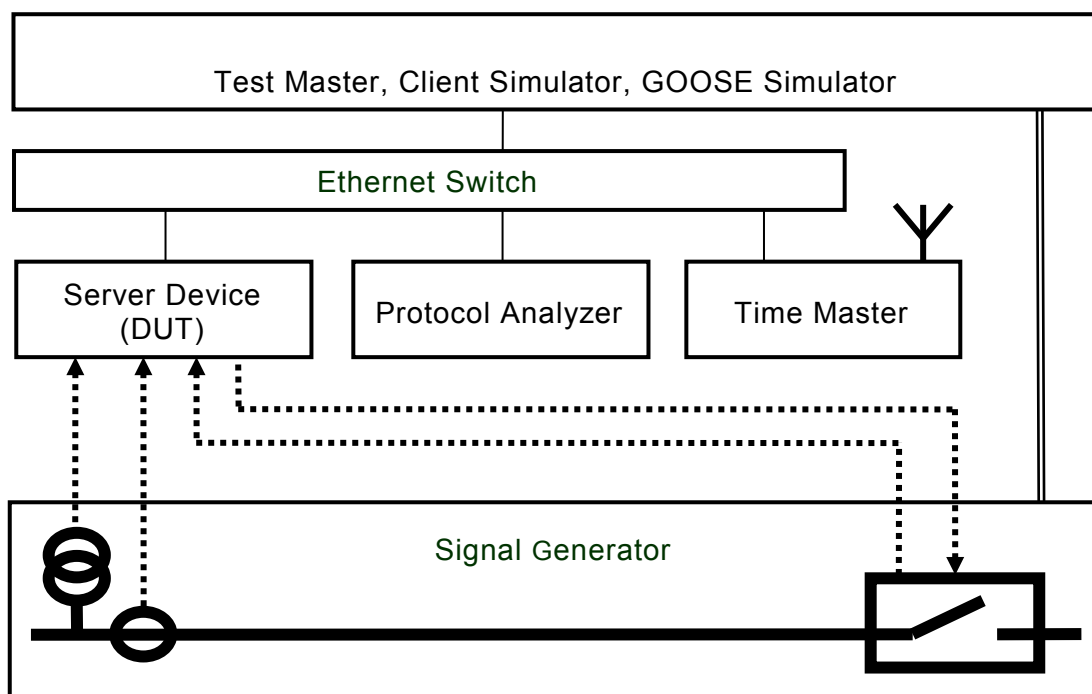
NOTE The SCSM specific test procedures are provided by test facilities agreed upon by the market participants.

6.2.4.2 Test system architecture to test a server device

In order to be able to perform a server device test, a minimum test set-up is necessary. The test architecture contains (see Figure 3):

- DUT;
- client simulator to initiate and generate TPAA messages;
- GOOSE simulator to send correct and incorrect GOOSE messages;
- test master to start/stop test cases, start/stop the analyzer and archive test results;
- time master;

- engineering tool to configure the DUT;
- protocol analyzer to store all the network traffic for each test case;
- signal generator to force binary and analogue events, controlled by the test master or test engineer.



IEC 2356/12

Figure 3 – 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 conformance statement according to IEC 61850-7-2 Annex A
sDoc2	Check if the major/minor software version in the PIXIT documentation and software version of the DUT does match (IEC 61850-4). PIXIT shall indicate the required information as requested in the test cases
sDoc3	Check if the major/minor software version in the MICS documentation and software version of the DUT does 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 in the TICS documentation and software version of the DUT does match (IEC 61850-4). TICS shall indicate the implemented technical issues.

6.2.4.4 Configuration file test cases

The test cases listed in Table 2 shall apply.

Table 2 – Server configuration test cases

Test case	Test case description
sCnf1	Test if the ICD configuration file conforms to the SCL schema (IEC 61850-6)
sCnf2	Check if the ICD configuration file corresponds with the actual data names, data types, data-sets, pre-defined data values exposed by the DUT on the network. When more data or services are exposed, attach a list and set the test result to Passed. When less data or services are exposed the test result is Failed.
sCnf3	Change at least 5 end-user configurable parameters that are exposed by the DUT on the network in the SCD configuration file, configure the DUT using the SCD configuration file (using the supplied configuration tool) and check the updated configuration using online services corresponds with the updated SCD file. Restore the original SCD file and re-configure the DUT to its original state.
sCnf4	Check if the server capabilities in the ICD "services" section do match with the IED capabilities
sCnf5	In case the control model is fixed (not configurable) check if the ICD correctly initializes the ctlModel values for all controllable objects
sCnf6	Check the edition 2 SCL changes: – version="2007" with revision="A" or higher – nameLength = 64
sCnf7	Check the "IdName" naming structure when supported. All online object references (including data sets and control block references) shall start with the "LDevice IdName" value instead of the "IED name" + "LDevice inst"

6.2.4.5 Data model test cases

The test cases listed in Table 3 shall apply.

Table 3 – 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 the IEC 61850-7-3, IEC 61850-7-4 and the applicable SCSM
sMdl8	Verify that the preconfigured enumerated data attribute values from the device and SCL are in specified range. Passed when all values are in range
sMdl9	Check if manufacturer specific data model extensions are implemented according to the extension rules in IEC 61850-7-1 Clause 14 (only when extensions are implemented). Passed when all extensions are implemented according to the rules
sMdl10	Check if the order of the data attributes within the functional constraints of the Data Object types match with IEC 61850-7-3. 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 Subclause 22.2 and SCSM

Test case	Test case description
sMdl12	Check that the rules for multiple data object instantiation are kept (IEC 61850-7-1,14.6, IEC 61850-7-4)
sMdl13	Check the logical device name space or the LLN0 logical node name space refers to edition 2
sMdl14	Check the correct use of name spaces for non-substation power utility applications like for example Hydro and DER

6.2.4.6 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 Figure 3 of IEC 61850-7-2:

- application association (sAss);
- server, Logical device, Logical node, Data, and Data Attribute model (sSrv);
- data set model (sDs);
- service tracking (sTrk);
- substitution model (sSub);
- setting group model (sSg);
- unbuffered report control model (sRp);
- buffered report control model (sBr);
- log control model (sLog);
- generic object oriented substation events (sGop and sGos);
- control model (sCtl);
- time and time synchronisation model (sTm);
- file transfer model (sFt).

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

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

A test case is mandatory when the applicable ACSI model and ACSI service is supported by the DUT. This is specified in the PICS according to IEC 61850-7-2, Annex A. The test result interpretation (passed/failed) depends on the declared IED capabilities e.g. in the ICD file as well as on the test result.

6.2.4.7 Application association model

6.2.4.7.1 Positive test cases

The test cases listed in Table 4 shall apply.

Table 4 – Association positive test cases

Test case	Test case description
sAss1	Associate and client-release a TPAA association (IEC 61850-7-2 Subclause 8.3.2)
sAss2	Associate and client-abort TPAA association (IEC 61850-7-2 Subclause 8.3.2)
sAss3	Associate with maximum number of clients simultaneously (PIXIT)

6.2.4.7.2 Negative test cases

The test cases listed in Table 5 shall apply.

Table 5 – 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 Subclause 8.3)
sAssN2	Check that with incorrect association parameters at server or client the association fails (IEC 61850-7-2 Subclause 8.3, PIXIT)
sAssN3	Set up maximum+1 associations, verify the last associate is refused
sAssN4	Disconnect the communication interface, the DUT should detect association lost within a specified period
sAssN5	Interrupt and restore the power supply, the DUT should accept an association request when ready
sAssN6	Verify the re-use of dropped association resources

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

6.2.4.8.1 Positive test cases

The test cases listed in Table 6 shall apply.

Table 6 – Server positive test cases

Test case	Test case description
sSrv1	Request GetServerDirectory(LOGICAL-DEVICE) and check response (IEC 61850-7-2 Subclause 7.2.2)
sSrv2	For each GetServerDirectory(LOGICAL-DEVICE) response issue a GetLogicalDeviceDirectory request and check response (IEC 61850-7-2 Subclause 9.2.1)
sSrv3	For each GetLogicalDeviceDirectory response issue a GetLogicalNodeDirectory(DATA) request and check response (IEC 61850-7-2 Subclause 10.2.2)
sSrv4	For each GetLogicalNodeDirectory(DATA) response issue a – GetDataDirectory request and check response (IEC 61850-7-2 Subclause 11.4.4) – GetDataDefinition request and check response (IEC 61850-7-2 Subclause 11.4.5) – GetDataValues request and check response (IEC 61850-7-2 Subclause 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 Subclause 11.4.2)
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 Subclause 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)

Test case	Test case description
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 (IEC 61850-7-3 Subclause 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 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)

6.2.4.8.2 Negative test cases

The test cases listed in Table 7 shall apply.

Table 7 – Server negative test cases

Test case	Test case description
sSrvN1	Request following data services with wrong parameters (unknown object, name case mismatch, wrong logical device or wrong logical node) and verify response– service error – GetServerDirectory(LOGICAL-DEVICE) (IEC 61850-7-2 Subclause 7.2.2) – GetLogicalDeviceDirectory (IEC 61850-7-2 Subclause 9.2.1) – GetLogicalNodeDirectory(DATA) (IEC 61850-7-2 Subclause 10.2.2) – GetAllDataValues (IEC 61850-7-2 Subclause 10.2.3) – GetDataValues (IEC 61850-7-2 Subclause 11.4.2) – SetDataValues (IEC 61850-7-2 Subclause 11.4.3) – GetDataDirectory (IEC 61850-7-2 Subclause 11.4.4) – GetDataDefinition (IEC 61850-7-2 Subclause 11.4.5)
sSrvN2	Request SetDataValues of ENUMERATED data with out-of-range value and verify response– service error (IEC 61850-7-2 Subclause 11.4.3)
sSrvN3	Request SetDataValues with mismatching data type (e.g. int-float) and verify response– service error (IEC 61850-7-2 Subclause 11.4.3)
sSrvN4	Request SetDataValues for read-only data values and verify response– service error (IEC 61850-7-2 Subclause 11.4.3)

6.2.4.9 Data set model

6.2.4.9.1 Positive test cases

The test cases listed in Table 8 shall apply.

Table 8 – Data set positive test cases

Test case	Test case description
sDs1	Request GetLogicalNodeDirectory(DATA-SET) and check response (IEC 61850-7-2 Subclause 10.2.2) For each response issue a – GetDataSetValues request and check response (IEC 61850-7-2 Subclause 13.3.2) – GetDataSetDirectory request and check response (IEC 61850-7-2 Subclause 13.3.6)
sDs2	Request a persistent CreateDataSet with one member and with maximum possible members and check response (IEC 61850-7-2 Subclause 13.3.4) and verify that the persistent data set is visible for another client
sDs3	Request a non-persistent CreateDataSet with one, maximum members and check response (IEC 61850-7-2 Subclause 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 the dataset has been deleted (IEC 61850-7-2 Subclause 13.1)
sDs7	Create a persistent dataset, release/abort the association, associate again and check the dataset is still present (IEC 61850-7-2 Subclause 13.1)
sDs8	Create and delete a persistent data set several times and verify every data set can be created normally
sDs9	Create and delete a non-persistent data set several times and verify every data set can be created normally
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 as specified in SCL
sDs12	Verify that the maximum number of non-persistent data sets with the maximum number of members can be created as specified in SCL
sDs13	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 Subclause 22.2)
sDs14	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 Subclause 22.2)

6.2.4.9.2 Negative test cases

The test cases listed in Table 9 shall apply.

Table 9 – Date set negative test cases

Test case	Test case description
sDsN1	Request following data set services with wrong parameters (unknown object, name case mismatch, wrong logical device or wrong logical node) and verify response– service error: – GetDataSetValues (IEC 61850-7-2 Subclause 13.3.2) – SetDataSetValues (IEC 61850-7-2 Subclause 13.3.3) – CreateDataSet (IEC 61850-7-2 Subclause 13.3.4) – DeleteDataSet (IEC 61850-7-2 Subclause 13.3.5) – GetDataSetDirectory (IEC 61850-7-2 Subclause 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 data sets until a correct response– service error is returned
sDsN5	Continue to create non-persistent data sets until a correct response– service error is returned
sDsN6	Create a persistent dataset with unknown member verify response– service error
sDsN7	Create a non-persistent dataset with unknown member 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 a (report) control class, and verify response– service error (IEC 61850-7-2 Subclause 13.1)
sDsN12	Delete a non-persistent dataset referenced by a (report) control class, and verify response– service error (IEC 61850-7-2 Subclause 13.1)
sDsN13	Request SetDataSetValues with a dataset with one or more read-only members, and verify response– service error

6.2.4.10 Service tracking model

6.2.4.10.1 General

The tracking services can be verified by verifying the tracking information while executing the corresponding test cases defined in the other clauses. For example during the execution of the control model test cases the tracked AddCause value shall be verified as well.

6.2.4.10.2 Positive test cases

The test cases listed in Table 10 shall apply. The control block tracking test cases shall be executed with the maximum control block and data set name length.

Table 10 – Service tracking test cases

Test case	Test case description
sTrk1	Verify the tracking of control block services: Buffered reporting, LTRK.BrcbTrk
sTrk2	Verify the tracking of control block services: Unbuffered reporting, LTRK.UrcbTrk
sTrk3	Verify the tracking of control block services: Log control block, LTRK.LocbTrk
sTrk4	Verify the tracking of control block services: GOOSE control block, LTRK.GocbTrk
sTrk5	Verify the tracking of control block services: Multicast sampled values control block, LTRK.MsvcbTrk
sTrk6	Verify the tracking of control block services: Unicast sampled values control block, LTRK.UsvcbTrk
sTrk7	Verify the tracking of control block services: Setting group control block, LTRK.SgcbTrk
sTrk8	Verify the tracking of control services: Single point control, LTRK.SpcTrk
sTrk9	Verify the tracking of control services: Double point control, LTRK.DpcTrk
sTrk10	Verify the tracking of control services: Integer control, LTRK.IncTrk
sTrk11	Verify the tracking of control services: Enumerated control, LTRK.EncTrk
sTrk12	Verify the tracking of control services: Analogue process value control with float command, LTRK.ApcFTrk
sTrk13	Verify the tracking of control services: Analogue process value control with integer command, LTRK.ApcIntTrk
sTrk14	Verify the tracking of control services: Binary step control, LTRK.BscTrk
sTrk15	Verify the tracking of control services: Integer step control, LTRK.IscTrk
sTrk16	Verify the tracking of control services: Binary analogue process value control, LTRK.BacTrk
sTrk17	Verify the tracking of other supported common services, LTRK.GenTrk

6.2.4.11 Substitution model

6.2.4.11.1 Positive test cases

The test cases listed in Table 11 shall apply.

Table 11 – 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 enabled (IEC 61850-7-3 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

6.2.4.12 Setting group control model

6.2.4.12.1 Positive test cases

The test cases listed in Table 12 shall apply.

Table 12 – Setting group positive test cases

Test case	Test case description
sSg1	Request GetLogicalNodeDirectory(SGCB) and check response+. For each SGCB request GetSGCBValues and check response+
sSg2	Verify the following setting group state machine path (IEC 61850-7-2 Clause 16, Figure 22); – SelectEditSG – Use SetEditSGValue [FC=SE] to change values – Use GetEditSGValue [FC=SE] to verify the new values – ConfirmEditSGValues
sSg3	Verify SelectActiveSG (IEC 61850-7-2 Clause 16, Figure 22); – SelectActiveSG of the first setting group – GetSGCBValues to verify active setting group and last activation time – Use GetDataValues/GetEditSGValue [FC=SG] to verify the values are of first setting group – Repeat for all setting groups
sSg4	Verify that after loss of association the server cancels the editing (EditSG=0) and the client can use SelectEditSG again to copy the values to the edit buffer (IEC 61850 7-2 Subclause 16.3.3)
sSg5	Verify that when SGCB ResvTms is present – The first client can edit the setting group when ResvTms = 0 – A second client cannot edit the setting group when ResvTms > 0 – A server resets the ResvTms when it does not receive a ConfirmEditSG within the reservation time
sSg6	Verify that when SGCB ResvTms is not present – The first client can edit the setting group – A second client cannot edit the setting group within a certain time (PIXIT)
sSg7	Verify that editing and activating the active setting group is allowed
sSg8	Verify that a client can cancel the editing of a setting group and that the original setting group values remain unchanged
sSg9	Request SelectEditSG of the first setting group, change one value and SelectEditSG of the second setting group without (ConfirmEditSGValues). Verify the response+
sSg10	Verify that when a setting group is being edited the SG values of that group can be read

6.2.4.12.2 Negative test cases

The test cases listed in Table 13 shall apply.

Table 13 – Setting group negative test cases

Test case	Test case description
sSgN1	Request following setting group <u>selection</u> services with wrong parameters (out of range values, or non-existent/null setting group) and verify response– service error – SelectActiveSG (IEC 61850-7-2 Subclause 16.3.2) – GetDataValues/GetEditSGValue [FC=SG] (IEC 61850-7-2 Subclause 16.3.6) – GetSGCBValues (IEC 61850-7-2 Subclause 16.3.7)
sSgN2	Request following setting group <u>definition</u> services with wrong parameters (out of range values, or non-existent/null setting group) and verify response– service error – SelectEditSG (IEC 61850-7-2 Subclause 16.3.3) – SetEditSGValue (IEC 61850-7-2 Subclause 16.3.4) – ConfirmEditSGValues (IEC 61850-7-2 Subclause 16.3.5) – GetEditSGValue [FC=SE] (IEC 61850-7-2 Subclause 16.3.6)
sSgN3	Request SetEditSGValue on an setting group value with FC=SG, verify response– service error
sSgN4	Request SetEditSGValue (FC=SE) without SelectEditSG (EditSG = 0), verify response– service error
sSgN5	Verify that when a client is editing settings, another client cannot edit settings

6.2.4.13 Unbuffered reporting model

6.2.4.13.1 Positive test cases

The test cases listed in Table 14 shall apply.

Table 14 – Unbuffered reporting positive test cases

Test case	Test case description
sRp1	Request GetLogicalNodeDirectory(URCB) and check response Request GetURCBValues of all responded URCB's
sRp2	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 Subclause 17.2.3.2.2.1), force/trigger a report and check the reports contain the enabled optional fields
sRp3	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 and data-reference and check the reports are transmitted according to the following (supported) trigger conditions: - on integrity - on update (dupd) - on update with integrity - on data change (dchg) - on data and quality change - on data and quality change with integrity period - Verify the validity of the ReasonCode (IEC 61850-7-2 Subclause 17.2.3.2.2.9) - Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2 Subclause 17.2.3.2.3.2) - Verify that reports are only sent when RptEna is set to True (IEC 61850-7-2 Subclause 17.2.2.5), when reporting is disabled no reports should be transmitted
sRp4	General interrogation (IEC 61850-7-2 Subclause 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.
sRp5	Segmentation of reports Verify that if a long report does not fit in one message, the report is split into sub-reports. Enable sequence-number and report-time-stamp optional field and check validity of: (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 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 Subclause 14.2.3.2.3.4)
sRp6	Configuration revision (IEC 61850-7-2 Subclause 17.2.2.7) - Verify that ConfRev represents a count of the number of times the configuration of the data set referenced by DataSet 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 DataSet is not null.

Test case	Test case description
sRp7	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)
sRp8	Buffer Time (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 17.2.2.9) – Verify that the BufTm value can contain at least the value 360 0000 (= 1 h in milliseconds)
sRp9	Verify the DUT can send reports with data objects
sRp10	Verify the DUT can send reports with data attributes
sRp11	Verify the DUT send any buffered events before the integrity report
sRp12	Verify the DUT send any buffered events before the GI report
sRp13	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. For a pre-assigned URCB the server resets the Owner to the pre-assigned client address
sRp14	Verify that the DUT can process an URCB with maximum name length for RptID and DataSet (IEC 61850-7-2 Subclause 22.2)

6.2.4.13.2 Negative test cases

The test cases listed in Table 15 shall apply.

Table 15 – 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 Subclause 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 sent when generating events (IEC 61850-7-2 Subclause 17.2.5.4)
sRpN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2 Subclause 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 Subclause 17.2.4.5)
sRpN6	Configure unsupported URCB options (PIXIT); Configure unsupported trigger conditions, optional fields and related parameters
sRpN7	Verify 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

6.2.4.14 Buffered reporting model

6.2.4.14.1 Positive test cases

The test cases listed in Table 16 shall apply.

Table 16 – Buffered reporting positive test cases

Test case	Test case description
sBr1	Request GetLogicalNodeDirectory(BRCB) and check response Request GetBRCBValues of all responded BRCB's
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 Subclause 17.2.3.2.2.1), force/trigger a report and check 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 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 Subclause 17.2.3.2.2.9) – Verify that when more trigger conditions are met preferably only one report is generated (IEC 61850-7-2 Subclause 17.2.3.2.3.2) – Verify that reports are only sent when RptEna is set to True. (IEC 61850-7-2 Subclause 17.2.2.5), when reporting is disabled no reports should be transmitted
sBr4	General interrogation (IEC 61850-7-2 Subclause 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 Subclause 17.2.3.2.2.5) – SqNum (not changed) – SubSqNum (0 for first report, incrementing, roll-over) – MoreSegmentsFollow – TimeOfEntry (not changed as SqNum is not altered) (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 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 (IEC 61850-7-2 Subclause 17.2.3.2.2.4 and 17.2.3.2.2.5)

Test case	Test case description
sBr6	Configuration revision (IEC 61850-7-2 Subclause 17.2.2.7) – Verify that ConfRev represents a count of the number of times the configuration of the data set referenced by DataSet 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 DataSet is not null
sBr7	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)
sBr8	Buffer Time (IEC 61850-7-2 Subclause 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 Subclause 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 Subclause 17.2.2.9) – Verify that the BufTm value can contain at least the value 360 0000 (= 1 h in ms)
sBr9	Verify the DUT can send reports with data objects
sBr10	Verify 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 Subclause 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 Subclause 17.2.3.2.3.3)
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 URCB. For a 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 DataSet (IEC 61850-7-2 Subclause 22.2)
	Specific to BRCB (leave a gap for future RP test cases)
sBr20	Buffered reporting (BRCB) state machine (IEC 61850-7-2 Subclause 17.2.2.5 figure 20) – Verify events are buffered after the association is released – Verify 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 Subclause 17.2.1, IEC 61850-7-2 Subclause 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 Subclause 14.2.2.14) – 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 Subclause 17 2.3.2.2.8)
sBr21	Buffered reporting (BRCB); buffering events (IEC 61850-7-2 Subclause 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.
sBr22	Verify that integrity reports are buffered

Test case	Test case description
sBr23	Verify successful ResvTms behaviour - On ResvTms = –1 the BRCB can be used by the pre-assigned 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 = –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 Subclause 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

6.2.4.14.2 Negative test cases

The test cases listed in Table 17 shall apply.

Table 17 – 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 Subclause 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 sent when generating events (IEC 61850-7-2 Subclause 17.2.3.2.3.4)
sBrN3	Setting the integrity period to 0 with TrgOps = integrity will result in no integrity reports will be sent (IEC 61850-7-2 Subclause 17.2.2.12)
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 Subclause 17.2.1)
sBrN6	Configure unsupported BRCB options (PIXIT); Configure unsupported trigger conditions, optional fields and related parameters
sBrN7	Verify 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

6.2.4.15 Log model

6.2.4.15.1 Positive test cases

The test cases listed in Table 18 shall apply.

Table 18 – 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 LCB's
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 DataSet (IEC 61850-7-2 Subclause 22.2)
sLog12	Verify that log entries are non-volatile and not lost after reboot and power loss

6.2.4.15.2 Negative test cases

The test cases listed in Table 19 shall apply.

Table 19 – 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 Subclause 17.3.2.5) – SetLCBValues (IEC 61850-7-2 Subclause 17.3.2.6) – QueryLogByTime (IEC 61850-7-2 Subclause 17.3.5.2) – QueryLogAfter (IEC 61850-7-2 Subclause 17.3.5.3) – GetLogStatusValues (IEC 61850-7-2 Subclause 17.3.5.4)
sLogN2	Request SetLCBValues when LCB is enabled and disabled and verify response– service error

6.2.4.16 Generic substation events model

6.2.4.16.1 Positive test cases

The test cases listed in Table 20, Table 21 and Table 22 shall apply. To verify the device processes the subscribed GOOSE message it is recommend to configure an observation mechanism, for example copy a subscribed state value to a local data object which is published.

NOTE The performance of sending and receiving GOOSE messages is verified by the GOOSE performance test procedures (see 8.2.3).

Table 20 – GOOSE publish positive test cases

Test case	Test case description
sGop1	Request GetLogicalNodeDirectory(GoCB) and request GetGoCBValues (IEC 61850-7-2 Subclause 18.2.2.5 and 10.2.2)
sGop2	GOOSE messages are published with a long (SCL maxtime) cycle time, check the GOOSE data with configured data; (IEC 61850-7-2 Subclause 18.2.3) – <u>gocbRef</u> is a valid GoCB reference – <u>timeAllowedtoLive</u> > 0 and the next GOOSE message is transmitted within the specified value of the current GOOSE message – <u>datSet</u> is same as the GoCB and contains a valid dataset reference – <u>goID</u> is same as the GoCB and SCL, the default value is the GoCB reference – <u>t</u> contains the time of the status increment or start-up – <u>sqNum</u> is incremented, stNum>0 and is not changed – <u>Simulation</u> is not present or if present with value FALSE – <u>confRev</u> >0 and is same as the GoCB and SCL (IEC 61850-7-2 Subclause 18.2.1.6) – <u>needsCommissioning</u> is not present or if present same as GoCB – <u>numDatSetEntries</u> matches with the number of data entries in allData – <u>allData</u> values match with the datSet element type
sGop3	Verify that a newly activated device sends the initial GOOSE message with stNum initial value one (1) (IEC 61850-7-2 Subclause 18.1, 18.2.3)
sGop4	Force a data change of a data value in the GOOSE dataset, DUT should publish GOOSE messages as specified/configured (SCL mintime), stNum is incremented, sqNum = 0
sGop5	When supported, verify that the DUT publishes GOOSE messages with the simulation flag set (IEC 61850-7-2 Subclause 18.2.3.8)
sGop6	Disable GoCB, verify that changing parameters with SetGoCBValues are active (IEC 61850-7-2 Subclause 18.2.1.3, 18.2.2.5 and 18.2.2.6) and no GOOSE messages are transmitted anymore
sGop7	Verify that a restart of the device shall not reset the Configuration revision value (IEC 61850-7-2 Subclause 18.2.1.6)
sGop8	Verify that ConfRev increments every time when the configuration of the data set referenced by DatSet has been changed (IEC 61850-7-2 Subclause 15.2.1.6). Changes that are counted are: – deletion of a member of the data-set – re-ordering of members in the data-set – changing the value of the attribute DatSet
sGop9	Verify that GoCB attribute NdsCom is set when DatSet is not yet configured (is NULL) (IEC 61850-7-2 Subclause 18.2.1.7)
sGop10	Verify the DUT can send GOOSE messages with data attributes and/or data objects
sGop11	Verify that the server can process a GoCB with maximum name length for DatSet, GoCBRef and GoID (IEC 61850-7-2 Subclause 22.2)

Table 21 – GOOSE subscribe positive test cases

Test case	Test case description
sGos1	Send GOOSE messages <u>with/without the VLAN tag</u> with new data and check if the message is received and the data has the new value by e.g. check binary output, event list, logging or MMI
sGos2	Send GOOSE messages with the ndsCom parameter set. Verify that on a status change the values are not used for operational purposes (IEC 61850-7-2 Subclause 18.2.3.8)
sGos3	Proper detection and action roll-over of sqNum with no status change (sqNum=max -> sqNum = 1) and with status change (sqNum=max -> sqNum = 0)
sGos4	Verify the logical node LGOS data object attribute values on receiving valid GOOSE messages, no GOOSE messages and GOOSE messages with mismatching ConfRev
sGos5	Verify that the server can subscribe to GOOSE messages with structured data (FCD)
sGos6	Send subscribed GOOSE messages with the Simulation parameter set (IEC 61850-7-2 Subclause 18.2.3.8). Verify that – when the subscriber is not in simulation mode (LPHD.Sim.stVal=false) the simulated values are ignored. The subscriber shall keep on using the "real" GOOSE messages – when the subscriber is in simulation mode (LPHD.Sim.stVal=true) the simulated values are used for operational purposes. The subscriber shall ignore the "real" GOOSE messages after a first simulated one has been received. The corresponding LGOS.SimSt shall be set when the first simulated message is received and cleared when LPHD.Sim.stVal is set to false.
sGos7	Verify that the server can subscribe GOOSE messages with maximum name length for DataSet, GoCBRef and GoID (IEC 61850-7-2 Subclause 22.2)

Table 22 – GOOSE management positive test cases

sGom1	Verify GOOSE services: request service with legal parameters and check response (IEC 61850-7-2 Subclause 15.2.2) – GetGoReference (IEC 61850-7-2 Subclause 18.2.2.3) – GetGOOSEElementNumber (IEC 61850-7-2 Subclause 18.2.2.4)
sGom2	Verify GOOSE management request: Check DUT request service with valid parameters and simulate valid response (IEC 61850-7-2 Subclause 15.2.2) – GetGoReference (IEC 61850-7-2 Subclause 18.2.2.3) – GetGOOSEElementNumber (IEC 61850-7-2 Subclause 18.2.2.4)

6.2.4.16.2 Negative test cases

The test cases listed in Table 23, Table 24 and Table 25 shall apply.

Table 23 – GOOSE publish negative test cases

Test case	Test case description
sGopN1	When GoEna=TRUE, no attributes of the GoCB control block can be set except for GoEna. (IEC 61850-7-2 Subclause 18.2.1.3)
sGopN2	Verify that if the number or size of values being conveyed by the elements in the dataset exceeds the SCSM determined maximum number, NdsCom is set to True. (IEC 61850-7-2 Subclause 18.2.1.7)

Table 24 – GOOSE subscribe negative test cases

Test case	Test case description
sGosN1	Check behaviour of DUT as specified in PIXIT on Missing GOOSE message
sGosN2	Check behaviour of DUT as specified in PIXIT on Double GOOSE message
sGosN3	Check behaviour of DUT as specified in PIXIT on Delayed GOOSE message, with and without exceeding timeAllowedToLive
sGosN4	Check behaviour of DUT as specified in PIXIT on Out of order GOOSE message
sGosN5	Check behaviour of DUT as specified in PIXIT on No GOOSE messages
sGosN6	Check behaviour of DUT as specified in PIXIT on invalid GOOSE messages – <u>gocbRef</u> different from GoCB and NULL – <u>timeAllowedtoLive</u> = 0 – <u>datSet</u> different from GoCB and NULL – <u>goID</u> different from GoCB and NULL – <u>t</u> contains the time of a status change minus/plus one hour – <u>confRev</u> different from GoCB and NULL – <u>numDatSetEntries</u> 0, more, less with the number of data entries in the allData – <u>allData</u> values do not match with the datSet element type

Table 25 – GOOSE management negative test cases

Test case	Test case description
sGomN1	Client request GOOSE management services with illegal parameters and verify DUT response-service error (IEC 61850-7-2 Subclause 18.2.2). Verify that NULL for MemberReference in GetGOOSEElementNumber indicates that no member of the referenced data set is defined. (IEC 61850-7-2 Subclause 18.2.2.4.2.2)

6.2.4.17 Control model

6.2.4.17.1 Test cases

The test cases listed in Table 26 shall apply.

Table 26 – Control 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 Subclause 20.2.1) – SBO-control with normal security (IEC 61850-7-2 Subclause 20.2.2) – direct with enhanced security (IEC 61850-7-2 Subclause 20.3.2) – SBO-control with enhanced security (IEC 61850-7-2 Subclause 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 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"

Test case	Test case description
sCtl7	Verify that with interlock or synchro check conditions the specified checks are performed and the command is executed accordingly (IEC 61850-7-2 Subclause 20.5.2.5) – 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 Table 47)
sCtl9	Select the same control object twice, verify that the second select request is rejected with AddCause "Object-already-selected" (IEC 61850-7-2 Table 47) 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 Table 47, 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 Table 47)
sCtl12	Select / Operate an unknown control object and verify that the control requests are rejected with AddCause "Unknown" (IEC 61850-7-2 Table 47)
sCtl13	Verify that the Select request on a direct operate control object is rejected with AddCause "Unknown" (IEC 61850-7-2 Table 47)
sCtl14	Operate the same direct control object twice from 2 clients (IEC 61850-7-2 Table 47, PIXIT) and verify that the last control request is rejected with AddCause "Command-already-in-execution"
sCtl15	Verify that the SBOs Operate or Cancel request with different control parameters than the SelectWithValue is rejected with AddCause: Inconsistent-parameters"
sCtl16	Verify that when Loc is set remote control requests are rejected with AddCause "Blocked-by-switching-hierarchy"
sCtl17	Verify that with station level control 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 Table 54)
sCtl19	Verify that when the blkEna is set the control requests are terminated 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 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 Table 54)
sCtl22	Verify that with insufficient access authority control requests are rejected with AddCause "No-access-authority". (IEC 61850-7-2 Table 54)
sCtl23	Verify that when an APC control action end position has overshoot the command terminates with AddCause "Ended-with-overshoot". (IEC 61850-7-2 Table 54)
sCtl24	Verify that when an 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 Table 54)
sCtl25	Verify that a cancel request is successful when the control object is in the unselected state (IEC 61850-7-2 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 Table 54)
sCtl27	Verify that the SelectWithValue request on a SBOs control object is rejected with AddCause "Unknown" (IEC 61850-7-2 Table 54)
sCtl28	Verify that the DUT can control an object with maximum name length for IED and Logical Device (IEC 61850-7-2 Subclause 22.2)

6.2.4.17.2 Control model specific test cases

The test cases listed in Table 27, Table 28, Table 29 and Table 30 shall apply.

Table 27 – SBOes test cases

Test case	Test case description
sSBOes1	Send a correct SelectWithValue and Operate request Verify 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)
sSBOes2	Send a correct SelectWithValue request Verify each of these paths will return the device to the Unselected state: – Send a correct Cancel request – Wait 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 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 each of these paths will return the device to the Ready state and the TimeActivatedOperateTermination-: – Force a '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 Subclause 20.2.2) or send incorrect SelectWithValue request
sSBOes7	Send a correct SelectWithValue request Verify that sending multiple Operate Many requests will return the device to the 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

Table 28 – 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 correct TimeActivatedOperate request Verify each of these paths will return the device to the Ready state and the TimeActivatedOperateTermination-: – Force a 'Test not ok' – Send a correct Cancel request

Table 29 – SBOs test cases

Test case	Test case description
sSBOs1	Send a correct Select request Send correct Operate request
sSBOs2	Send a correct Select request Verify each of these paths will return the device to the Unselected state: – Send a correct Cancel request – Wait for select timeout – Send a Release request – Send an Operate request, resulting in 'Test not ok'
sSBOs3	Send a correct Select request – Send an incorrect TimeActivatedOperate request resulting in respond-
sSBOs4	Send a correct Select request Send a TimeActivatedOperate request, thereby making sure the device will generate a 'Test Ok'. Verify the TimeActivatedOperateTermination+
sSBOs5	Send a correct Select request Send a correct TimeActivatedOperate request Verify each of these paths will return the device to the Ready state and the TimeActivatedOperateTermination-: – Force a 'Test not ok' – Send correct Cancel request
sSBOs6	Send a Select request resulting in respond-. Verify the device returns to the Unselected state.
sSBOs7	Send a correct Select request Verify that sending multiple Operate Many requests will return the device to the Ready state Verify that sending a Cancel request will return the device to the Unselected state

Table 30 – DOes test cases

Test case	Test case description
sDOes1	Send a correct Operate request Verify 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, resulting in 'Test not ok'.
sDOes3	Send a TimeActivatedOperate request, resulting in respond-
sDOes4	Send a correct TimeActivatedOperate request Verify the TimeActivatedOperateTermination+ Verify 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)
sDOes5	Send a correct TimeActivatedOperate request Verify each of these paths will return the device to the Ready state and the TimeActivatedOperateTermination-: – Force a 'Test not ok' – Send a correct Cancel request

6.2.4.18 Time and time synchronisation model

6.2.4.18.1 Positive test cases

The test cases listed in Table 31 shall apply.

Table 31 – Time positive test cases

Test case	Test case description
sTm1	Verify the DUT supports and executes the SCSM time synchronisation as configured in SCL
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

6.2.4.18.2 Negative test cases

The test cases listed in Table 32 shall apply.

Table 32 – Time negative test cases

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

6.2.4.19 File transfer model

6.2.4.19.1 Positive test cases

The test cases listed in Table 33 shall apply.

Table 33 – File transfer positive test cases

Test case	Test case description
sFt1	Request a GetServerDirectory(FILE) with correct parameters and verify the response (IEC 61850-7-2 Subclause 8.2.2, PIXIT)
sFt2	For each responded file: – request a GetFile with correct parameters and verify the response (IEC 61850-7-2 Subclause 23.2.1) – request a GetFileAttributeValues with correct parameters and verify the response (IEC 61850-7-2 Subclause 23.2.4) – request a DeleteFile with correct parameters and verify the response (IEC 61850-7-2 Subclause 23.2.3)
sFt3	Verify the SetFile service with a small and large file and the maximum number of maximum sized file
sFt4	Request a GetFile from two clients simultaneously if more than one client association is supported (PIXIT)
sFt5	Request a GetServerDirectory(FILE) with the wildchar parameter and verify the response (IEC 61850-7-2 Subclause 7.2.2)

6.2.4.19.2 Negative test cases

The test cases listed in Table 34 shall apply.

Table 34 – File transfer negative test cases

Test case	Test case description
sFtN1	Request following file transfer services with an unknown file name and verify the appropriate response– service error – GetFile (IEC 61850-7-2 Subclause 23.2.1) – GetFileAttributeValues (IEC 61850-7-2 Subclause 23.2.4) – DeleteFile (IEC 61850-7-2 Subclause 23.2.3)

6.2.4.20 Network redundancy

6.2.4.20.1 Test cases

The test cases listed in Table 35 shall apply.

Table 35 – Network redundancy test cases

Test case	Test case description
sPrp1	Verify that the device support PRP redundancy according to IEC 62349-3
sPrp2	Verify that if one channel fails no packets are lost in the device and LCCH data values are updated
sHsr1	Verify that the device support HSR redundancy according to IEC 62349-3
sHsr2	Verify that if one channel fails no packets are lost in the device and LCCH data values are updated

6.2.5 Test cases to test a client device

6.2.5.1 General

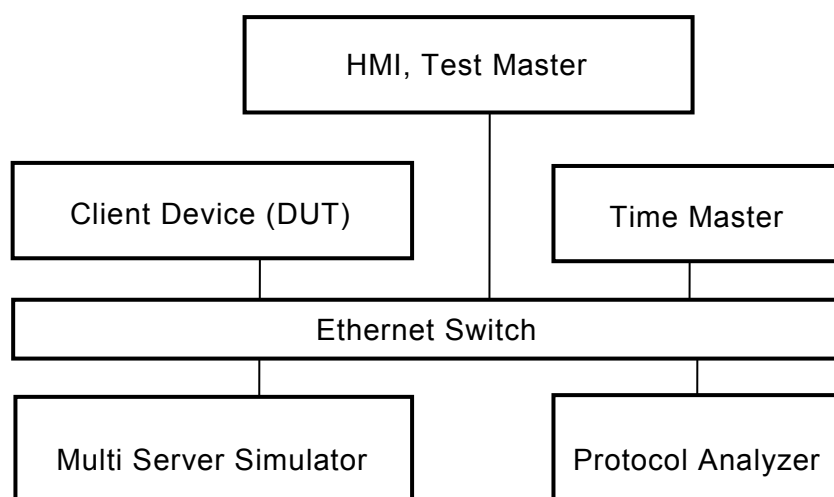
This part of the IEC 61850 series specifies the test system architecture and abstract test cases (see 6.2.5.7 to 6.2.5.19) for client devices. The abstract test cases shall be used for the definition of test procedures to run in tests.

NOTE The SCSM specific test procedures are 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:

- 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 analyze and archive test results;
- time master;
- engineering tool to configure the DUT;
- protocol analyzer to store the all network traffic for each test case.



IEC 2357/12

Figure 4 – 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 cases listed in Table 36 shall apply.

Table 36 – Client documentation test cases

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 in the PIXIT documentation and software version of the DUT does match (IEC 61850-4). PIXIT shall indicate the required information as requested in the test cases
cDoc3	Check if the major/minor software version in the MICS documentation and software version of the DUT does match (IEC 61850-4). MICS shall indicate which CDC's and/or CDC parts are supported by the DUT, for example arrays
sDoc4	Check if the major/minor software version in the TICS documentation and software version of the DUT does match (IEC 61850-4). TICS shall indicate the supported technical issues.

6.2.5.4 Configuration file test cases

The test cases listed in Table 37 shall apply.

Table 37 – Client configuration test cases

Test case	Test case description
cCnf1	Check if the DUT processes the data names, data types as configured in the SCL configuration file.
cCnf2	Change at least 5 end-user configurable parameters that are displayed by the DUT in the SCL configuration file, configure the DUT using the SCL configuration file (using the supplied configuration tool) and check the updated configuration. Restore the original SCL file and re-configure the DUT to its original state.
cCnf3	Verify that client can handle the ConfigRev management in SCL and exposed by the server in LLN0.NamPIt.configRev as described in the PIXIT. On a mismatch the DUT shall behave as described in the PIXIT (note that, if the PIXIT describes that the DUT does not check such a mismatch, no action is required by the DUT)

6.2.5.5 Data model test cases

The test cases listed in Table 38 shall apply.

Table 38 – Client data model test cases

Test case	Test case description
cMdl1	Verify that the client can handle the maximum name length according to IEC 61850-7-2 Subclause 22.2 and SCSM and 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) setting group control block e) GOOSE control block f) Log control block
cMdl3	Verify that DUT can read and process the mandatory and optional attributes from the CDCs in IEC 61850-7-3 unless stated otherwise in the MICS

6.2.5.6 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 Figure 3:

- application association (cAss);
- server, Logical device, Logical node, Data, and Data Attribute model (cSrv);
- data set model (cDs);
- service tracking (cTrk);
- substitution model (cSub);
- setting group model (cSg);
- unbuffered report control model (cRp);
- buffered report control model (cBr);
- log control model (cLog);
- GOOSE control block model (cGcb);
- control model (cCtl);
- time and time synchronisation model (cTm);
- file transfer model (cFt).

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

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

A test case is mandatory when the applicable ACSI model and ACSI service is supported by the DUT. This is specified in the PICS according to IEC 61850-7-2, Annex A. The test result interpretation (passed/failed) depends on the declared capabilities.

6.2.5.7 Application association model

6.2.5.7.1 Positive test cases

The test cases listed in Table 39 shall apply.

Table 39 – 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 Subclause 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
cAss4	Verify the DUT can handle servers with small and large MMS PDU size, the DUT should keep on proposing it's original MMS PDU size (PIXIT)

6.2.5.7.2 Negative test cases

The test cases listed in Table 40 shall apply.

Table 40 – 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 Subclause 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 Subclause 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 Subclause 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).

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

6.2.5.8.1 Positive test cases

The test cases listed in Table 41 shall apply.

Table 41 – 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 the DUT requests a GetServerDirectory(LOGICAL-DEVICE) to all the logical devices of the configured servers (see Note 2) (IEC 61850-7-2 Subclause 7.2.2)
cSrv2	If the DUT implements Autodescription, for each GetServerDirectory(LOGICAL-DEVICE) response check the DUT issues a GetLogicalDeviceDirectory request (IEC 61850-7-2 Subclause 9.2.1)
cSrv3	If the DUT “implements Autodescription”, for each GetLogicalDeviceDirectory response check the DUT issues a GetLogicalNodeDirectory(DATA) request (IEC 61850-7-2 Subclause 10.2.2)
cSrv4	If the DUT “implements Autodescription”, for a subset of the GetLogicalNodeDirectory(DATA) response check the DUT issues at least one of the following services: a) GetDataDirectory request and check response (IEC 61850-7-2 Subclause 11.4.4) b) GetDataDefinition request and check response (IEC 61850-7-2 Subclause 11.4.5)
cSrv5	Verify that after start up the DUT is able to update the process values of the configured servers.
cSrv6	Request a SetDataValues of the different basic types (with for example FC=CF) and check the services (IEC 61850-7-2 Subclause 11.4.3)
cSrv7	Request GetDataValues and check if the DUT updates its model (IEC 61850-7-2 Subclause 11.4.2)
cSrv8	Request GetAllDataValues for the required functional constraints and check if the DUT updates its model (IEC 61850-7-2 Subclause 10.2.3)
cSrv9	Verify that the client is able to set/reset blkEna (IEC 61850-7-3 Subclause 6.2.6)

Implement Autodescription means that there is a way to configure the DUT to update the image of the model of one of the servers it has to communicate with using the ACSI services.

Configured servers means the servers the DUT is configured to communicated with. The DUT at least needs to know the parameters to establish an association with them.

6.2.5.8.2 Negative test cases

The test cases listed in Table 42 shall apply.

Table 42 – Server negative test cases

Test case	Test case description
cSrvN1	If the DUT implements autodescription, force the DUT to start the autodescription and check 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/notifies 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/notifies 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.

6.2.5.9 Data set model

6.2.5.9.1 Positive test cases

The test cases listed in Table 43 shall apply.

Table 43 – 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 Subclause 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 Subclause 13.3.6)
cDs3	Check the DUT can request a GetDataSetValues and handle the respond (IEC 61850-7-2 Subclause 13.3.2)
cDs4	Check the DUT can request a SetDataSetValues and handle the respond (IEC 61850-7-2 Subclause 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 Subclause 13.3.4)
cDs7	Request a DeleteDataSet service and check the DUT sends the request properly and is able to process the response of the server (IEC 61850-7-2 Subclause 13.3.5)