RealtimeInterface

Realtime **Interface**
System Operator - DER

Dutch implementation of RfG interface requirements
Appendix C - Compliance verification plan

Netbeheer Nederland

01-07-2025 version 1.1

Contents

Document management and distribution

Document management

Version	Date	Changes	Author
1.0 final	February 20th 2024	Test procedures in line with updated technical specification	Technical specification WG
1.1 beta 1	May 1th 2025	Added test cases to verify IEC 62351 implementation	Technical specification WG
1.1 final	July 1st 2025	Review remarks processed	Technical specification WG

Distribution

Version	Distribution date	Receivers
1.0 final	February 20th 2024	Publicly available via website
1.1 beta 1	May 1th 2025	Product development, Testing facility and all other relevant stakeholders
1.1 final	July 1st 2025	Publicly available on website

1. Introduction

This chapter gives a brief background on this compliance verification plan. The chapter explains the purpose of the document, its scope and the outline of the remainder of this document.

1.1. Background

The energy transition is ongoing. Increasing amounts of distributed energy resources (DER) such as solar photovoltaic (PV) systems and wind turbines are connected to the power system. The existing transmission and distribution networks are not designed to handle large amounts of DER. Dutch System Operators are more and more confronted with shortage of network capacity and cannot reinforce their networks at the same pace DER are able to be installed.
In the Netherlands, System Operators therefore investigate ways to connect larger amounts of DER to the existing infrastructure. Examples are implementing congestion management as a method to reduce the impact of scarce network capacity during the time needed to reinforce their transmission and distribution networks, and connecting DER without N-1 network redundancy. The Dutch regulator furthermore published regulatory changes, enabling System Operators to apply congestion management on a large scale.

One of the tools being developed to enable such use cases is an interface between connected Grid Connection Owner and their System Operator, which allows connected Grid Connection Owner and System Operator to interact. In 2020, the Dutch System Operators, united in Netbeheer Nederland (NBNL), started a project in close collaboration with market parties (Figure 1) to describe a Realtime Interface (RTI).

This RTI has the goal to enable System Operators and connected Grid Connection Owners to communicate real-time. To this end, the (preliminary) specifications of version 1, together with supporting technical documentation and the regulatory framework within which the RTI is applied, are published on the website of NBNL: https://www.netbeheernederland.nl/realtimeinterface

In May 2025, the (preliminary) specifications of version 1.1 are published. This version introduces encryption and authentication on the IEC 61850 communication (IEC 62351). Additional test procedures are written to verify that the additional specifications introduced by RTI version 1.1 are met.

1.2. Purpose of the document

The purpose of this document is to elaborate on the required functional tests with regards to both the Customer and System Operator Endpoint of the RTI. To this end, the compliance verification processes are introduced, and the tests are defined.

This document shall be used by the (independent) Test Facility (TF) to perform the compliance verification tests on behalf of the entity requesting the Test Facility to certify a certain Endpoint'

1.3. Scope

In scope of this compliance verification document:

1. Procedures and process of compliance verification from the perspective of a Test Facility
2. Functional related requirement tests
3. Non-functional requirement tests

Out of scope, not included in the compliance verification:

4. Commissioning process
5. Interaction of the Customer Endpoint with rest of DER installation
6. Security tests are part of the commissioning process of the System Operator

1.4. Disclaimer

This document is published and maintained by Netbeheer Nederland and valid until a new version is released. For questions, see the following website: www.netbeheernederland.nl/realtimeinterface.

1.5. Outline

This section gives an outline of each chapter and helps to understand how this document is organized.

Chapter 2 elaborates on the compliance verification process.
Chapter 3 describes the required functional testing.
Annex A provides the detailed test procedures needed for testing.

The appendix describes the detailed test procedures

2. RTI Compliance Verification Process

The compliance verification process is the check on IEC 62351 and IEC 61850 conformance and testing the functional and non-functional behaviour against the RTI-specification, with a compliance verification document as result.

2.1. IEC conformance

Communication over the RTI is based on IEC 61850 series of standards. The security implementation for the RTI is based on the IEC 62351 series of standards. Conformance testing is required to determine whether the implementation of this protocol by the requesting entity (RE) is compliant. To test conformance, the RE's system is connected to a reference system maintained by a Test Facility. Procedures for conformance testing are part of specific standards within the IEC 61850 and IEC 62351 series.

The conformance tests are only designed to evaluate the device against the standards, and don't address the (RTI-specific) functional behavior of the device itself. The communication interface of the device will be tested under different operational conditions.

Conformance testing is usually done at the end of the product development process. This is a quality process to prove that the device has passed the test and ensures that it can properly use all the parts as described in the RTI Protocol Implementation Document (PID).

As shown in the flowchart below (Figure 1), there are several steps for performing the conformance test and issuing an RTI PID conformance statement. At first, there must be a UCA IEC 61850 certificate available. It should be checked to ensure that the certificate covers all the requirements of the RTI Protocol Implementation Document, for the IEC 61850 parts and the RTI specification document for the IEC 62351 implementation:

- If all the requirements are covered by this certificate, no additional test will be performed.

- Otherwise, an additional test for the extra services of the RTI PID is required. For this purpose, the IEC standard test procedures should be tailored according to the RTI PID

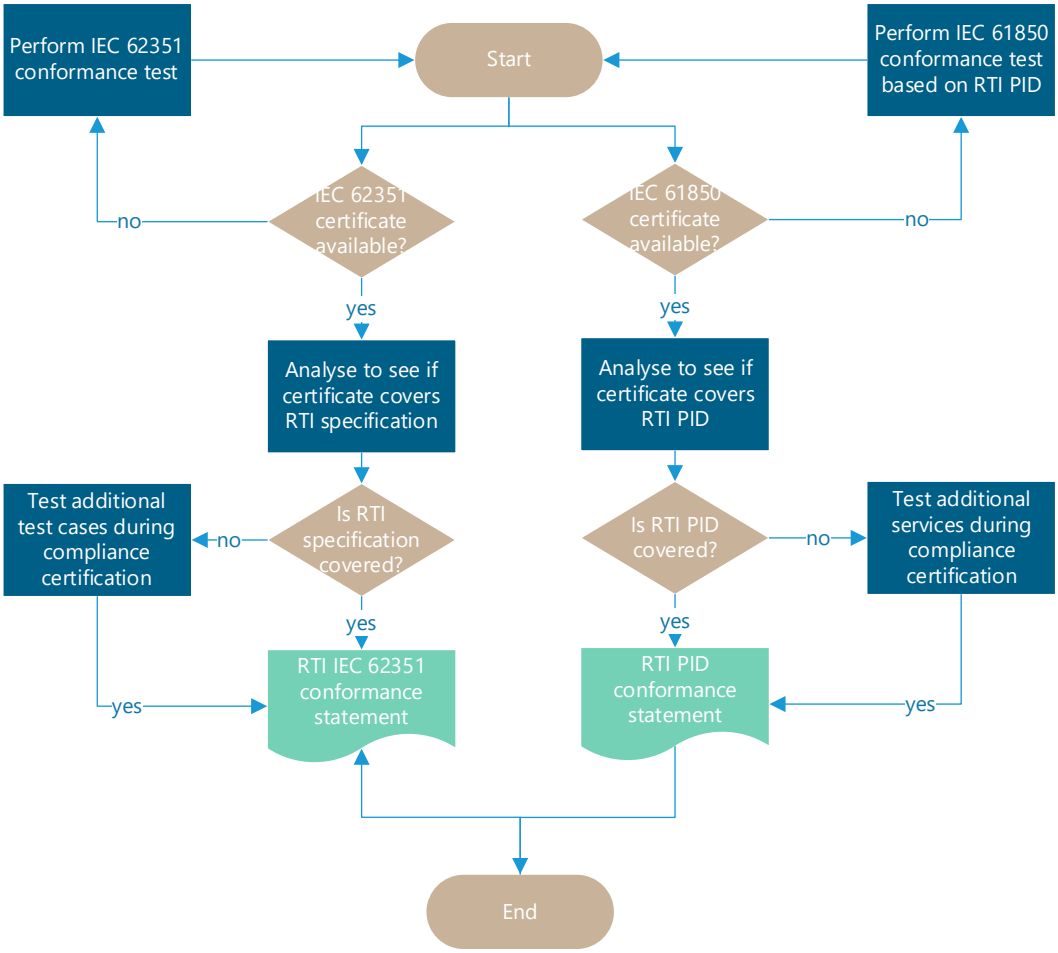


Figure 1: Process flow for IEC 61850 / IEC 62351 RTI conformance certification

There are several Test Facilities for testing communication protocols in equipment. These TF follow test procedures that are being maintained by the specific IEC working group. For IEC 61850 and IEC 62351 testing, the UCAIug has defined detailed test procedures for different implementations (Server, Client). It is possible to check of a product has a certificate via a public database on the website of the UCA International User Group[1].

Testing additional services during the conformance certification can be performed by one of these official Test Facilities as well. Nevertheless, this can be performed also by the Test Facility that's doing the compliance verification if the tools and know-how are available.

[1] https://redmine.ucaiug.org/projects/iec-61850-certificate/

2.2. RTI Compliance Verification Endpoint

The previous paragraph described the process of getting an RTI PID and IEC 62351 conformance certificate, which are required to start the RTI compliance verification (Figure 2). Together with the RTI Technical Specification document and the compliance verification test procedures at the end of this document, these form the starting point of the RTI compliance verification of the Endpoint.

Compliance verification verifies that the equipment under test (EUT) meets the functional and non-functional requirements of the RTI specification. Although security is an important topic, the compliance verification process does not include security tests. Security tests are part of the commissioning process and are therefore out of scope for this document.

The functional and non-functional requirements should be verified by an independent Test Facility, which has been approved by Netbeheer Nederland to perform the RTI compliance verification certification. Netbeheer Nederland approves Test Facilities accredited by the Dutch Raad van Accreditatie (accreditation council). Approved Test Facilities can be found the website of the Raad van Accreditatie. The RE is free to choose any of the approved laboratories of the list for the verification of its product. Every approved Test Facility which is interested to be referred to on the Netbeheer Nederland website, can contact Netbeheer Nederland.

The Test Facility will verify the behavior of the Endpoint by simulating the counter Endpoint (either System Operator or Customer Endpoint) and monitoring the behavior of the tested Endpoint when all the functional and non-functional requirements are verified. The compliance verification is only looking at the behavior of the Endpoint on the RTI. The interaction of the Endpoint with the rest of the DER-installation or System Operator's internal systems is out of scope of the compliance verification process.

When the compliance verification process is successfully passed, the Test Facility grants the Requesting Entity a product compliance verification certificate.

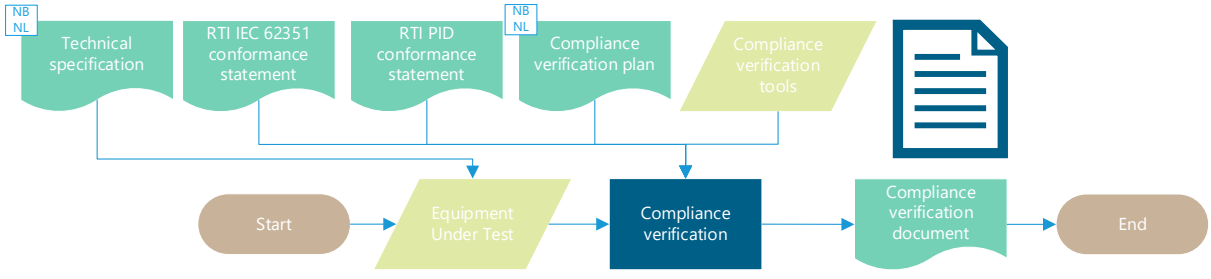


Figure 2: RTI Compliance Verification Test

3. Functional and non-functional testing

This chapter describes the preconditions, components and procedures to test. It concludes with the expected information on the certification.

3.1. Components in the test environment

The following components should be present in the test environment:

Table 1: Components present at compliance verification

Item	Responsibility
Endpoint (Equipment Under Test)	Requesting Entity
Opposite Endpoint (simulated)	Test Facility
Communication Network	Test Facility

The Equipment Under Test (EUT) implementation can differ. If the Endpoint is a singular and local device, this device should be physically available at the Test Facility. If the functional behavior is not part of the physical Endpoint, then the EUT shall be a representation of the chain, including at least the Endpoint and the devices responsible for the functional behavior. The physical RJ45 connection shall be available at the Test Facility. Nevertheless, the TF should be able to verify the behavior of the Endpoint, for example by means of logs, monitoring, et cetera.

3.2. Preconditions to start compliance verification

Before the compliance verification test can start, some preconditions have to be fulfilled:

- The EUT is configured and pre-wired by the RE
- The EUT has an option to monitor the performance of the Endpoint during the test
- A representative of the RE should be present during the test to assist.

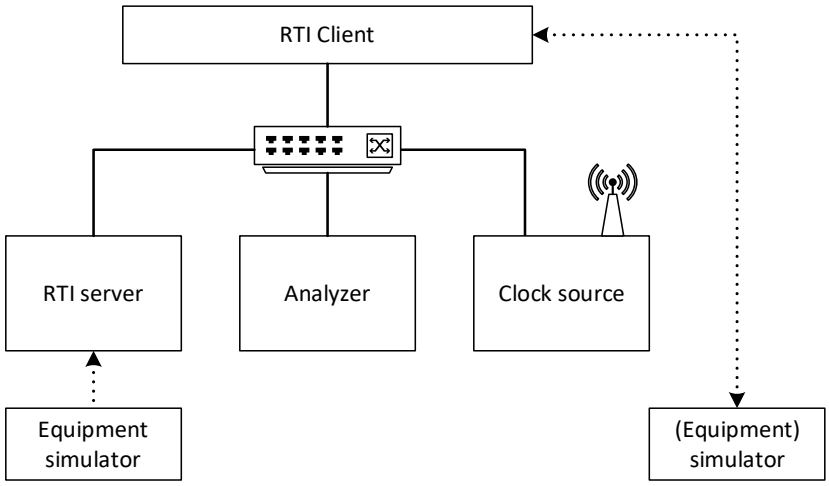


Figure 3: Test setup

3.3. Overview of the test procedures

The test procedures that need to be performed during the compliance verification are:

- [A1] RTI PID conformance test procedure: Many PID requirements are already verified during the IEC 61850-10 based conformance test. The remaining PID requirements are verified in the test procedures.
- [A2] For the TLS conformance, many tests already have been performed in the IEC 62351-100 based conformance tests. Specific cases to be tested are written down in separate test cases.
- [A3] RTI Functional test procedure: This verifies the functionality like setpoints, measurements, safe-/boot modes and Customer configuration/updates.
- [A4] RTI Non-Functional test procedure: Tests requirements that specifies criteria that can be used to judge the operation of a system

3.4. Expected information on compliance certificate

In a specific test, all steps need to be successfully executed to 'pass'. When all the test procedures are passed successfully, the Test Facility can hand over a certificate to the RE. At least the following information should be presented on the certificate:

- Identification of the EUT and any associated equipment, e.g., brand name, product type, serial number, software version
- Representative operating conditions of the EUT
- Date when the tests were finalized
- Name of Test facility
- Signature of Test Facility delegate

Besides the certificate, a report with all the individual test results must be delivered. There must be a clear link between the certificate and the report.

4. Abbreviations

EUT	Equipment Under Test
NBNL	Netbeheer Nederland
RE	Requesting Entity
TF	Test Facility
UCAIug	UCA International User Group

5. Definitions

Requesting Entity	Entity requesting the Test Facility to certify a certain Endpoint
Netbeheer Nederland website	www.netbeheernederland.nl/realtimeinterface
Test Facility	listed on the website of the Raad van Accreditatie, see www.rva.nl/en/alle-geaccrediteerden

Annex A – Detailed test procedures

A1 PID test procedures

Many PID requirements are already verified during the IEC 61850-10 based conformance test. Compare Annex B for detailed comparison. The remaining PID requirements are verified in the test procedures below.

The table below gives an overview of the test cases and the PID requirements. Each test **case** is specified in detail in a test **procedure**.

Test case ID (PID requirement)	Test case description	Applicable for
R.1, R.4, R.11	Verify that the server IED accepts maximum one client association with configured parameters and TCP_KEEPALIVE 20 secs	Client, Server
R.8	Verify that Client IEDs gracefully terminates (when needed) the association to a server IED by using the release or abort service	Tested during conformance
R.14	At least 50 Data set attributes	Server
R.19	Verify the RCB.RptID is configurable	Server
R.32	Verify that the client system explicitly reserves any RCB by writing for each BRCB the ResvTms > 0 and for each URCB Resv=T	Client
R.35	Verify that when the time-stamp differs more than 10 seconds, commands shall be rejected	Server
R.39	TimeAccuracy shall equal or less than 10ms	Server
R. 40-48	Verify that the RTI server is able to change the data model: • IED name • Logical device instance • Logical device ldName • Logical node prefix • Logical node instance • Assign logical nodes to logical devices	Server
R.49	Verify that no vendor specific changes to LNs are used outside the RTI SCL	Server
R.52	Verify Mandatory LN's	Server
R.53	Verify Reference data model used in all RTI	Server

Detailed test procedures (not applicable test procedures will be removed in the test report)

R.1, R.4, R11	Server accepts max 1 association with configured parameters	PASSED/ FAILED
RTI Server 1. RTI server accepts the associate request 2. Client or Server sends TCP_KEEPALIVE every 20 seconds when no 61850 messages are transmitted 3. RTI server refuses the associate request		
RTI Client 1. Client associates to the server with the configured (non-default) called transport/session/presentation selectors 2. Wait 1 minute for TCP_ALIVE messages 3. Another Client associates to the server 4. Use the analyzer to verify the Associate messages		
Comment		

R.14, R.15 R.18, R.19	RCB.RptId is configurable and at least 50 Data set attributes	PASSED/ FAILED
RTI Server The Server .ICD file has: 1. Services ReportSettings rptID=Conf or Dyn 2. Services ConfDataSet maxAttributes >= 50 3. Services ConfReportControl max>=3		
Comment		

R.32	Client reserves URCB and BRCB	PASSED/ FAILED
RTI Server 1. RTI server accepts the URCB reservation 2. RTI server accepts the BRCB reservation		
RTI Client 1. Client associates to the server 2. Client reserves each URCB before configuration/enabling by writing URCB.Resv=T 3. Client reserves each BRCB before configuration/enabling by writing BRCB.ResvTms>0 4. Use the analyzer to verify the client sends the URCB.Resv and BRCB.ResvTms write requests		
Comment		

R.35	Server reject commands when time differs >10 seconds	PASSED/ FAILED
RTI Server 1. RTI server accepts the Operate request 2. RTI server refuses the Operate request		
RTI Client 1. The client and server are in-time-synch 2. Client sends an operate request with no time difference 3. Change the time in the time server for the client only to force a time difference of 12 seconds 4. Client sends an operate request with a 12 second time difference 5. Use the analyzer to verify the server accepts the first Operate and refuses the second Operate		
Comment		

R.39	Server time accuracy <10ms	PASSED/ FAILED
RTI Server 1. RTI server send reports with timestamp accuracy < 10ms		
RTI Client 1. Client reserve and enables URCB 2. Wait for reported measurement values		
Comment		

R.40-48	Server supports flexible data modeling	PASSED/ FAILED
RTI Server 1. RTI server accepts the Operate request 2. RTI server enables the URCB/BRCB and sends reports accordingly		

RTI Client

Test engineer uses the RTI server engineering tool to change:

- The IED name
- The logical device instance on one logical device
- Add logical device ldName on another logical device
- The logical node prefix in one logical node with 10 chars and instance with 3 digits
- Assign the measuring logical node(s) in a separate logical device and the control logical nodes to another logical device

Test engineer loads the configuration into the RTI server and updates the server configuration in the RTI client

1. The client associates to the server
2. Client sends an operate request
3. Client reserves configures and enables at least one URCB and BRCB
4. Client processes the reports from the server as normal
5. Use the analyzer to verify all MMS requests are reponded positively by the server

Comment

R.49, R52, R53	**No vendor specific Logical Nodes and Data Objects**	**PASSED/ FAILED**

RTI Server

Compare the SCL from the RTI server and/or the MICS and compare them with the 7-4 and 7-420 logical nodes and data objects. No extensions are allowed. All RTI SCL LNs and DOs need to be present in the RTI server device.

Comment

A2 TLS security test procedures

Many security requirements are already verified during the IEC 62351-100 based conformance tests. The remaining RTI-specific security requirements are verified in the test procedures below.

Test case ID (functional requirement)	Test case description	Applicable for
TLS-Customer-Standards-1-2-3	Verify Conformance test certificates based on the IEC 62351-3:2013 and the IEC 62351-4:2018+AMD1:2020 CSV for Transport Security in the native mode of operation. Check support for TLS 1.2 and 1.3.	Server

TLS-Customer-Ciphers-1-2-3	Verify
	• Support for cipher suites TLS 1.2:
	  • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	  • TLS_RSA_WITH_NULL_SHA256
	• Support for cipher suites TLS 1.3:
	  • TLS_AES_256_GCM_SHA384
	  • TLS_SHA384_SHA384
	• And activate only the requested cipher suites.
		Server

TLS-Customer-Cert-1	Verify The possibility to include the following information in the certificate: - Validity = between 0 and including 15 years - Key usage = digital signature - Extended key usage = TLS WWW Server Authentication (OID.1.3.6.1.5.5.7.3.1)	Server
TLS-Customer-Cert-2-3	Verify The possibility to export certificates by the Customer Endpoint. Exported certificates shall only have public keys. There shouldn't be an option to export private keys from the Customer Endpoint.	Server
TLS-Customer-Cert-4	Verify There shouldn't be an option to import private keys.	Server
TLS-Customer-Mon-1-2	Verify The Customer Endpoint generates at least the following events related with certificate management: - Generation - Trusted certification authorities (adding or removing individual root certificates) - Validation - Expiration - Revocation - Renewal The events can be extracted according to the message format described in RFC 5424.	Server
TLS-Customer-Auth-1-2-3	Verify Authentication of SO Endpoint. It shall only complete connections to authenticated Customer Endpoints. SO certificates shall be validated based on date of expiration, certification chain and revocation status.	Server

Test case ID (functional requirement)	Test case description	Applicable for
TLS-Customer-Auth-4	Verify The connection shall still be established if there is a mismatch between the IP address in the SO Endpoint certificate and the IP address of the SO Endpoint. An alert shall still be generated.	Server
TLS-Customer-Chain-1	Verify It shall be possible to add or remove individual root certificates from the Endpoint through firmware or software update or through user configuration.	Server
TLS-Customer-Revo-1	Verify The Endpoint shall be able to validate that a certificate is not revoked even without connecting to a central system.	Server

Detailed test procedures (not applicable test procedures will be removed in the test report)

TLS-Customer-Standards-1	**Conformance test certificates based on the IEC 62351-3:2023 and the IEC 62351-4:2018+AMD1:2020 CSV for Transport Security in the native mode of operation. Check support for TLS 1.2 and 1.3.**	**PASSED/ FAILED**
RTI Server 1. Perform 'documentation verification' and check relevant conformance test certificates as requested in the technical specification		
Comment		

TLS-Customer-Ciphers-1	**Support for cipher suites TLS 1.2:** • **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** • **TLS_RSA_WITH_NULL_SHA256** **Support for cipher suites TLS 1.3:** • **TLS_AES_256_GCM_SHA384** • **TLS_SHA384_SHA384** **Activate only the requested cipher suites**	**PASSED/ FAILED**
RTI Server 1. Perform 'documentation verification' and check relevant conformance test certificates as requested in the technical specification to verify that the required cipher suites are available. 2. The DUT shall be able to show that the selected cipher suite is used, and no other. 3. Repeat this test by selecting all other requested cipher suites from the list above for both TLS 1.2 and 1.3.		
Comment		

TLS-Customer-Cert-1	**The possibility to include the following information in the certificate:** **- Validity = between 0 and including 15 years** **- Key usage = digital signature** **- Extended key usage = TLS WWW Server Authentication (OID.1.3.6.1.5.5.7.3.1)**	**PASSED/ FAILED**
RTI Server 1. Export the certificate from the Customer Endpoint. 2. Verify that the exported certificate includes the discriminated fields as described in the requirement. 3. Repeat the test for validity of 0.5, 1 and 15 years configured.		
Comment		

TLS-Customer-Cert-2-3	**The possibility to export certificates by the Customer Endpoint** **Exported certificates shall only have public keys. There shouldn't be an option to export private keys from the Customer Endpoint.**	**PASSED/ FAILED**
RTI Server 1. Export the certificate from the Customer Endpoint. 2. Verify that the export function does not give an option to export private keys. 3. Verify that the exported certificate does not include the corresponding or any other private keys. 4. Verify that the exported certificate contains the public key.		
Comment		

TLS-Customer-Cert-4	**There shouldn't be an option to import private keys.**	**PASSED/ FAILED**
RTI Server 1. Verify that the import function does not import private keys by default nor give the option to do so.		
Comment		

TLS-Customer-Mon-1-2 **TLS-Customer-Auth-1-2-3** **TLS-Customer-Chain-1** **TLS-Customer-Revo-1**	**The Customer Endpoint validates SO Endpoint certificates, authenticates the SO Endpoint, enables certificate management and logs the associated events as required in the technical specification.**	**PASSED/ FAILED**

RTI Server

Events

Follow these steps individually for both **TLS 1.2 and TLS 1.3**:

1. **Generate** or import a Customer Endpoint certificate
2. Verify that an event was created associated with the step above
3. **Import** the root certificate of the SO Endpoint
4. Verify that an event was created associated with the step above
5. Generate a SO Endpoint certificate to use in the next step
6. Set up a TLS connection between RTI client (or simulator) and RTI server
7. Verify that an event associated with the **validation** of the SO certificate is generated
8. Perform the certificate **expiration** test
9. Verify that an event associated with the expiration of the SO certificate is generated
10. **Revoke** the SO certificate in the Customer Endpoint
11. Verify that an event associated with the revocation of the SO certificate is generated
12. Verify that there is no connection anymore
13. Verify that it isn't possible to establish a connection between SO Endpoint and Customer Endpoint
14. **Renewal**: Generate a SO Endpoint certificate to use in the next step
15. Set up a TLS connection between RTI client (or simulator) and RTI server
16. Verify that an event associated with the validation of the SO certificate is generated
17. **Remove/revoke** root certificate of the SO Endpoint
18. Verify that an event was created associated with the step above
19. Verify that there is no connection anymore
20. Verify that an event was created associated with the step(s) above
21. **Import** the root certificate of the SO Endpoint into the Customer Endpoint
22. Verify that an event was created associated with the step above
23. Generate a SO Endpoint certificate to use in the next step
24. Set up a TLS connection between RTI client (or simulator) and RTI server
25. Verify that the old SO Endpoint certificate is not usable anymore
26. **Extract** the logs that are generated during the steps above
27. Verify that the events in the log are formatted according to the Syslog message format in RFC 5424

Comment

Use a certificate with a short lifetime or another way to test the expiration of the certificate.

TLS-Customer-Auth-4	**The connection shall still be established if there is a mismatch between the IP address in the SO Endpoint certificate and the IP address of the SO Endpoint. An alert shall still be generated.**	**PASSED/ FAILED**
RTI Server Follow these steps individually for both **TLS 1.2 and TLS 1.3**: 1. **Generate** or import a Customer Endpoint certificate 2. Verify that an event was created associated with the step above 3. **Import** the root certificate of the SO Endpoint 4. Verify that an event was created associated with the step above 5. Generate a SO Endpoint certificate to use in the next step 6. The IP address of the SO Endpoint in the SO certificate (on all places where the IP address is mentioned or can be filled in) shall be different from the presented IP address for the SO Endpoint configured in the network 7. Set up a TLS connection between RTI client (or simulator) and RTI server 8. Verify that an event associated with the **validation** of the SO certificate is generated 9. Verify that the event mentioned above mentions the IP address mismatch 10. **Extract** the logs that are generated during the steps above 11. Verify that the events in the log are formatted according to the Syslog message format in RFC 5424		
Comment Step 6 shall include at least the fields *Common Name* and *Subject Alternative Name*.		

A3 Functional test procedures

Below table gives an overview of the test cases and the corresponding functional requirements. Each **test case** is specified in detail in a **test procedure**.

Test case ID (functional requirement)	Test case description	Applicable for
Setpoint-1	Verify Change the setpoint for the upper limit of generated active power P as a percentage [%] of the maximum capacity LN **DWMX.WMaxSptPct with a positive value**. Setpoint-1 is the maximum allowed generated active power at the PCC. The Setpoint is defined as a percentage of the accumulative "Maximum Capacity (MW)" in the PGMD form(s).	Client, Server
Setpoint-2	Verify Change a setpoint for the upper limit of **generated** active power P in [MW] in **DWMX.WMaxSpt with a positive value**. Setpoint-2 is the maximum allowed generated active power at the PCC	Client, Server
Setpoint-3	Verify Change a setpoint for the upper limit of consumed active power P in [MW] in **DWMX.WMaxSpt with a negative value**. Setpoint-3 is the maximum allowed consumed (load) active power at the PCC	Client, Server
Setpoint-8	Verify Change the reason why a setpoint is sent by the System Operator in LN **DWMX.SptReas** (clause 5.3.3.3). Setpoint-8 reflects the reason for which use case a setpoint is sent by the System Operator. The reason is represented by an integer value. The explanation of the different reasons are described in [3].	Client, Server
Measurements-1	Verify Send actual active power measurement on PoCC in [MW] in **MMXU.TotW**. The actual active power on the PoCC in MW. The value is the total power of all three phases.	Client, Server
Measurements-2	Verify Send actual reactive power measurement on PoCC in [MVAr] in **MMXU.TotVAr**. The actual reactive power on the PoCC in MVAr. The value is the total reactive power of all three phases.	Client, Server
Measurements-4	Verify Send actual current measurement on PoCC in [A] in **MMXU.A**. The actual current on the PoCC for all the three phases in A. This applies for all three phases individually. The values of the currents are always absolute values. (because in IEC 61850-7-4 the current is a vector with magnitude and optional angle).	Client, Server
Measurements-7	Verify Send actual phase-neutral measurements on PoCC in [kV] in **MMXU.PhV** . The actual phase-neutral voltages on the PoCC for all the three phases in kV. This applies for all three phases individually	Client, Server

Test case ID (functional requirement)	Test case description	Applicable for
Measurements-8	Verify Send actual p phase-phase measurements on PoCC in [kV] in **MMXU.PPV**. The actual phase-phase voltages on the PoCC for all the three phases in kV. This applies for all three phases individually	Client, Server
Safe-Mode-1	Verify In case of lost communication for a duration of a configurable time in **DWMX.WMaxFto**, restrict actual generation of power to a configurable level Safe-Mode-1 restricts the amount of generated active power in case of a communication interruption on the RTI. The Customer Endpoint falls back to a predefined “safemode” setpoint. The configurable time shall be exchanged by the **DWMX.WMaxFto** Data Object	Compare Safe Operating Mode
Safe-Mode-2	Verify Retrieve safe mode setpoint in percentage [%] of the maximum capacity in [MW] in **WMX.WMaxSetPct** Safe-Mode-2 is the setpoint to which the Customer Endpoint has to fall back in case of a communication interruption on the RTI. The System Operator should be able to retrieve the actual setpoint value from the Customer Endpoint	Client, Server
Safe-Mode-3	Verify Set safe mode setpoint in percentage [%] of the maximum capacity In **DWMX.WMaxSetPct** or in absolute value [MW] in **DWMX.WMaxSet** The System Operator shall be able to set the setpoint for the safe mode at the Customer Endpoint through the RTI	Client, Server
Safe-Mode-5	Verify After restoring communication, buffered 15 minutes **average** active power measurements [MW] for the past 8 hours should be pushed to the System Operator using 'buffered reporting' of **MMXU.AvWPhs** The System Operator shall receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes average values of the ‘TotW’ data object, with a maximum time span of 8 hours. To limit the test time use 1 minute average for a timespan of 32 minutes.	Client, Server
Safe-Mode-6	Verify After restoring communication, buffered 15 minutes **maximum** active power measurements [MW] for the past 8 hours should be pushed to the System Operator using 'buffered reporting' of **MMXU.MaxWPhs** The System Operator shall receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes maximum values of the ‘TotW’ data object, with a maximum time span of 8 hours. To limit the test time use 1 minute average for a timespan of 32 minutes.	Client, Server
Safe-Mode-7	Verify After restoring communication, buffered 15 minutes **minimum** active power measurements [MW] for the past 8 hours should be pushed to the System Operator 'buffered reporting' of **MMXU.MinWPhs** The System Operator shall receive measurement values for a period where there was no communication with the Customer Endpoint through the RTI. The measurement values should be presented as 15 minutes minimum values of the ‘TotW’ data object, with a maximum time span of 8 hours. To limit the test time use 1 minute average for a timespan of 32 minutes.	Client, Server
Customer-Configuration-1	Verify that the System Operator can retrieve the actual state of the Customer Endpoint in **DGEN.DEROpSt.** The System Operator shall receive changes of the value for a period when there was no communication, with a maxium of 8 hours.	Compare the process description

Test case ID (functional requirement)	Test case description	Applicable for
Customer-Configuration-7	Verify that the System Operator can retrieve the RTI version information of the Customer Endpoint in **LLN0.NamPlt.configRev = "1.1.0"**	Client, Server
Customer-Updates-1	Verify that The operating system at the Customer Endpoint is able to perform updates and/or patches During the technical life time of the Customer Endpoint, new functionality may have to be added or security risks can occur. Therefore, the Customer Endpoint has to be able to perform updates and patches to for example gain new functionalities. The **LLN0.NamPlt.swRev** shall be updated	Server

	Verify that the Customer Endpoint can apply the specified network parameters provided by the DSO and act accordingly. In case it is possible to use multiple gateway addresses in the Customer Endpoint the one provided by the DSO will be prioritised.	Server

Detailed test procedures (not applicable test procedures shall be removed in the test report)

The following test cases have the precondition “Operational Mode”

Setpoint-1 **Setpoint-8**	**Change the setpoint: DWMX.WMaxSptPct with a positive value.**	**PASSED/ FAILED**
RTI Server 1. RTI server accepts the Operate request 2. RTI server responds the same value as in the operate request, updated the time stamp and valid quality 3. RTI server responds the updated value and time stamp and valid quality 4. RTI server refuses the Operate request 5. RTI server refuses the Operate request		
RTI Client 1. Client sends reason and within 10 seconds Operate request to **DWMX.WMaxSptPct (APC)** matching its control model 2. Client reads or receives a report with **WMaxSptPct .mxVal, .q and .t** 3. Client reads or receives a report with **WMaxSpt .mxVal, .q and .t** 4. Client sends reason and after 11 seconds Operate request to **DWMX.WMaxSptPct** 5. Client sends not relevant reason and within 10 seconds Operate request to **DWMX.WMaxSptPct** 6. Use the analyzer to verify the Operate request and responded values are valid		
Comment Compare RTI specification clause 5.3.3.1, the RTI client has to send a valid reason within 10 seconds before changing one setpoint. The RTI server shall refuse the setpoint in case >10 seconds after the reason or reason is not relevant. Version 1.0 only supports reasons for limiting active power (not for safe mode settings).		

Setpoint-2 **Setpoint-8**	**Change the setpoint: DWMX.WMaxSpt with a positive value.**	**PASSED/ FAILED**
RTI Server 1. RTI server accepts the Operate request 2. RTI server responds the same value as in the operate request, updated the time stamp and valid quality 3. RTI server updated the value and time stamp and valid quality		
RTI Client 1. Client sends reason and within 10 seconds Operate request to **DWMX.WMaxSpt (APC)** matching its control model with a positive value 2. Client reads or receives a report with **WMaxSptPct .mxVal, .q and .t** 3. Client reads or receives a report with **WMaxSpt .mxVal, .q and .t** 4. Use the analyzer to verify the Operate request and responded values are valid		
Comment		

Setpoint-3 Setpoint-8	**Change the setpoint: DWMX.WMaxSpt with a negative value.**	**PASSED/ FAILED**
RTI Server 1. RTI server accepts the Operate request 2. RTI server responds the same value as in the operate request, updated the time stamp and valid quality		
RTI Client 1. Client sends reason and within 10 seconds Operate request to **DWMX.WMaxSpt (APC)** matching its control model with a negative value 2. Client reads or receives a report with **WMaxSpt .mxVal, .q and .t** 3. Use the analyzer to verify the Operate request and responded values are valid		
Comment		

Measurements 1-2—4-7-8	**Report the measurements in correct units**	**PASSED/ FAILED**
RTI Server 1. RTI server enabled the URCB 2. RTI server send reports with matching measurement values in the expected units (MW, MVAr, kV and A), quality valid and matching time stamps 3. RTI server responds correct units.SIunit and units.mulitplier		
RTI Client Test engineer configures a measurement data set with MMXU.TotW, TotVAr, A, PhV and PPV and assigns this to an URCB with a 5 second integrity period. 1. Client reserves, configures and enables the measurement URCB 2. Use equipment simulator to generate different 3 phase voltages and currents for a few minutes 3. Client reads the measurement units 4. Use the analyzer to verify the MMS request and responded values are valid		
Comment		

Safe Mode 2 and 3	Set and retrieve the safe mode setting DWMX.WMaxSetPct and DWMX.WMaxSet	PASSED/ FAILED

RTI Server

1. RTI server responds the safe mode settings, values match
2. RTI server accepts the safe mode percentage setting value
3. RTI server responds the safe mode settings, values match
4. RTI server accepts the safe mode MW setting value
5. RTI server responds the safe mode settings, values match

RTI Client

1. Client reads the safe mode settings **DWMX.WMaxSetPct** and **DWMX.WMaxSet**
2. Client changes the safe mode percentage setting **DWMX.WMaxSetPct**
3. Client reads the safe mode settings **DWMX.WMaxSetPct** and **DWMX.WMaxSet**
4. Client changes the safe mode MW setting **DWMX.WMaxSet**
5. Client reads the safe mode settings **DWMX.WMaxSetPct** and **DWMX.WMaxSet**
6. Use the analyzer to verify the MMS requests/responds and the values are valid

Comment

Safe-Mode 5-6-7	Report the Min, Max and Average power measurements after communication loss	PASSED/ FAILED

RTI Server

1. RTI server enabled the BRCB
2. RTI server send reports with matching measurement values in the expected units (MW), quality valid and matching time stamps
3. RTI server buffers the reports
4. RTI server accepts the resynch and sends the buffered reports with no buffer overflow
5. Verify that the buffer is only purged when an attribute value changes. If the same value is written, purging should not be done.

RTI Client

Test engineer configures a power measurements data set with **MMXU.AvWPhs, MinWPhs and MaxWPhs** and assigns this to an BRCB with an 1 minute integrity period.

1. Client reserves, configures and enables the power measurements BRCB
2. Use equipment simulator to generate different 3 phase voltages and currents for a few minutes
3. Test engineer disconnects the ethernet cable and waits at least 32 minutes while generating different voltages and currents
4. Test engineer connects the ethernet cable
5. Client reconnects, resynchs to the last received report and enables the power measurements BRCB
6. Use the analyzer to verify the MMS reports

Comment

Customer-Configuration-1	**Changes to DGEN.DEROpSt are buffered when there is no communication for at least 8 hours.**	**PASSED/FAILED**
RTI Server 1. Test engineer disconnects ethernet cable between Endpoints. 2. Wait till Customer Endpoint goes into Safe Mode. Note time. 3. Test engineer connects ethernet cable between Endpoints. 4. Buffered reports with DEROpSt value changes are being send.		
RTI Client 1. Client receives reports with DEROpSt changes. Verify time stamp of state change to Safe Mode (3).		
Comment		

Customer-Updates-1 & Customer-Configuration-7	**Customer Endpoint can be updated or patched and the system operator can retrieve the RTI version**	**PASSED/ FAILED**
RTI Server 1. RTI server responds valid **LLN0.NamPlt.swRev** and **LLN0.NamPlt.configRev** = "1.1.0" 2. RTI server responds an updated value for **LLN0.NamPlt.swRev**		
RTI Client 1. Client reads **LLN0.NamPlt** 2. Test engineer uses the engineering tool to update or patch the firmware in the RTI server 3. Client associates and reads **LLN0.NamPlt** 4. Use the analyzer to verify the MMS requests/responds and the values are valid		
Comment		

	Verify that the Customer Endpoint can apply the specified Network parameters provided by the DSO and act accordantly. **In case it is possible to use multiple gateway addresses in the Customer Endpoint the one provided by the DSO will be prioritised.**	**PASSED/ FAILED**
RTI Server 1. Configure RTI server: IP-address: 192.168.1.2 Subnet: 255.255.255.0 Default Gateway: 192.168.1.1 2. Establish the connection 3. Configure RTI server: IP-address: 192.168.10.2 Subnet: 255.255.255.0 Default Gateway: 192.168.10.1		
RTI Client: 1. Use the analyzer to verify the MMS requests/responds and the values are valid 2. Use the analyzer to verify the MMS requests/responds and the values are valid		

Comment

Below table gives an overview of the test cases for each Process mode.

Test case ID (process mode)	Test case description	Applicable for
Initial Boot Mode	Verify the initial boot mode process: The server waits for communication (**DEROpst #2**) and when client sends the settings and reason+setpoint the server moves to “Operational mode”	Client, Server
Reboot Mode	Verify the reboot mode process: The server has communication within the waiting period (**DEROpst #10**) and when client send the reason+setpoint the server moves to “Operational mode” OR The server wait for communication (**DEROpst #1**) and the server moves consequently consequently to “Safe mode”; when the server has communication (**DEROpst #10**) and when client send the reason+setpoint the server moves to “Operational mode”	Client, Server
Safe Operating Mode	Verify the Safe Operating Mode process: The server has communication (**DEROpst #3**) and when client send the reason+setpoint the server moves to “Operational mode”	Client, Server
Operational Mode	Verify the Operational Mode process: The server send reports as requested by the SO and act according to the received setpoints When the DER is available report (**DEROpSt #6**) When the DER is partially unavailable report (**DEROpSt #98**) When the 61850 connection fails start the **WMaxFto** timer and when connection is restored within the timeout reset **WMaxFto** and keep (**DEROpSt #6**) When the 61850 connection fails start the **WMaxFto** timer and when connection is restored after the timeout move to “Safe Operation Mode”	Client, Server

Detailed Test Procedures

Initial Boot Mode	Client loads initialsettings and setpoints on initial boot	PASSED/ FAILED
RTI Server 1. RTI server accepts the communcation 2. RTI server responds **DGEN.DEROpSt = #2** 3. RTI server accepts the operational settings/setpoints, reason and changes to “Operational mode” 4. RTI server responds **DGEN.DEROpSt = #6 or #98**		
RTI Client 1. Client establishes communication to an “initial boot” server 2. Client reads or receives a report with the operational state **DGEN.DEROpSt** 3. Client loads safe mode settings (**DWMX.WMaxSet[Pct]** and **DWMX.WMaxFto**) and reason+setpoint (**DWMX.WMaxSpt[Pct]**) with a valid reason (value 0000-9999) **DWMX.SptReas** 4. Client reads or receives a report with the operational state **DGEN.DEROpSt** 5. Use the analyzer to verify the MMS requests/responds and the values are valid		
Comment		

Reboot Mode	Client loads setpoints on reboot	PASSED/ FAILED
RTI Server 1. RTI server accepts the communication 2. RTI server responds **DGEN.DEROpSt = #10** and the operation setpoint = safe mode setpoint 3. RTI server accepts the operational setpoints, reason and changes to “Operational mode” 4. RTI server responds **DGEN.DEROpSt = #6 or #98**		
RTI Client 1. Client establishes communication to an “reboot” server 2. Client reads or receives a report with **DGEN.DEROpSt** and setpoint value **DWMX.WMaxSpt.mxVal** 3. Client loads reason+setpoint (**DWMX.SptReas** and **DWMX.WMaxSpt[Pct]**) with a valid reason (value 0000-9999) 4. Client reads or receives a report with the operational state **DGEN.DEROpSt** 5. Use the analyzer to verify the MMS requests/responds and the values are valid		
Comment		

Safe Operating Mode	Communication reconnect inside and outside the fallback timeout; when outside the safe mode shall be activated	PASSED/ FAILED

RTI Server

1. RTI server accepts the safe mode setting
2. RTI server accepts the **DWMX.WMaxFto** (ING) setting
3. Settings and setpoint values match with step 1 and 2
4. RTI server activates the safe-mode settings and accepts the connection
5. RTI server responds the safe (fall back) mode values, (**DEROpSt #3)**
6. RTI server accepts the settings and changes to Operational mode, (**DEROpSt #6 or #98)**
7. RTI server uses the operational setpoint (not the safe mode values), **DEROpSt** does not change

RTI Client

Precondition: the client is connected and the server is in Operational Mode (**DEROpSt #6**)

1. Client changes the safe mode power setting **DWMX.WMaxSet (ASG)** to 50% of the operational mode setting (**DWMX.WMaxSpt**)
2. Client changes the **DWMX.WMaxFto (ING)** setting to 5 minutes (300 seconds)
3. Client reads or receives a report with **DWMX.WMaxSet [SP], DWMX.WMaxSetPct [SP], DWMX.WMaxFto [SP]**
4. Test engineer disconnects the ethernet cable, wait 6 minutes and reconnect the cable and client connect
5. Client reads or receives a report with **DWMX.WMaxSpt [MX], DWMX.WMaxSptPct [MX] and DEROpSt**
6. Client sends the reason and valid setpoints
7. Repeat step 1 to 5 but reconnect before **DWMX.WMaxFto** expiration

Comment

The DER stays in Safe Mode until the System Operator Endpoint updates the setpoint.

Operational Mode	Operational Mode – DER unit partially unavaillable	PASSED/ FAILED

RTI Server

2. RTI server responds **DGEN.DEROpSt = #98**
4. RTI server responds **DGEN.DEROpSt = #6**

RTI Client

Precondition: the client is connected and the server is in Operational Mode (**DEROpSt #6**)

1. Force the DER unit into (partially) unavailable
2. Client reads or receives a report with **DGEN.DEROpSt**
3. Force the DER unit to available
4. Client reads or receives a report with **DGEN.DEROpSt**

Comment

A4 Non-Functional Tests

Below table gives an overview of the test cases related to the non-functional requirements. Each test **case** is specified in detail in a test **procedure**.

Test case ID (non-functional requirement)	Test case description	Applicable for
Availability-1	IEC 60870-4 class A1: 99,00%	Not applicable for lab test
Accuracy-1	Class 1, as described in the IEC 61869 set of standards	Not applicable for lab test
Accuracy-2	Customer Endpoint: Maximum deviation with UTC-time of 10 seconds. Accuracy of time synchronization. Reference is UTC.	Server
Accuracy-3	System Operator: Maximum deviation with UTC-time of 10 seconds. Accuracy of time synchronization. Reference is UTC.	Client
Bandwith-1	Local interface is standard Ethernet (10/100/1000Mbit)	Client, Server
Response-Time-1	Response time communication interface (acknowledge) between System Operator Endpoint and Customer Endpoint (communication line) shall <4 seconds	Server
Response-Time-2	Response time electrotechnical (asset) response at Customer side. Time from receiving setpoint from System Operator to achieving the desired setpoint within the agreed upon framework	Not applicable for lab test
Response-Time-3	System Operator: time to restore communication after power failure < 3 minutes	Client
Response-Time-5	Customer Endpoint: time to restore communication after power failure < 3 minutes	Server
Response-Time-6	Time to restore communication after a restart of the system operator Endpoint < 3 minutes	Client
Response-Time-8	Time to restore communication after a restart of the Customer Endpoint < 3 minutes	Server

Detailed test procedures (not applicable test procedures shall be removed in the test report)

Accuracy-2	**Customer Endpoint: Maximum deviation with UTC-time of 10 seconds**	**PASSED/ FAILED**
RTI Server 1. RTI server enables the RCB 2. The RTI server sends a data-change report. The timestamp accuracy is <10 seconds		
RTI Client Connect RTI server to the (S)NTP time server 1. Client reserves, configures the RCB with trigger option data change and enables the RCB 2. Use the equipment simulator to force an event. 3. Use the analyzer to verify the event time stamp in the report message		
Comment		

Accuracy-3	**System operator: Maximum deviation with UTC-time of 10 seconds**	**PASSED/ FAILED**
RTI Server 1. RTI server accepts or ignores the operate request		
RTI Client Connect RTI client to the (S)NTP time server 1. Client operates a control object 2. Use the analyzer to verify the timestamp in the Operate request message		
Comment		

Bandwith-1	**Local interface is RJ-45 Ethernet (10/100/1000Mbit)**	**PASSED/ FAILED**
RTI Server 1. RTI server accepts the associate request		
RTI Client Connect RJ-45 ethernet cable to the RTI client and RTI server 1. Client sends associate 2. Check if the etnernet connector LEDs are OK		
Comment		

Response-Time-1	Response-time of the server shall be <4 seconds	PASSED/ FAILED
RTI Server Use the analyser and check all acknowledge times of the server in the network trace of test procedure “Measurement 1-2-3-4” <4 seconds		
Comment		

Response-Time-3	System operator: start communivations after power failure < 3 minutes	PASSED/ FAILED
RTI Server 3. RTI server accepts the associate		
RTI Client Configure the RTI client with one RTI server 1. Disconnent and connect the power of the RTI client 2. Client shall try to communicate to the server within 3 minutes 3. Use the analyzer to measure the time from connecting the power to the first associate attempt		
Comment		

Response-Time-5	Customer Endpoint: start communivations after power failure < 3 minutes	PASSED/ FAILED
RTI Server 3. RTI server accept the associate and setpoints within 3 minutes		
RTI Client Configure the RTI client with one RTI server 1. Disconnect and connect the power of the RTI server 2. Client tries to communicate to the server, when success loads setpoints 3. Use the analyzer to measure the time from connecting the power to the last setpoint respond		
Comment		

Response-Time-6	System operator restart < 3 minutes	PASSED/ FAILED
RTI Server 3. RTI server accepts the associate, setpoints and reason		
RTI Client Configure the RTI client with one RTI server 1. Client associates to the server 2. Restart the RTI client 3. Client shall restore the communications to the server, load setpoint and reason within 3 minutes 4. Use the analyzer to measure the time from restart to the last setpoint request		
Comment		

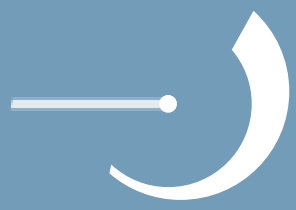
Response-Time-8	Customer Endpoint restart < 3 minutes	PASSED/ FAILED
RTI Server 3. RTI server accepts the associate, setpoints and reason		
RTI Client 1. Client associates to the RTI server 2. Restart the RTI server 3. Client succeeds to associate, loads setpoint and reason in the server within 3 minutes 4. Use the analyzer to measure the time from restart to the last setpoint response		
Comment		

ANNEX B – PID requirements tested during conformance test

Many requirements in the RTI PID are already verified during the conformance test. These requirements don't need to be tested again during the RTI test. Below table shows the conformance test case for each PID requirement.

PID requirement	UCAiug client/server conformance test case	Conformance test case	RTI test case
Association			
R.1	Max 1 association	sAss3	R.1
R.2	Each connection is 1 association	sAss3	
R.3	Authentication not used	Out-of scope	
R.4	Association parameter configurable	sAssN1	R.4
R.5	Retrieve data model = only what is needed, retrieve Datasets and Control blocks	cDs5 cRpN1	Client shall check dataset contents or confRev
R.6	Accept associate after complete start	sAss3	
R.8	Client Release		R.8
R.9	Free network resources	sAssN6	
R.10	Client shall reconnect on interrupt	cAss1	
R.11	TCP KEEPALIVE value 20 soconds	cAssN4	R.11
Data sets			
R.12	Reporting	cSrv4	
R.13	Static reports	sDs1	
R.14	50 data attributes in a dataset		R.14
R.15	3 data sets	(sDs1)	R.15
R.16	Same number of data set as RCBs	sMdl6	
Reporting			
R.17	RCB are configured in SCL	sMdl6	
R.18	3 RCB's	(sMdl6)	R.18
R.19	RCB.RptID shall be not fixed	(sRpN4)	R.19
R.20	All optional fields	sRp2	
R.21	All trigger options	sRp3	
R.22	Segmented reports mandatory	sRp5	
R.23	BufTm > 0	sRp8	
R.24	URCB and BRCB	sMdl6	
Unbuffered Reporting			
R.25	TrgOps=data-chg	sRp3	
R.26	TrgOps=integrity	sRp3	
Buffered Reporting			
R.27	Buffer size 1MB	(sBr20)	Measurement 1-2-3-4
R.28	Buffer overflow	sBr20	
R.29	BRCB	sMdl6	
R.30	TrgOps=data-chg	sBr3	
R.31	Client shall set EntryID	cBr31	

PID requirement	UCAiug client/server conformance test case	Conformance test case	RTI test case
R.32	Reserve BRCB resvTms	(cBr33)	R.32
R.33	TrgOps=integrity	sBr3	
Time-synchronization			
R.34	UTC	sTm1	
R.35	Time difference in control >10s shall be rejected		R.35
R.36	Time quality	sTm2	
R.37	LeapSecondsKnow	sTm2	
R.38	ClockFailure	sTm2, sTmN2	
R.39	Timestamp accuracy <10ms		R.39
Data modelling and naming			
R.40-R.48	Flexible data model is partly covered		R.42-49
R.50	No vendor specific LN		R.50
R.51	Object length < 128	sMdl19	
R.52	Mandatory LN		R.52
R.53	Mandatory DO and DA	sMdl1, sMdl2	
R.54	Reference data model shall be used in all RTI		R.54



RealtimeInterface