

314

**PROTOCOL CONFORMANCE
TESTING**

**Task Force
D2.12**

February 2007



PROTOCOL CONFORMANCE TESTING

Task Force D2.12

HENK SPELT, The Netherlands
RUDOLF BAUMANN, Switzerland
WAN AZLAN, Malaysia

Copyright © 2007

“Ownership of a CIGRE publication, whether in paper form or on electronic support only infers right of use for personal purposes. Are prohibited, except if explicitly agreed by CIGRE, total or partial reproduction of the publication for use other than personal and transfer to a third party; hence circulation on any intranet or other company network is forbidden”.

Disclaimer notice

“CIGRE gives no warranty or assurance about the contents of this publication, nor does it accept any responsibility, as to the accuracy or exhaustiveness of the information. All implied warranties and conditions are excluded to the maximum extent permitted by law”.

PROTOCOL CONFORMANCE TESTING

HENK SPELT, The Netherlands
RUDOLF BAUMANN, Switzerland
WAN AZLAN, Malaysia

ABSTRACT

In different international and national organizations standardization work is in progress on data communication protocols, data exchange procedures and on the handling for electronic document interchange. By using IT-products, which conform to the international standards, the time and again demanded interoperability can be realized.

A Conformance Test of such products, and the resulting attestation of conformity, gives safety and confidence to the end users that the products protocol implementation is according to the international standard. Furthermore it helps the end users to avoid unnecessary commissioning, test time and resources.

The products that have passed Conformance Testing guarantee the fulfilling of the basic compatibility and functionality requirements. This way the user can choose products best suitable for his particular requirements. In addition, the end user can expect that its device will interoperate with various other devices with an attestation of conformity for the same international standard now and in the future.

Conformance Test procedures and systems have been developed for several international communication protocols, especially from IEC TC57, as well as for metering data transmission and for the exchange of information for the energy market. By using these Conformance Test systems the supplier of products can prove the conformity to the international standards.

This technical report shows, based on different real life experiences, what Conformance Testing involves and how it is performed on different applications and standards.

All this benefits the utilities, in their continuous demand for more permanent and efficient ways of installing and commissioning new or extended systems for information exchange.

Table of contents	Page
1 Introduction.....	4
1.1 Background.....	4
1.2 Scope and objective	4
1.3 Intended audience	4
1.4 References	4
2 General view of conformance testing.....	6
2.1 What is a Conformance Test?.....	6
2.2 Why conformance testing?	6
2.3 Conformance test approaches	7
2.3.1 Definition of Conformance	7
2.3.2 Conformance Test Process	7
2.3.2.1 Static Test	8
2.3.2.2 Dynamic Test.....	9
2.4 Who can do conformance tests?	9
2.5 At what time should conformance test be performed?.....	10
3 Protocol and conformance testing overview	11
3.1 IEC 60870-5 companion standards.....	12
3.2 IEC 61850.....	14
3.3 DNP3 De-facto standard (USA)	16
3.4 DLMS/COSEM (Metering standard).....	17
3.5 TASE.2	18
3.6 ELCOM90	18
3.7 Market protocols Edine, EDIG@S, ESS	19
3.8 CIM.....	22
3.9 WISP+: An Example Proprietary Protocol.....	25
4 Recommendations.....	26
4.1 Recommendations for utilities	26
4.2 Recommendations for vendors/manufactures	27
4.3 General remarks.....	27

1 INTRODUCTION

1.1 Background

In different organizations standardization work is in progress on communication protocols, data exchange procedures and on process handling of electronic document interchange. By using products, which conform to these standards, the highly demanded interoperability can be realized.

Conformance Test procedures and -systems have been prepared for different communication protocols, especially from IEC TC57, and also for metering data transmission and for the ETSO Scheduling system (ESS). Conformance tests are also performed by some utilities on proprietary communication protocols. By using these Conformance Test procedures the supplier of products can prove the conformity according to the standards

1.2 Scope and objective

Within the scope are mainly all specified IEC TC57 protocol standards and their derivatives to be used in the Utility world. This report shows what Conformance Testing for those standards includes and how it is performed for different applications, using real life examples.

Different ways of testing possibilities are discussed, and it is demonstrated which experiences and results exist and how conformity to a particular standard will finally be achieved.

In this document the following items will be elaborated:

- Introduction to conformance testing
- Method and scope of tests, what is possible and what is not
- The benefits of Conformance Testing of existing installations
- Demonstrate when such a testing procedure is (not) suitable
- Problems and difficulties during such tests
- Discuss the conformance testing of all relevant standards like IEC 60870, 61850, ETSO ESS
- Preparation of conformance test procedures for proprietary protocols like the Westinghouse System Limited, Extended WISP+ protocol
- List the existing and further developments of Conformance Testing systems/equipment
- Available information on all existing testing equipment and laboratories

1.3 Intended audience

This report, written by the D2 TF 12, should be published as a technical report (or an article) in *Electra*. It will be addressed to the management and technical staff of the utilities to understand the benefits of Conformance Testing for international standards.

1.4 References

- [1] Information Technology, Open System Interconnection, Conformance Testing Methodology and Framework, International Standard IS-9646, ISO, Geneva
- [2] Conformance Testing Guideline for Communication in Substations, Technical Brochure TB-236, Task Force B5.01, CIGRE, Paris
- [3] CIGRE Report SC B5 WG B5.01 (ref 236); "Conformance testing guideline for communication in substations", published by CIGRE in 2003

- [4]** IEC 61850 Communication networks and systems in substations, Part 10: Conformance Testing (IEC 61850-10)
- [5]** Telecontrol equipment and systems; Part 5-6: Guidelines for Conformance Testing the IEC 60870-5 Companion Standards edition 1.0 (2006-3-8)
- [6]** Technical Report No 3825.02 dated August 1999 from EFI "ELCOM-90 User Element Conventions"
- [7]** DLMS UA 1001-1, "Yellow Book"; COSEM Conformance Test Tool – Specification
- [8]** TNB Extended WISP+ Protocol Conformance and Integration Test Plan and Procedures, "Tenaga Nasional Berhad" – company documentation

2 GENERAL VIEW OF CONFORMANCE TESTING

2.1 *What is a Conformance Test?*

A Conformance test is a quality assurance activity that ensures interoperability among hardware or software from different suppliers based upon a common standard. A Conformance test is usually associated with the need to make communication systems or computer languages work in an interoperable manner. Compliance does not mean that the complete standard is implemented. Compliance does mean that the parts of the standard, that are implemented, conform to the applicable (parts) of the standard.

2.2 *Why conformance testing?*

Testing of standard interfaces can help to prevent or solve problems such as:

- Implementations differ because the standard leaves room for different interpretations
- Vendors make interpretation mistakes (they also are human)
- Products contain 'child deceases' or teeth problems
- Functionality of the implementation is not clear to the market
- The processing of error situations is not complete or different
- Extending the lifetime of existing systems by emulating communication protocol on a new equipment platform

Uncertainties are frequently present to the end users related to equipments adequate performance, operation and interoperability based on the applicable standard. These problems could easily lead to a substantial throughput time and cost increase during the implementation phase for IT vendors as well as for their clients. There will be a considerable risk that errors in communication will surface later in the operational phase causing even bigger financial damage. Therefore in most cases, the main reason why a conformance test is performed is for an organization to contain cost due to non-conformity, in an early stage of a systems lifecycle. The cost due to non-conformity may arise from several factors including non-interoperable equipment i.e. incompatible equipment, waste of engineering effort in preparing configuration databases, operational malfunctions, for example, accidental circuit breaker tripping or hazardous environment.

A Conformance Test of products, with positive outcome, validates that the functionality is in accordance with the requirements and assures a certain degree of safety and confidence to the users. Furthermore it helps users avoid unnecessary commissioning, test time, and resources. In other words, a product that has passed Conformance Test guarantees fulfilment of the basic compatibility and functionality requirements. It provides users with freedom to choose from a wide range of models and manufacturers. In addition, the end user has almost¹ the guarantee that its device will interoperate with various other devices with an attestation of conformity for the same international standard. In the case of legacy proprietary systems, conformance testing will enable users to create local standards that allow other manufactures to emulate the proprietary system, to ensure future system survival.

¹ Full certainty of interoperability between the individual conformance tested products can only be realized when the 'freedom space/optional features' of the involved protocol standard in the products has not been used at all. In all other cases extra interoperability testing is necessary based on the project related choices of the protocol standard which are normally laid down in a project specific Protocol Implementation Conformance Statement (PICS)

In short, the role of conformance testing is to reduce anguish and optimise use of resources in an organization for the larger part of a systems lifecycle.

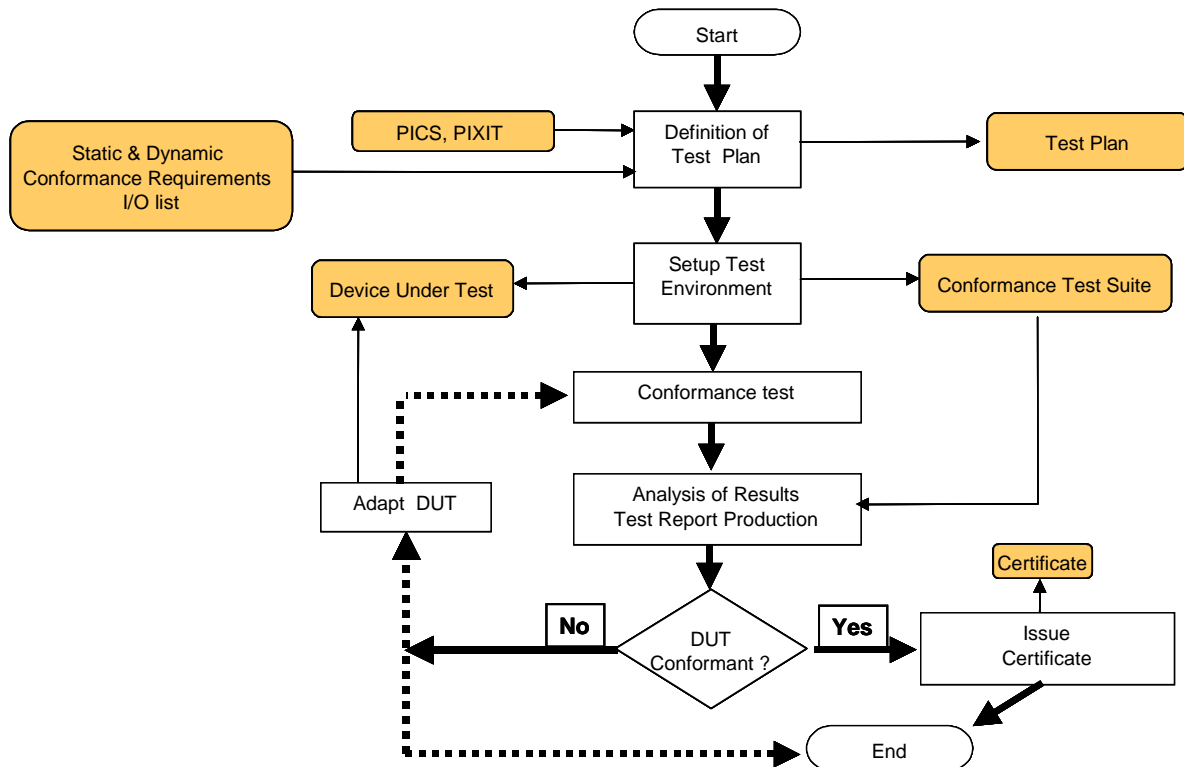
2.3 Conformance test approaches

2.3.1 Definition of Conformance

According to ISO, a conforming item is equipment or a product that exhibits behaviour conforming to the specifications of an applicable standard. Thus, in the case of protocol conformance test, the equipment shall meet conformance requirements as specified in a protocol standard. Normally, conformance specifications can be expressed positively i.e. what to do and negatively, what not to do.

2.3.2 Conformance Test Process

In general, conformance testing addresses the functional (static test) and performance requirements (dynamic test) of the device under test (DUT)². For an overview of the different steps of the conformance testing procedure see next picture.



To perform the conformance test, the test facility needs from the equipment manufacturer:

- Protocol Implementation Conformance Statement (PICS);
- Protocol Implementation eXtra Information for Testing statement (PIXIT);
- A sample device, configured for the test
- Ancillary software/hardware and engineering support during the test to configure, control, and query the device when necessary

² For example a DUT could be a device or system which communicates with a Substation Automated System or with a Control Centre

A conformance test uses the Conformance Test Suite as basis for the testing process. It forms the informal test specification. The formal test specification is for example the suite of the ‘application layer’ of the associated standard protocol. Each suite is normally divided in test groups (program unit for a particular feature) and each test group consists of several test cases (program routine for a particular aspect). The conformance test consists of a collection of test cases drawn from a standard in such a way as to test each feature and communication service for which support is claimed (positive test). Furthermore an appropriate response is expected in the following cases:

- Erroneous objects or services
- Object and services not implemented (negative test)

2.3.2.1 *Static Test*

Static conformance test validates the declaration that a DUT conforms to a standard in a standalone environment. As the name implies, static testing mainly involves review of relevant documentation, physical inspection of DUT and simple validation that the DUT performs as declared when connected. Most standards allow options to tailor a protocol for particular implementation or requirement. An implementer would then use the already mentioned PICS form to select relevant options for implementation. The PICS form usually accompanies a protocol standard. Initial activities in a static test would be:

- Review PICS document: Determine options that are declared supported and match user requirement to the options
- Review equipment configuration: Prior to further testing, equipment-specific parameters must be made known and established. ISO admits implementation specific information in the Protocol Implementation Extra Information for Testing (PIXIT)
- Review of datasheet or other equipment type test document: Determine environmental, system or logistical requirements of the equipment matches user requirements

Basic equipment information may be recorded, for example, equipment model number, firmware or software version number and file checksum (CRC checksum of binary executables). When the reviews are satisfied the static test can proceed to further activities of basic interconnection testing and capability testing.

2.3.2.1.1 *Basic Interconnection Test*

Basic interconnection test validates that a DUT can establish sufficient conformance for interconnection without performing thorough testing. The motivation for basic interconnection test is to reduce testing cost, before more elaborate and expensive tests are performed on the DUT. Depending on equipment availability, test tools maybe required. A protocol simulator, which instigates or responds to data exchanges, is physically connected to the DUT. The simulator requires a user interface to monitor and observe data exchanges. On the other hand, the DUT can be physically connected point-to-point to the actual equipment.

The equipment is treated as a black box. A conformance tester observes the input and output of the equipment. Input and output typically consists of digital signals, analogue signals, digital outputs, analogues outputs or serial data streams.

The following items of interest to this test are as follows:

- Basic request and response: The tester observes LED indicators to examine whether steady stream of data exchange is established after device initialisation.
- Event transmission: Stimulus is applied to the DUT and the resulting outcome is observed at the simulator or the monitoring end
- Command transmission: Command is sent to the DUT from the simulator and the resulting outcome is observed at the simulator or monitoring end.

2.3.2.1.2 *Capability Test*

Capability test verifies the conformance of implemented options to those declared in the PICS. In addition to a protocol simulator and physical plant injection, a protocol analyser is used to log and decode message transactions that occur on the physical connection. The following activities will be performed by this test:

- **Validate communication services:** Validates the DUT implements communication services as specified by the standard. The procedure would include examination of protocol frame format, flags, message structure etc. that the DUT must adhere.
- **Feature testing:** Feature testing validates the level of application of communication services meeting the requirements of target system. For example a system refresh is satisfied by the station interrogation command.

2.3.2.2 *Dynamic Test*

Dynamic test validates that a DUT conforms to a particular standard in an integrated environment i.e. in the presence of other equipment operating with a similar standard. The validation criteria evaluate dynamic aspect of the equipment, for example, correct DUT behaviour, presence or lack of timing delays and correct behaviour of other equipment that interacts with the DUT. Redundancy handling and regressing testing could be also part of the dynamic test.

It should be noted that acceptance criteria for dynamic test might vary depending on user needs because standards generally do not define acceptable performance or behaviour of DUT except in critical areas. However, successful completion of static test should be the pre-requisite before commencing dynamic test.

If possible, dynamic test should be conducted in an environment similar to the actual operating environment. In this case, the dynamic test would validate end-to-end result of the test that manifests on actual equipment, for example, all information from the actual RTU's to the SCADA dispatcher display. Acceptance criteria for dynamic test in this type of environment would normally be influenced by how well the DUT assimilates and interacts with existing equipment.

Dynamic testing overlaps for a small part the so-called interoperability testing. Within interoperability testing, the behaviour when working with other implementation is tested. Does the DUT work with other devices?

2.4 *Who can do conformance tests?*

Of course the manufacturers should perform tests during the development of the device to ensure the device will pass any third-party conformance test. Some (large) users will have their own test lab and qualified personnel that are capable to do conformance tests. Users and manufacturers without a protocol test lab can rely on unbiased independent test facilities that can perform conformance tests. For proprietary communication protocols, utilities have to engineer their own Conformance Test plan and procedures. It is in the utilities' best interest to ensure that the proprietary system documentation contains adequate detail and depth on the system interfaces. As an alternative, utilities will probably have to hire a data communication specialist to develop and define system interfaces by re-constructing behaviour from the live system.

Nevertheless, any test facility should perform the test according to a "conformance test quality plan", which meets the requirements of the involved standard and contains:

- The measures for the scope of work and/or deliveries in the area of budget, organization, time, information and quality
- A complete and detailed description of the work methods, all tasks to be performed and

organization

- A method for handling deviations, changes and modifications during all stages of the test
- A sign off procedure and description of the documentation to be supplied
- A test and inspection plan describing what will be tested, the purpose and expected result of the test, the test procedures and standards, and by whom the test will be performed

2.5 At what time should conformance test be performed?

The conformance test is the type test for a communication protocol and does not replace the project specific system tests such as the factory (FAT) and site (SAT) acceptance test. They should normally not be part of the project itself but should already be covered by the vendor before a tender process for a customer starts. It should be (in the ideal situation) a responsibility of the vendor of the communication devices. In cases that such testing in an early stage (before the project starts) is not possible then the conformance tests should be part of the project in the so called pre-FAT phase, but preferable as early as possible in order to minimize user losses and investment risks due to future identification of inadequate performance, operation or interoperability based on the applicable standard.

For proprietary protocols, the issue of conformance test arise when a utility needs to validate that a vendor has successfully interface to an existing system. In this case the vendor will normally expect the utility to provide detail information on the interface. In order to avoid protracted contractual problems due to unavailable information, it is advisable for the utility to outline the scope of interfacing work to include investigation on the existing interface and conformance test of the interface.

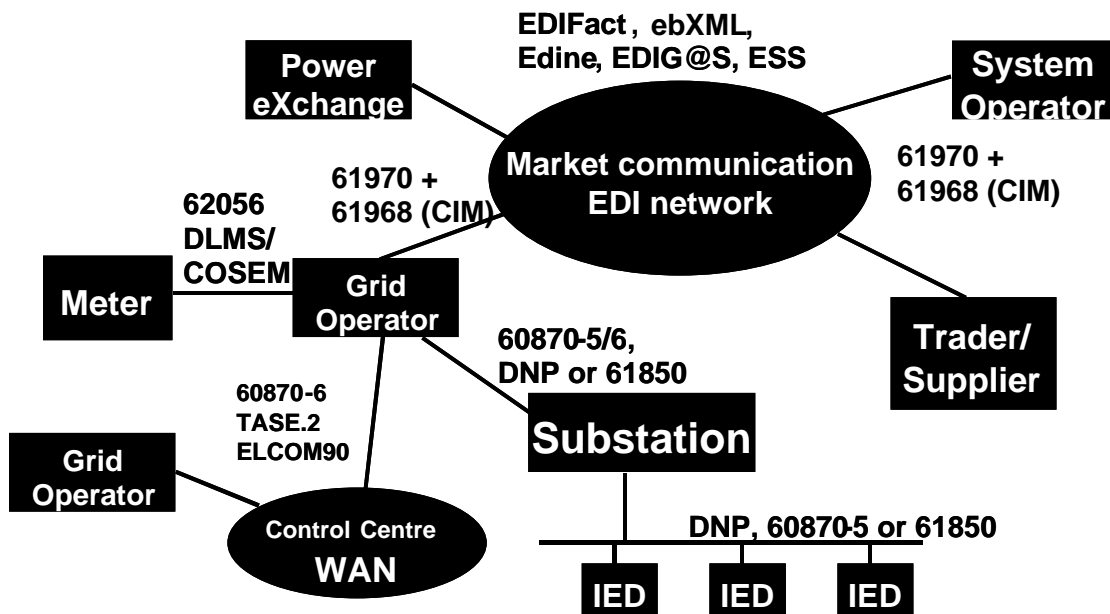
The vendor also must be prepared to interact with manufacturer of existing proprietary system. Judging from experience, this is also true even for standard IEC TC57 protocols for example on systems that use early versions of IEC 60870-5-101 or for uncommon implementation of the standard like the balanced-mode implementation of IEC 60870-5-101. Clarification and conformance testing may also be needed when implementing obscure information objects for example implementation of Binary Coded Decimal (BCD), file transfer or even double-bit information in DNP 3.0 for example. In this regard, the utility must ensure that the proprietary system manufacturer allow disclosure of proprietary technical information for the purpose of internal company use and extending system lifetime.

3 PROTOCOL AND CONFORMANCE TESTING OVERVIEW

The working groups in TC57 have worked out several protocols in response to the need of utilities worldwide. This chapter gives an overview of existing IEC TC57 standards for which conformance testing will be handled in more detail in this technical report.

The users benefit the most from standardisation, but suppliers also recognize that standardisation is beneficial. This is amongst others due to the shorter life cycle of new technologies. And using standards can be an important aspect for achieving an acceptable ROI³.

A global overview of these (de-facto) standard protocols and their usage area is pointed out in the picture below⁴:



The following de-facto and IEC standard protocols as well as a proprietary protocol are covered:

- 1) IEC 60870-5 companion standards 101, 103 and 104
- 2) IEC 61850
- 3) DNP (USA de-facto standard)
- 4) DLMS COSEM (IEC 62056 metering standard)
- 5) TASE.2 (IEC 60870-6)
- 6) ELCOM-90 (de-facto standard IEC 60870-6)
- 7) Edine, EDIG@S, ESS ETSO (trade messages), ebXML
- 8) CIM model (IEC 61970 and IEC 61968)
- 9) WISP+: An example proprietary protocol

³ ROI=Return On Investment (pay back period).

⁴ In some countries the utilities are not organised like a ‘System operator’ and ‘Grid Operator’. In those countries we see for example only one utility with a National Control Centre and various Regional Control Centres

3.1 IEC 60870-5 companion standards

IEC 60870 series introduction

End 80's there was a need for an open communication protocol for telecontrol purposes. This has led to the development and completion of the IEC 60870 protocol series in the 90's. The completed so-called Companion Standard is:

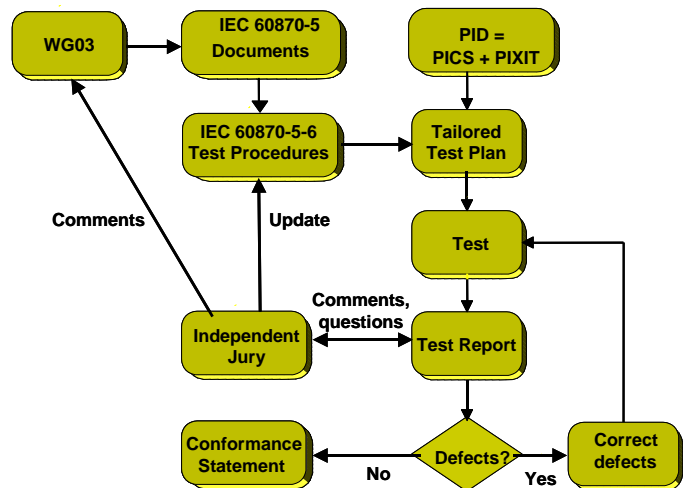
- IEC 60870-5-101 Companion standard for basic telecontrol tasks
- IEC 60870-5-102 Transmission of integrated totals in electric power systems
- IEC 60870-5-103 The informative interface of protection equipment
- IEC 60870-5-104 Network access for IEC 60870-5-101 using standard transport profiles

These protocols have nowadays a high installed base in Europe primarily and the rest of the world except Northern America. North America uses DNP (with reference to a paragraph in this document) for the same purposes and is basically based on the IEC 60870-5 basic documents. Both protocols are together the world standard for telecontrol tasks. The IEC Technical Committee 57 Working Group 3 is responsible for the documents and is still working on enhancements and maintenance.

Current status regarding protocol testing

The responsible Working Group 3 is now working on the following documents:

- IEC 60870-5-6 Guidelines for conformance testing for the IEC 60870-5 companion standards
- IEC 60870-5-601 Conformance test cases for the IEC 60870-5-101 companion standard
- IEC 60870-5-604 Conformance test cases for the IEC 60870-5-104
- Consideration is the Conformance test cases for Companion Standards 102 and 103, but not planned.



Available documentation, tools and existing test labs

Documentation can be found at www.iec.ch website and standard documents can be bought via the national committees.

Several tools, software stacks are available on the website. For different users there are applicable tools. From comprehensive simulator tools capable to simulate Normal and Reversed direction communication and several redundancy architecture concepts, practical Simulators & Database testing tools to speed up acceptance testing, analysing tools with and without error detection are freely available on the market.

Services to assist utilities, vendors, and system integrators in starting up and using the 60870-5 Companion Standards are training, interoperability testing, conformance testing, communication stacks and problem investigation.

There are existing test labs available to perform interoperability and conformance testing off- or on-site as a vendor and as vendor Independent test laboratory with international acceptance. No formal accreditation of test-labs is available.

Practical experiences with conformance testing

Mid 90's a New Work Item Proposal (NWIP) to set-up conformance test procedures was rejected. In 00's it was issued again and accepted. Why? Several reasons, but an important one was that the experience in practice has proven that conformance testing is an important step in quality control. In these 90's a private supplier independent party started to set-up conformance test procedures because they were asked by utilities. It started with approximately 40 pages and is after lots of tests 130 pages for only one Companion Standard. Lots of experiences are in these test plans and have also increased the quality of the next edition(s) or amendments of the standards.

Experience has learned that conformance testing pays back because problems are detected in an early stage. At a FAT or SAT it is not the goal to detect communication problems, but test on functional level. This means that you have to banish communication problem to an earlier stage, the conformance test. The table⁵ below shows the sequence of the tasks of the different test phases in the project execution.

Phase	Mile stone	Goal of the test in the specific phase	To detect following errors
Define/choose Project(s)	<i>Company priority</i>		
Protocol specification	<i>RFQ</i>		
Tender	<i>Order</i>		
Manufacturing	<i>Conformance test passed Y/N?</i>	<i>Protocol implementation according PID</i>	<i>Protocol errors & Mismatches</i>
FAT/SAT plan and Test Procedures from vendor	<i>Approval from the customer</i>		
Pre-FAT	<i>IOA addresses in SAS & CC test passed Y/N?</i>	<i>Configuration IOA in SAS and CC</i>	<i>IOA mismatches</i>
FAT	<i>Ship Y/N?</i>	<i>Functionality SAS & CC separately from each other</i>	<i>Lacks of functionality of SAS & CC separately</i>
First availability test with short duration	<i>Oke Y/N?</i>		
SAT	<i>In operation Y/N?</i>	<i>Functionality SAS & CC together</i>	<i>Lacks of functionality of the connection end-to-end</i>
Commissioning		<i>Functionality SAS & CC together</i>	
Second availability test with long duration	<i>Oke Y/N?</i>		
DUT/system in operation and warranty period starts	<i>Only if long availability test passed</i>		

Last few years the number of IEC (conformance) tested protocol implementations have increased. More than 50% of the first tests failed due to a) non-conformant behaviour; b) reasonable cause for interoperability problems; c) a reasonable cause for expecting operational problems. An example is: E.g. a complete area may suffer from a blackout after sending a break-off command by the control

⁵ SAS=Station Automated System; CC = Control Centre; IOA=I/O addresses used in 60870-5-101 and 104 standard

centre (which means ‘do not switch’), after which this command is false interpreted by the substation control system and executed as a normal command.

Detecting protocol communication mismatches pay for both utility and supplier. For a utility by better control of the planning of a project and reduce the outage time necessary for commissioning to the minimum and controllable. For the vendor it is a matter of reputation (no errors in the field) and costs for solving the problem on-site. Only from costs point of view conformance test is beneficial if it reduces twice (may be even only once) the costs of fly an engineer local to solve the problem.

What do you need for a conformance test? This is necessary but the question how a utility wants to use the protocol in its company is more valid. A Protocol Implementation Document (PID=PICS+PIXIT) is mandatory to have. It does not rewrite the standard, but only what optional parts of the standard are used, how to deal for example with redundancy etc. It is simply not enough to require from the vendor e.g. an IEC 60870-5-104 implementation. Interoperability is definitely not guaranteed.

The experiences with the IEC 60870-5 series was one of the reasons why writing the IEC 61850-10 conformance testing was not an issue, it was mandatory.

3.2 IEC 61850

IEC 61850 introduction

The goal of IEC 61850 is to achieve interoperability of intelligent electronic devices (IED) in substations, distributed energy resources (DER), wind-power plants and hydroelectric power plants. In general, IEC 61850 provides:

- Standardized information models for things like circuit-breakers, transformers, and so forth
- Information exchange methods to access the data of the information models, report sequences-of-events, log historical data, control devices, sampled value distribution, fast peer-to-peer process data exchange, etc.
- A unified system configuration language (XML based) and device online self-description.

This concerns the following applications: protection, monitoring and control, integration of innovative sensor and switch technologies, metering, supervisory control and data acquisition (SCADA), remote monitoring and fault diagnosis, automated dispatch and control, asset management and condition monitoring and diagnosis.

Current status regarding protocol testing

Conformance testing is an important part of the quality assurance process (see figure 3.2).

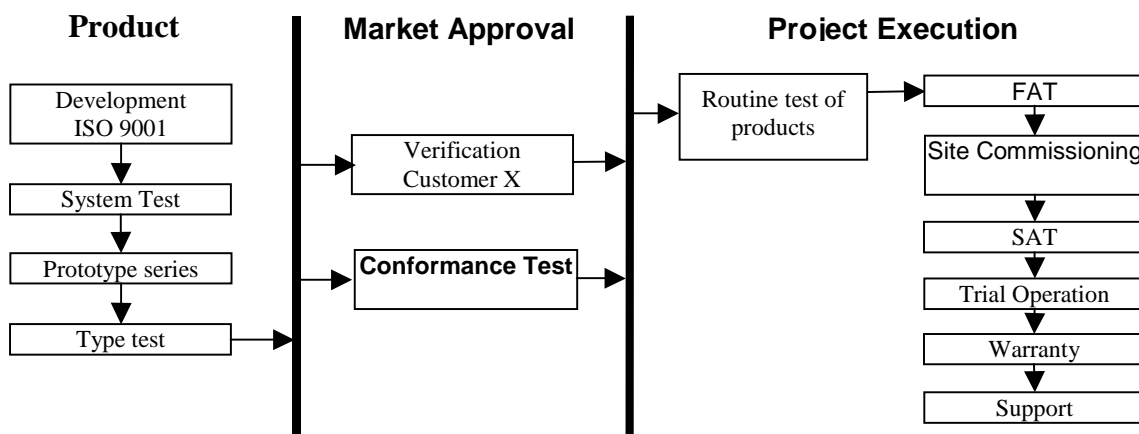


Figure 3.2 - Quality assurance stages (IEC 61850-4)

To ensure and verify interoperability the standard includes IEC 61850 part10 “Conformance testing” [4], describing how to perform a conformance test. The UCA international users group (UCA IUG) used part 10 to set-up more detailed test lab accreditation procedures and device test procedures. The first conformance tests of IED’s have been performed in 2005.

Available documentation, tools and existing test labs

The IEC 61850 part 10 has reached IS status in March 2005. The IS version will be available from www.iec.ch. Members of the UCA IUG can download the test lab accreditation and device test procedures from www.ucausersgroup.org. KEMA has been accredited by the UCA IUG as test lab to perform independent third party conformance testing and issue certificates. KEMA also provides an optimised conformance test set and IEC 61850-protocol analyser to support and automate conformance testing. Since 2000 the IEC 61850 user group is part of the already existing international UCA User Group.

Practical experiences with conformance testing

For 8 IED devices, conformance tests according to IEC 61850 part 10 and the UCA IUG device test procedures have been performed in 2005. All these tests failed the first time. This resulted in several technical issues related to the IEC 61850 standard, the UCA IUG test procedures and conformance test systems. The IEC TC57 working group 10 manages these issues concerning the standard. The UCA IUG test subcommittee manages the issues regarding the test procedures. The test system developers manage the test system issues.

It is impossible to test all system configurations using devices from different worldwide suppliers. Therefore, a standardized conformance test system (Figure 3.3) with equipment simulators should be used. The use of such a test system implies agreement about its configuration and the test procedures applied in order to achieve compatible results. Figure 3.3 gives a schematic view of the test configuration to test an **Intelligent Electronic Device (IED)** like a protection / control device. For other types of IEDs quite similar configurations will be applicable.

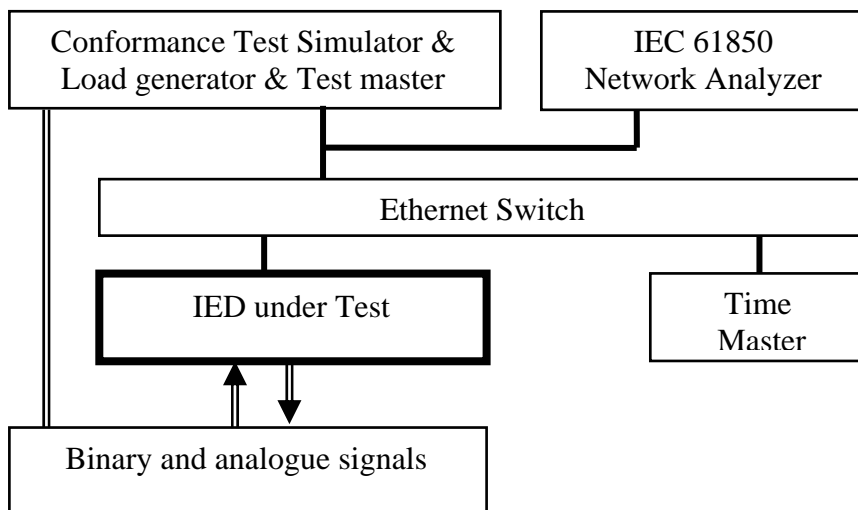


Figure 3.3 Test configuration (example)

To reproduce a representative set of error and stress situations, test facilities need an advanced & automated protocol conformance test simulator and test master. An accurate IEC 61850-network analyser is necessary to trace and analyse all communication messages on the Ethernet and to measure message response times. Also the necessary analogue/binary signals of the device under test need to be simulated, for example to force switchgear control and position errors by a switchgear simulator.

To support end-users in the selection and specification of the required subset of IEC 61850, the UCA international user group defined 14 conformance blocks. The supported and approved conformance blocks of an IED are specified on the certificate. The popular conformance blocks are:

- 1: Basic services
- 2: Data Sets
- 5: Unbuffered reporting
- 6: Buffered reporting
- 9: GOOSE (Generic Object Oriented Substation Events)
- 12a: Direct control
- 12d: Select before operate with enhanced security
- 13: Time synchronisation
- 14: File transfer

3.3 DNP3 De-facto standard (USA)

DNP3 introduction

DNP is also widely used outside of the USA and is the de facto standard in South Africa, Australia and New Zealand. DNP3 is a protocol for transmission of data from point A to point B using serial or TCP/IP communications. DNP3 is an open, intelligent, robust, and efficient modern SCADA protocol. DNP3's value for South Africa was mainly found in point-to-multipoint telecommunications networks and the value of its ability to operate in unsolicited mode especially in low bandwidth telecommunication networks. It has been used primarily by utilities like the electric companies, but it operates suitably in other areas. DNP3 provides the rules for slave station computers (servers) and master station computers (Clients) to communicate data and control commands. DNP was originally created by Westronic Inc. (now GE Harris) in 1990. In 1993, the protocol specification was released into the public domain. Ownership of the protocol was given over to the newly formed DNP Users Group in October of that year. Since that time, the protocol has gained worldwide acceptance but is most popular in the USA, Latin America and Asia.

Current status regarding protocol testing

There are a large number of DNP3 implementations all over the world. Therefore there is a large need for conformance testing. The DNP Users Group recognized this need and published an official Conformance Test policy and test procedures for DNP3 slave implementations. The conformance test procedures for master implementations are currently under development. The DNP3 organization recognizes that supporting every feature of DNP3 is not necessary for every device. Some devices are limited in memory and speed and do not need specific features, while other devices must have the more advanced features to accomplish their task. Therefore the DNP3 Users Group defined three conformance levels. At the lowest level, level 1, only very basic functions must be provided and all others are optional. Level 2 handles more functions, objects and variations, and level 3 is even more sophisticated. Within each level only certain combinations of request formats and response formats are required. This was done to limit software code in clients and servers while still assuring interoperability.

Available documentation, tools and existing test labs

The DNP Users Group (www.dnp.org) provides the official DNP documentation and conformance test procedures to all interested parties. No formal conformance test tools are available on the market but test tools are available which use the DNP users group test procedures as a basis. A number of test labs offer DNP3 conformance tests, amongst which KEMA, Subnet Solutions, Advanced Control Systems, and Reltronix. Most of the test labs use the DNP Conformance test tool developed by Triangle

Microworks. Their test harness can be used for factory acceptance testing, conformance testing of DNP3 implementations and to resolve communication issues.

Practical experiences with testing

During most conformance test performed by the available testing laboratories several DNP3 issues are detected and resolved by the manufacturer. This proves the need for conformance testing DNP3 implementations in order to ensure interoperability.

3.4 DLMS/COSEM (Metering standard)

DLMS/COSEM introduction

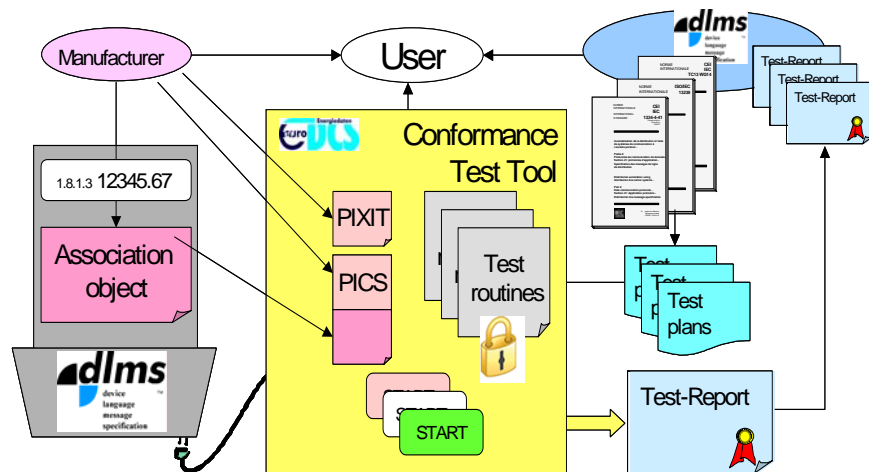
DLMS/COSEM is designed for the exchange of energy meter data of any kind of product (electricity, gas, heat, etc). It uses standardized objects to model all the information and functionality of the meter. To identify these objects OBIS codes are used which ensures that the meaning of the objects is always clear. At the moment only DLMS over a serial line is used, but the standard allows other transport layers as well, such as TCP/IP. For TCP/IP use the standard will be amended. XML support is under discussion within DLMS User association. The design is extensible and it supports plug and play.

Current status regarding protocol testing

For conformance testing [7] there is an official test system: the Conformance Test Tool of the DLMS User Association (see next picture).

The manufacturers can use this tool during the development and for self-testing.

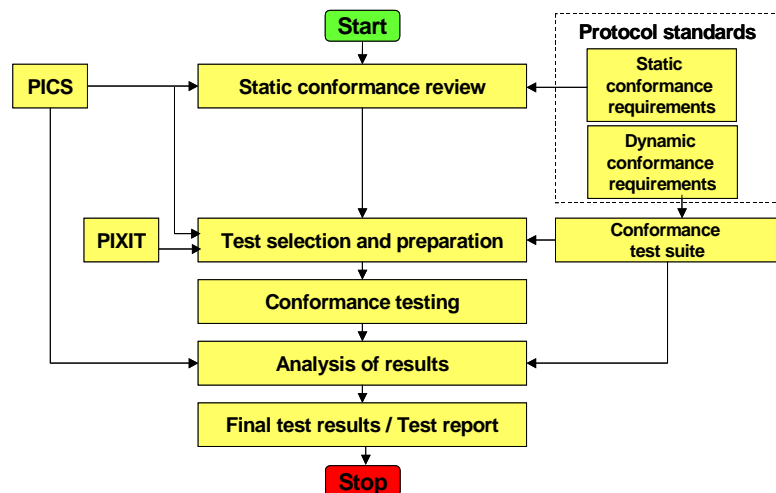
The testing process follows the procedure as drawn out in the picture below.



Currently there are 18 certified products of which 17 have certified by the manufacturer themselves and an independent party has tested only one.

Available documentation, tools and existing test labs

Information regarding the DLMS/COSEM standard documentation has been published at the DLMS User Association site



(www.dlms.com). There are 3 test laboratories that offer third party conformance testing, KEMA, CPRI and EuroDCS. The conformance test system can be ordered by EuroDCS (the developer in close cooperation with the DLMS UA (www.dlms.com) and is also the maintainer of the conformance test tool). Several DLMS services are offered. The DLMS User Association, KEMA and Landis+Gyr offer Training and consultancy. Two of the meter manufacturers (Actaris and Landis&Gyr) offer a DLMS protocol stack.

To be able to investigate the communication between two systems, KEMA has developed a protocol analyser that captures all the bytes and decodes it into easy to read text.

Practical experiences with testing

Mostly the vendors did their own conformance testing to solve problems within their own implementation. Conformance testing could be used during development phase of the product. KEMA has assisted several companies/vendors during the development phase and on regular times a test was performed and the results with advice to solve problems was reported.

3.5 TASE.2

TASE.2 introduction

The Telecontrol Application Service Elements 2 (TASE.2) protocol allows for data exchange over Wide Area Networks (WAN) between a utility control centre and other control centres, other utilities, power plants and substations. TASE.2 is based on the MMS protocol that is applicable in many industries and situations. The work on TASE.2 (also called ICCP, the Inter Control Centre Communications Protocol) was initiated by EPRI in the US as a part of the Utility Communication Architecture (UCA).

Current status regarding protocol testing

The number of TASE.2 implementations is relatively small. Therefore there is little need for conformance testing, because it's more economical to organize interoperability test. Such interoperability test haven been performed twice in the USA in 1996, participated by over 8 manufacturers.

Available documentation, tools and existing test labs

No formal conformance test tools are available on the market. KEMA has a TASE.2 test simulator that can be used for factory acceptance testing. Some users can install their TASE.2 software on a laptop that can be used to set-up new links. Many TASE.2 users use KEMA's TASE.2 protocol analyser to detect and resolve communication issues.

Practical experiences with testing

During each factory acceptance test performed by the available testing laboratories several TASE.2 issues are detected and resolved by the manufacturer. Because there is no formal conformance test the factory acceptance test should include the TASE.2 communication testing. Many users have difficulties to set-up new TASE.2 links. With help of the TASE.2 analyser they can quickly detect the cause of the problem and resolve it or ask for support.

3.6 ELCOM90

ELCOM90 introduction

The ELCOM90 protocol has been standardized as Telecontrol Application Service Elements 1 (TASE.1) protocol. Its usage area covers the data exchange over Wide Area Networks (WAN) between a utility control centre and other control centres, other utilities, power plants and substations. TASE.1 is never used in practice but the ELCOM90 standard is still used worldwide with the focus on

the Northern part of Europe. Originally the protocol was founded in 1983 by EFI, now Sintef, in close cooperation with the SCADA vendors Siemens and ABB and different Northern Electricity Utilities.

Current status regarding protocol testing

Conformance testing was done by EFI (Sintef) mainly in the time period from 1983-1998, and the target group are the Northern European Utilities. KEMA developed in 1993 a comparable 'conformance' test system but their target area was focused on the Dutch and Belgian regions and the other European countries. In the year 1998 both conformance test systems were verified against each other. The conclusion was that there were small differences seen regarding the testing protocol functionality. Furthermore the amount of test cases in the KEMA test system related to negative testing was quite large in relation to the Sintef 'conformance' test system for ELCOM90.

Available documentation, tools and existing test labs

Both testing systems of Sintef and KEMA are not formal conformance test tools. KEMA developed an ELCOM analyser as a tool during interoperability testing, which can also be used during FAT, and SAT testing. Documentation related to ELCOM see [6].

Practical experiences with testing

During each 'conformance' test performed in the past, several ELCOM90 issues were detected and were resolved by the manufacturer. When a new vendors ELCOM90 implementation was the system under test (SUT), in several cases the conformance testing could not be finished because of the large amount of non-conformity items found by the test facility. But after some years and after different retesting of a vendor's implementation the amount of issues was only related to functionality, which was not specified clearly in the standard. Therefore the so-called PID document was defined to specify the freedom aspects of the protocols on a project base. The PID is like the PICS document as nowadays used for the new standard protocols and conformance testing.

3.7 Market protocols Edine, EDIG@S, ESS

Introduction to market protocols Edine, EDIG@S, ESS

Years ago the energy supply industry was a rather stable technical oriented business area. The de-regulation of this market, that started around 1995, caused many changes in such a way that most markets are still finding their optimal structure. The structure such as the role of and relation between System Operators, Grid operators, Balance Responsible Parties, Market Operators etc. and presence of Regulators differs from country to country and still is changing. Commercial trading with many similarities to the financial markets has been introduced, where in early stages the technical expertise was ruling the game.

De-regulation of energy markets has lead to tremendous growth of message exchange between existing and new market players: System operators, Grid operators, Power Exchanges, Power Generators, Suppliers, Traders, Metered Data Collectors, etc. Where first information was exchanged between different processes within a utility, now pre-defined messages must be exchanged between different market players. With the increasing number of consumer groups that have a free choice of supplier also the number and size of messages exchanged between two market players increases. This trend imposes heavy requirements on functionality, performance and security of the communication networks used.

A necessary condition for a market to be really open and make it easy for new companies to enter the arena, is standardization of the message exchange so new players can easily enter existing markets. Electronic Data Interchange (EDI) is the acronym used to indicate inter or intra company messages exchange making use of IT systems and digital data networks.

EDIFACT is one of the early formatting techniques defined by UN/CEFACT to create open trade markets. In the energy industry this formatting standard was embraced by the European Gas

Transmission Companies to create the [EDIG@S](#) standard, now being used for communication among and with the Transmission System Operators. In the early stages of the NORDEL market EDIFACT was the basis of its EDIEL communication infrastructures. In The Netherlands it was the basis for the EDINE standard and in Germany for the VDEW message definitions. The typical approach of message standardization nowadays is still a national one: most countries create their own standard. Although the basis is the same (EDIFACT) the resulting messages and transaction schemes are different. This approach hinders the opening of global markets and that's why international initiatives are taken to work towards international standardization.

With the increasing use of the Internet and its associated techniques, XML message formatting is gaining popularity. Also UN/CEFACT started working on a successor for its EDIFACT standard: ebXML (IEC 621195 "Power System Control and Associated Communications-Deregulated Energy Market Communications").

There is a trend to slowly replace EDIFACT messaging with XML messaging. New standards for exchanging schedules are already formatted in XML. The issue of migration is an important one because the industry already invested substantial amounts in conventional standards such as EDIFACT. The power industry will be reluctant to accept new standards when advantages are not very clear and no smooth migration is offered.

The European Transmission System Operators (ETSO) released a market model and among others an XML based message structure released in 2002 for the exchange of schedules (the ESS standard). This standard is used among others in France, Germany, Switzerland and Austria starting in 2003.

The European Federation of Energy Trading companies (EFET) defined, also in 2002; an XML based messaging system for exchange of deals and confirmations.

Technical committee 57 of the IEC defines communication protocols for the power industry. Working Group 16 of IEC TC57 finished a communication infrastructure definition with an example implementation based on ebXML early 2003. This infrastructure comes along with migration paths for existing EDIFACT based networks.

So EDI standardization activities are taking place and show a trend towards global solutions based on internet techniques.

Current status regarding protocol testing

The advantages of using EDI standards are numerous:

- Enable hybrid IT infrastructures (different IT suppliers)
- Create open markets
- Availability of migration paths
- Availability of expertise
- Etc.

Another important advantage is that test facilities are commercially available to analyse message formats (syntax), the meaning of the data (semantics) and transaction flows and prove that vendor implementations are working according the standard.

Finally a new communication partner being connected could disturb a stable network.

The chance that problems, mentioned above, cause strategic and economic damage will substantially decrease by performing conformance tests in front of connecting new participants to an operational network.

Vendors can use EDI interface testing facilities to test their products in an early (development) stage to see if they are on the right track. This possibility will save them development costs. EDI interface testing is extra valuable when new standards, new messages or versions thereof are introduced. In the early life cycle phase of a new standard (version), the testing activity will discover interpretation differences in products, ambiguities and 'holes' in the standard. Feedback to the organization that maintains the standard is then well received and will improve the specifications and support the introduction of the standard.

With respect to testing, different approaches can be recognized such as interoperability testing, conformance testing and performance testing.

With interoperability testing the possibility of data exchange between systems of different vendors is evaluated. If communication is possible the test result is positive. This does not imply that the data exchange is working according standard specifications.

Conformance testing will reveal if vendor's implementation is complying with the standard specifications. To be able to prove compliance, vendors system is connected to a reference test system that is maintained by a test organization. When implementation differences occur the organization that maintains the standard specifications will take a decision. After that the party that made a wrong interpretation will change its implementation. In most Power markets, TSO's will do certification of the market participants that have to communicate with them. In front of this participant certificate the vendor can have its IT system certified to gain the trust in his product and advertise compliance in the market before the product or new version is installed. For this product certification a separate (vendor independent) testing facility is needed. Also some TSO's may not certify message exchange between participants not involving themselves, what also implies the need for a separate testing facility. Performance testing evaluates the IT systems behaviour in stress situations. In is particular the case when after a communication breakdown, a backlog of messages has to be processed.

An initiative of German vendors and consultants was founded in the year 2000 to support the implementation of national and international EDI standards. Early 2006 the EDNA launched the EDNA International working group. This working group will focus on European energy market communication protocols. Besides knowledge transfer activities and support of standardization efforts, EDNA has introduced a certificate for EDI implementations of its members in order to practise their slogan: "We just make it work".

Available documentation, tools and existing test labs

EDINE: TenneT the Dutch TSO for electricity and all market parties uses EDINE messages to exchange data. The EBO is the Dutch National organization for creating and maintaining all EDINE messages. These EDINE messages are described in so called Message Implementation Guides (MIG's) or UNSM models. These EDINE MIG's and models are subsets from the EDIFACT standard. These EDINE messages are used to exchange data concerning balancing, measurements, trades, etc. EDINE stands for EDI in the Dutch energy sector. These messages are exchanged over a by TenneT owned and maintained communication infrastructure. Since 1st January 2005 the Dutch regulator DTe has obligated all market participants to test and certify their EDINE interfaces to achieve an open, transparent and interoperable electricity market. In addition to this the DTe has assigned TenneT as the party who is responsible for testing and certification of these EDINE messages. Because of this TenneT is implementing a new test and certification facility to certify all market parties.

EDIG@S: Since 2004 the Dutch system operator for gas in The Netherlands, Gasunie transport services, and all market parties uses the EDIG@S standard to exchange EDIG@S allocation and reconciliation messages. UN/CEFACT is responsible for creating and maintaining the EDIFACT standard. The European EDIG@S commission defines Message Implementation Guides based on the EDIFACT documents that are suitable for the gas sector. In The Netherlands the EBO working group Gas is responsible for defining how these MIG's are used in the Netherlands. The EBO is also responsible for maintaining these documents also called templates. The messages are exchanged over a Private Virtual Network and signed and encrypted with the Applicable Statement 2 protocol AS2 between the Dutch TSO (Gasunie transport Services) and market participants as shippers, suppliers and regional system operators. The Dutch TSO for gas has obligated EDIG@S conformance testing before connecting to the production environment. Because all AS2 implementations delivered by suppliers who also deliver an EDIG@S implementation are already conformance tested and certified by the "Drummond Group" only an EDIG@S conformance test need to be performed. For the Dutch gas market KEMA has created and operates an EDIG@S test and certification facility that is available for all market participants that are connected to the VPN.

EFET is the European federation of energy traders and have defined an XML based electronic confirmation and matching standard eCM. EFET uses ebXML as the transport layer to exchange EFET eCM messages. The EFET eCM standards consist of the definition of the exact message flow, message content and message structure for the information exchanged during an eCM process. The EFET eCM Project Workgroup is responsible for creation, maintenance and version control of the eCM standard. EFET is in the process of obligating all vendors and participants to perform a conformance test.

Practical experiences with testing

Since early 2004 both market participants and Gasunie transport Services have acquired experience in conformance testing their EDIG@S implementations against KEMA's test and certification facility. In general, feedback from participants was very positive. From Gasunie transport service, which is responsible for a smooth migration phase, also positive feedback was received. No problems on protocol level occurred.

The EDNA initiative asked KEMA to create a test facility for EDI interfaces. This facility is now available and is able to test interfaces based on the ETSO ESS standard. Message exchange takes place over the internet and can continue 24 hours per day 7 days per week.

Users can choose out of about 150 different transaction scenarios for development testing. In addition to other EDI testing services available on the market, this facility is able to test specific energy related transactions such as nomination and allocation and check the contents of the messages according the specific energy industry standards and regulations.

In order to receive a certificate, EDNA specified the procedure and obligatory scenarios.

The test facility can easily be extended for other message formats (EXCEL, EDIFACT, ebXML) and transactions whenever the market requires such testing.

3.8 CIM

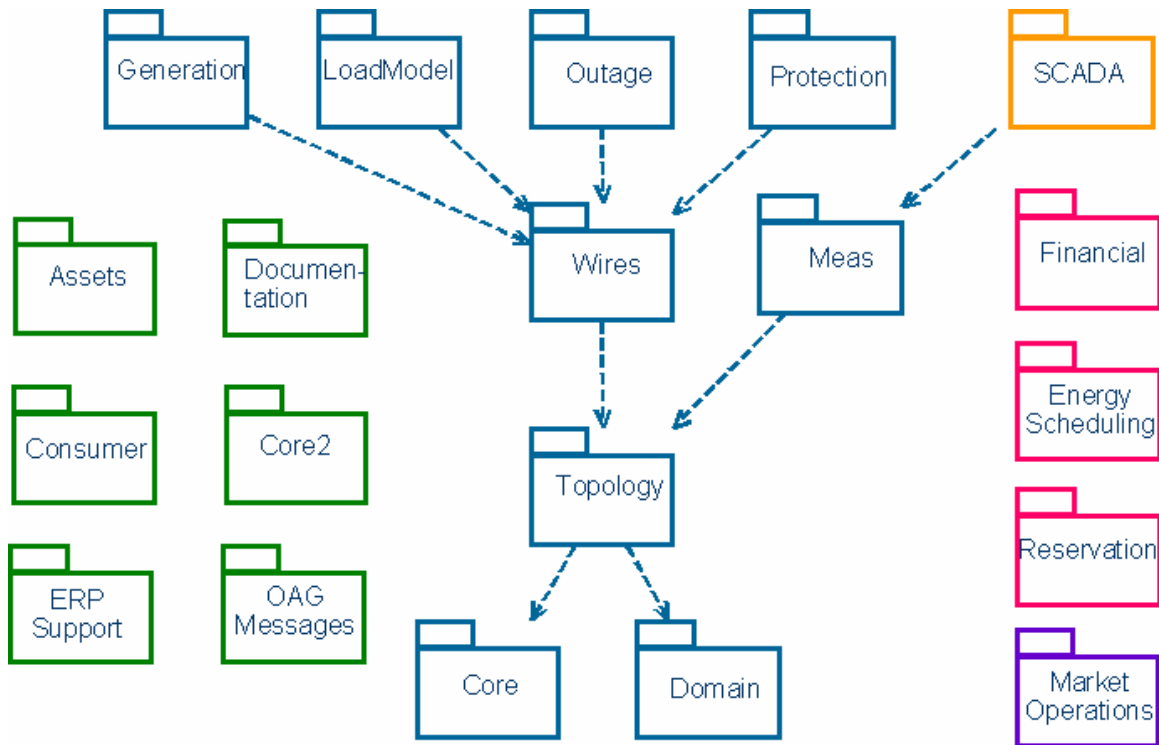
CIM introduction

The Common Information Model (CIM) is defined in the IEC61968 and IEC61970 standard. The goal of the IEC 61968 standard (TC57 WG14) is to facilitate inter-application integration of the various distributed software application systems supporting the management of utility electrical distribution networks. The goal of the IEC61970 standard (TC57 WG 13) is to reduce the cost and time needed to add new applications to an EMS or other (real-time) system and protect the investments in existing application functions that are working effectively. Furthermore it seeks to improve the capability to exchange information in the control centre environment.

While IEC61968 is focusing on inter-application integration, IEC61970 is focusing on intra-application integration. Intra-application integration is aimed at programs in the same application system, usually communicating with middleware that is embedded in their underlying runtime environment, and tends to be optimised for close, real-time, synchronous connections and interactive request/reply or conversation communication models. IEC61968, by contrast, is intended to support the inter-application integration of a utility enterprise that needs to connect disparate applications that are already build or mew (legacy or purchased applications), each supported by dissimilar runtime environments.

Current status

The component standard describes the interfaces and not the functions. The interfaces cover both semantics and collection mechanism (CIM) and the technical implementation options. The first available results are the guidelines document and implementation framework and the CIM base object definitions and usage glossary. Among others, the document IEC61970-301 has reached the IS status in 2003. Work on energy scheduling, SCADA etc. is under development. Next picture below describes the CIM UML packages.



Available documentation, tools and existing test labs

In order to achieve the intended advantages, compliancy of the implementation to the standard must be ensured. Therefore EPRI is sponsoring interoperability tests since 2000. The objectives of the interoperability tests are to: 1) demonstrate compliance with the standard and 2) demonstrate interoperability of different vendor products based on the CIM XML standard. Scope of the tests is among others: CIM XML power system model transfer, CIM GID and parts of the IEC61968 message standard.

Since 2005 The CIM User Group is merged into the UCA International User Group.

A new CIM compliance testing task force is established in order to accelerate interpretation, implementation and procedures for conformance testing. CIM conformance means that at the public interface the data-representation and messages/data exchange complies with the CIM in terms of semantics (naming and meaning of data), syntax (data types and format) and relational aspects.

UCA International Users Group Organization



The documentation stack for the IEC 61968 standard is listed below.

- Part 1: Interface architecture and general requirements
- Part 2: Glossary
- Part 3: Interface standards for network operation
- Part 4: Interface standards for Records and Asset management
- Part 5: Interface standards for Operational Planning and Optimization
- Part 6: Interface standards for Maintenance and Construction
- Part 7: Interface standards for Network Extension Planning
- Part 8: Interface standards for Customer Inquiry
- Part 9: Interface standards for Meter Reading and control
- Part 10 Interface standards for Systems external to, but supportive of, distribution management

The documentation stack for the IEC 61970 standard is listed below.

- Part 1: Guidelines and General Requirements (status: IS)
- Part 2: Glossary (current document is CDV)
- Part 3XX: Common Information Model
- Part 301 - Electrical network classes for topology, wires and generation (status: IS)
- Part 302 - Defines energy trading and scheduling (deregulated operation)
- Part 303 - Covers supervisory control and data acquisition (SCADA)
- Part 4XX: Component Interface Specifications (CIS)
- Part 401 - Component Interface Specifications Framework
- Part 402 – 449 Common Data Access (CDA) for specific services
- Part 450 – Renormalized CIS Exchange Model
- Part 451 – 499 Specific information exchange requirements
- Part 5XX: CIS Technology Mappings
- Part 501 - Interface Model - Data Access Facility (DAF)

Practical experiences/References

The IEC TC57 WG13/14 maintains close cooperation on the CIM topic with various partners (listed below) and participates in international standardization groups (OMG, OPC etc.):

- North American Electricity Reliability Council (NERC) Security coordinators.
- Object Management Group (OMG) Utilities Domain Task Force (DTF)
- European Community IST 30067 Project “ScadaOnWeb”

Actual implementations of the CIM protocol are listed (incomplete) below. Various suppliers implement CIM data models to their new product lines (excluded):

- British Columbia Hydro of Canada: Voltage Stability Analysis
- China Light and Power Company, Hong Kong: Data Repository System
- ONS, Brazil: Operator Training Simulator
- California ISO: Energy Management System Replacement
- Commonwealth Edison Florida: Operator Training Simulator
- East Midlands Electricity (UK): Inter-application Integration
- NEPCO Jordan: Open Application Integration Platform
- Public Service Companies of New Mexico: Maintenance System

3.9 WISP+: An Example Proprietary Protocol

WISP+ Protocol Introduction

The WISP+ protocol is an example of a proprietary protocol. This protocol was developed by Westinghouse Systems Limited, U.K for its WESDAC32 master system and TALUS RTU. There are several variants of WISP+ around the world. The TNB Extended WISP+ protocol is a variant developed for the Tenaga Nasional Berhad SCADA/EMS project in 1990.

WISP+ is a serial protocol for transmission of data between the SCADA master station and RTU. WISP+ is a robust, and efficient SCADA protocol, which likes DNP3, was modelled after the IEC 870-5-101 frames. Among many of the WISP+ redeeming features include ability to transmit several information object types simultaneously, RTU fault codes, archive transmission and data tunnelling e.g. remote VT-terminal emulation. The TNB Extended WISP+ protocol supports a limited Link Layer routing called the *loop switch* feature that was inherited from an earlier ASEA Sindac4 system. Since TNB private data circuits of that period use low speed Power Line Carrier (PLC), the loop switch function allows master station operator to manually select data transmission direction in order to avoid congestion, for example, for power stations under AGC control. The protocol specification is now in the public domain. However specific company implementations remained proprietary.

Current Status Regarding Protocol Testing

In TNB, successful WISP+ conformance test is mandatory before new RTU and Substation Control System (SCS) are admitted into the SCADA system. With exception to several TALUS RTU specific messages, almost all WISP+ features described in the original documentation are mandatory. During static test, the emphasis is on DUT correctness and throughput efficiency of messages, for example, the tester evaluates the size of multipart messages transmitted. In dynamic test, the emphasis is on the DUT time sensitive functions and synchronized operation with RTUs of different make and model, especially during loop switching. Equipment that passes WISP+ conformance test is monitored under actual operating and field conditions for a period of several months.

Available documentation, tools and existing test labs

TNB develops its own conformance test plans and procedures based upon the original manufacturer documentation. Initially due to its closed nature, no formal WISP+ conformance test tools are available in the market but since the protocol was released into the public domain at least one WISP+ test tool is commercially available. However for utility-specific WISP+ variants, like TNB, testing relies on the TLINE software developed by the manufacturer for static tests and the master station for dynamic tests.

Practical experiences with testing

Unlike standard protocols, proprietary protocols lack structured functional and test documentation. In the case of TNB, test documentation had to be developed from scratch. For static test procedures, the original manufacturer documentation and control centre operations are carefully analyzed to develop use cases. The use case notation is based upon the Unified Modelling Language (UML) standard. The advantage of use case is in its ability to synthesize scenarios in a structured manner. It allows testers to easily develop positive and negative tests. Some static test procedures are further developed to include tests for software equivalence classes and boundary conditions. For example tests for register rollovers caused by natural word-boundary overflows.

Dynamic test procedures are developed by careful analysis of the master station and RTU behaviour. Each data object is analyzed with a protocol analyzer to measure polling loop delays, line idle times and interbyte gaps. These performance measures are used to evaluate the quality of WISP+ implementation and its hardware platform.

4 RECOMMENDATIONS

4.1 *Recommendations for utilities*

Using conformance-tested products is the key to ensuring interoperability among different vendor's products. This keeps you from getting caught in the middle between two supposedly "compliant" products. When problems arise in getting products to communicate, there is no doubt on the one who will ultimately pay the bill. Conformance testing - a one-time cost to the supplier - saves the costly headaches that could otherwise be endured by hundreds of customers.

To archive the best results for a utility, it is recommended to follow a structured project approach as defined below:

- Define a Protocol Implementation Document (PID). Take as the basis the PICS (Interoperability sheet) and add a PIXIT⁶ containing additional requirements (e.g. redundancy, performance). The PID is used to close all open ends in the standard and specifies the use of the standard for one network. The network can be a utility, a group of utilities, a country or a continent. To reduce inter-operability risks, prevent the use of proprietary extensions for as much as possible
- Include the PID as part of the contract between vendor and user.

The above 2 steps have to be taken before the delivery contract between supplier and utility is signed. The next steps take place after signing the contract:

- Only accept a verified protocol implementation in the delivered product before installing the equipment on-site, resulting in a conformance statement to the PID. It is highly preferred to verify this before the FAT and add a pre-FAT in the planning for protocol verification. In case of failure a re-test is necessary that affects budget and planning of the projects negatively (60% of the tests fail).
- Interoperability testing on-site for detecting and solving configuration mismatches and telecom problems. This depends on the strategy and approach on how to put new systems into operation, which can differ per utility.
- Since dynamic integration testing with actual equipment on-site is critical, in cases where only partial interoperability testing is feasible, it is advisable for utilities to consider conditional acceptance of new equipment until full interoperability tests can be performed.

Finally, after the system has been put into operation, the following steps apply:

- Update the PID with the experiences of the last project and possibly with additional functionality.
- Require a verified implementation of the updated software before installing it on-site. Software can easily affect the system functionality after a minor software change. Software release management of the supplier is a very important issue in the Quality Assurance program.
- The updated PID is part of the next tender containing the experiences of the past projects. Try to define a company wide protocol requirement specification (not for each project separately).

Following this approach will result in an open system within your company resulting in the benefits defined before.

⁶ Protocol Implementation eXtra Information for Testing

The structured project approach is being used in practice and an increasing number of utilities are following this approach. An indicator is the increasing number of IEC (conformance) tested protocol implementations the last few years.

Putting a telecontrol connection into operation requires only a minimum of time if protocol problems are eliminated by a passed protocol conformance test. Users of the equipment confirm this, compared to the commissioning of equipment not being conformance-tested before the FAT.

4.2 Recommendations for vendors/manufactures

To prevent the use of proprietary extensions for as much as possible. To set-up a conformance test laboratory to test your products.

To perform one or more conformance tests during the development. To finish development with a conformance test by an independent test laboratory resulting in a certificate.

4.3 General remarks

It will be obvious that, in their request for tender, users include the statement that devices/systems with a protocol standard interface will pass / have passed a conformance test before system integration as a standard term.

The question for the user is to:

- Accept the manufacturers conformance test report, tested according to the manufacturer specification based on IEC standard
- Require a conformance statement and test report from an independent test facility, tested according to the test facility specification based on the associated standard

The last option gives a manufacturer independent guarantee for interoperability but adds some extra costs for the manufacturer when devices haven't been certified yet. Manufacturers can spread the costs over all devices sold and a certified device may have a competitive advantage. Risk factors to consider are the maturity of the standard, maturity of the specifications, maturity of the device, project size and complexity, and possible damage on protection/communication failures and project/outage delay. Finally, it will be a cost driven optimisation process. May be new basic device family members will be tested in independent labs but all derived devices at manufacturers' site. The experience of system integrators will be very decisive.