Kerberos

Verification of the LXI Functionality of Measuring Instruments

TSEP offers with its product Kerberos a hardware and software solution for the selfcertification of measuring instruments for the core functionality of the LXI Standard. Additionally, with Kerberos it is also possible to self-certify the extended functions for support of IPv6, for the communication over VXI-11 or HiSlip, and the IEEE 1588 functionality. The current Kerberos version has implemented the same test protocols as the current LXI Conformance test suite of the LXI consortium. But with the addition, that the test parameters in Kerberos are more restrictive such that the tests are executed more thourougly. However, Kerberos offers a unique and holistic solution from hardware, software, and client for the execution, evaluation, and self-certification of LXI Conformance tests. Kerberos can also be used to validate existing compliant products in regression tests in addition to the conformance test.

Highlights

LXI All-In-One LXI Self-Certification Solution

Regression Test and Developer Support

IEEE 1588 Verification Tests

Control And Visualization By Client

Continuous Support and Further Development

Hardware

The Kerberos hardware includes a stand-alone core and various hardware components to perform each test. In addition, Kerberos hardware has been integrated with auto-disconnect hardware (network plugin/unplug), IEEE 1588 testing and transmission speed detection hardware. The measuring device (DUT) to be examined runs in its own separate network and is thus completely sealed off from interfering influences from the outside. All necessary network settings are made via an integrated router (Open-WRT). This ensures that all necessary network protocols and settings for IPv4 and IPv6 can be performed.

Within the Kerberos hardware runs a Linux operating system with the actual Test Suite software. All test-specific data is stored directly on the hardware. Signing the testrelevant data ensures, that only data records generated by the test suite can be recognized and processed as such. Since all data is generated directly on the Kerberos hardware, it is not possible to manipulate the test results.

The Kerberos hardware configuration takes place via TCP/IP, for this the hardware has its own network interface, which is used for this communication. The network interface for the DUT and the network interface for communication with the hardware are physically separate.

The touch screen is actually only used to visualize the running tests. The user can choose between several level of details for the visualization of the log-screen. The box can be shut down or restarted from the touch screen. Any direct manipulation of the test procedures or a change of the test cycles is not possible directly on the hardware.

The update of the Kerberos software is carried out via an update software from an external USB stick. Existing test data and settings are not deleted here. To back up the existing test data and settings, Kerberos has the ability to replicate data to an external device. The data can then be reapplied to the Kerberos at any time.

Software

General

The Kerberos software is designed as client / server software. On the Kerberos hardware runs the server, which is responsible for the execution of the tests and the reporting (i.e. the generation of the test report). The Kerberos Client is used to define the DUT, define the test parameters, select the tests, and finally control the process. The client software is available for both Windows (Windows 7 and 10) and Linux (Ubuntu). There are three variants of the Kerberos:

- Base;
- Regression Tests;
- Ultimate.

Base

This variant of the Kerberos solution is intended primarily for test houses or for LXI members who wish to maintain existing LXI implementations. This variant of the Kerberos solution allows you to run the test and log it accordingly.

Regression Tests

This variant of the Kerberos solution contains all functionalities of the "Kerberos Base" variant. In addition, this variant contains functionalities that allow an automated regression test. For this purpose, a client software is provided which can be used in batch or script mode. Thus, this solution can be easily integrated into automated testing. In addition, this variant can be used to generate a result file (JSON format), which can then be processed by the test automation. This version is intended for members who want to create current and new devices and check their compliance during the development and maintenance cycle.

Ultimate

This variant of the Kerberos solution contains all the functionalities of the "Kerberos Regression Test" variant. In addition, this variant contains functionalities that include improved troubleshooting support. This version is for software developers who want to reintegrate the LXI standard into their meter or want to search for errors in existing software.

Highlight: IEEE 1588 PTP Extended Function

With the LXI Clock Synchronization Extended Function, Kerberos also verifies your IEEE 1588 PTP stack according to the LXI PTP Profile. Here the PTP functionality is tested to ensure all various LXI relevant PTP messaging is available. This goes from synchronization messages to management messages. The tests also ensure the timing constraints for synchronization are upheld.

The LXI Consortium recommends +/- 40 nanoseconds accuracy. However, the tests neither test nor verify the accuracy and performance of the PTP stack as the focus is on upholding the PTP functionality of the device within the LXI conform measurement system. The issues performance and accuracy hve to be tested and verified by the vendor.

Highlight: LAN Events+Event Log Extended Function

The LXI LAN Event Messaging Extended Function and LXI Event Log Extended Function are also included in the TSEP Kerberos. On the side of the LAN Event Messaging the protocol is checked for correctness as well as the ability to trigger events. But not only the ability to trigger events is checked but also the time when a LAN event shall be triggered is verified, as time base triggering is a capability of the LAN events.

In combination with the LAN Event Messaging the LXI Event Log is very useful to display the events being triggered by the event messaging. To ensure the LXI Event Log is behaving correctly the Kerberos tests not only the semantic of the event log, but also the format of the event logs. Keeping the same format for event logs and event messaging increases the interoperability between multiple devices.

Kerberos Client-Software

The Kerberos client software is used to control and visualize the results of the Kerberos hardware. The client has the possibility to identify all Kerberos hardware in the network and to connect to one of them after the selection.

If an existing session on the hardware is already being tested, it will be reloaded immediately by the Test Suite. Otherwise it is possible to create a new test session. In the following, the DUT is defined with its properties. These include which "Extended Functions" are supported, as well as some device-specific information. (e.g., whether mDNS can be disabled or the ICMP Ping Responder can be disabled). As soon as the DUT configuration has been completed, the tests determined from the configuration are loaded for this session.

There are several ways to run groups or individual tests. Either the filters can be adjusted, or you can select and start specific tests. Furthermore, the client visualizes a detailed procedure in the form of test steps and their documentation. Since the documentation of the standard is included for each rule and in addition the individual test steps are described in detail, the user is always clearly visualized which test procedures of Kerberos are necessary for a particular test. In addition to the description, a test protocol is created during the runtime of each test, so that the test process can be followed at any time. At the end of a test, a detailed result output is displayed to the user.

Fig. 1. Kerberos Client-Software in the Perform Test Phase.
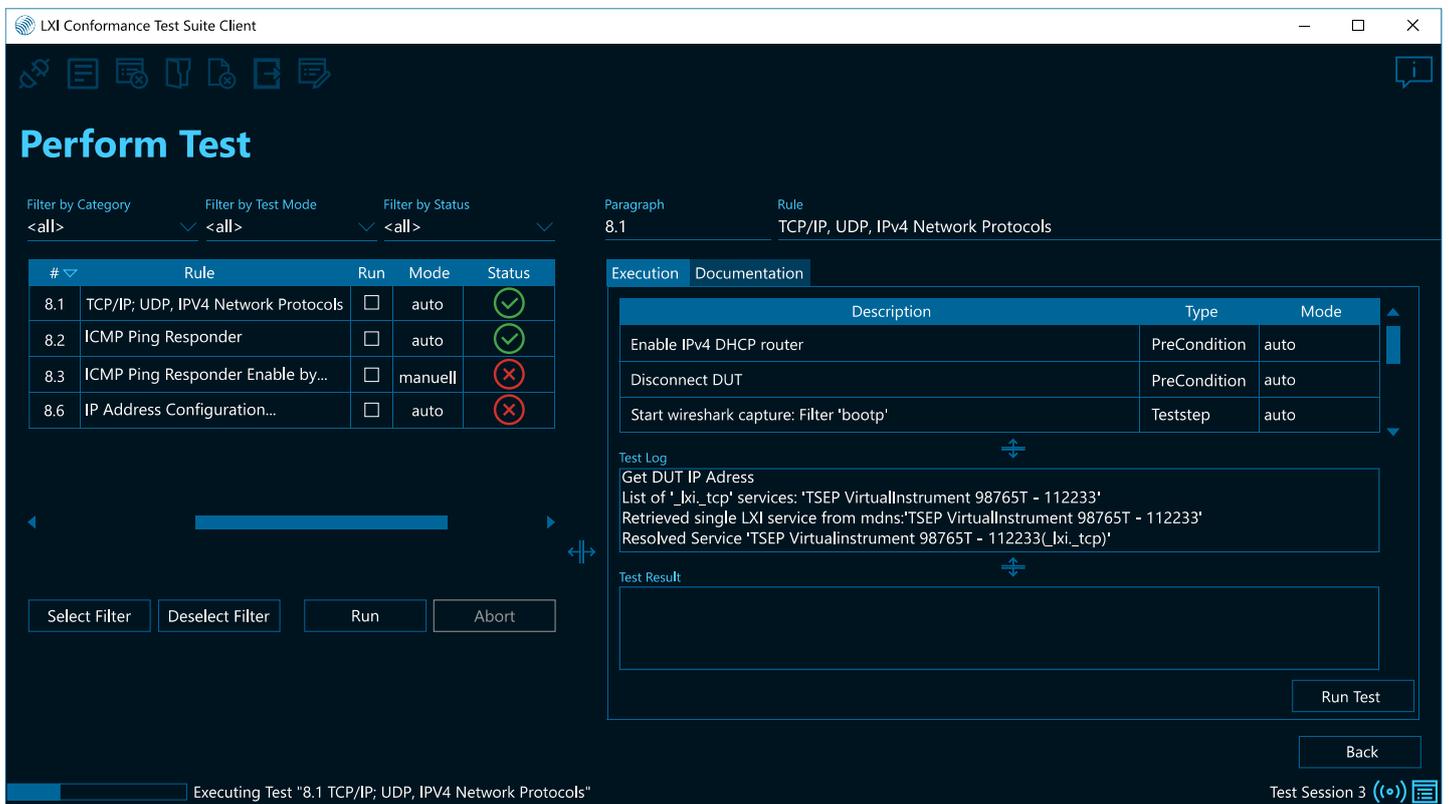
The LXI Standard

Overview

The LXI standard defines how test and measurement devices should behave at the network interface and defines additional features that simplify and expand the interaction of multiple test and measurement devices in the network. The standard is divided into several subcomponents. The "LXI Device Specification 2016" component contains all the basic components such as network configuration, web server for controlling the devices via a web browser and other subcomponents, such as mDNS for the automatic identification of the devices in the network. Other subcomponents are optional, such as Event Messaging, HiSlip, Wired Trigger Bus and Clock Synchronization according to the IEEE1588 standard or Event Logging.

Partnership: TSEP and the LXI Consortium

TSEP has been working on the LXI instrument standard for more than 10 years and is also an active member of the LXI consortium. To provide a technical blueprint for vendors the LXI consortium commissioned in 2014 TSEP to develop the LXI Reference Design and Implementation according to the LXI standard. Going hand in hand with this task, TSEP has been certified as an LXI test house and conducts LXI certification tests for various LXI member companies. As current advancements for Kerberos the topics "LXI Security" and the self-certification of devices by LXI members stand in the foreground. TSEP is actively involved in both topics and participates in the various LXI working groups.

Upcoming Features

Continuous Development

TSEP uses the close connection to the LXI consortium to ensure that the future extensions of the LXI standard are supported by the Kerberos Test Suite.

Network Monitoring of Test

TSEP is going to extend the Kerberos with a new debug feature, a network monitoring service to log the network traffic. With this possible interfering network traffic which leads to a failed test can be detected.

LXI Security

Security is a critical attribute of industrial networks and Industry is giving a growing amount of attention to cybersecurity issues. Since LXI instruments are connected to company networks cybersecurity is also an important topic for the LXI consortium. TSEP is directly involved in the LXI Security Working Group and is responsible for the implementation of the Security Standard in the LXI Reference Design. TSEP will use this close insight to design and implement tests accordingly for all requirements in the LXI Security Standard.

Order Information

Kerberos Base Options

Order Ref.	Description
KER-BASE	Kerberos, Base-Line
KER-REG	Kerberos, Regression Test-Line
KER-ULT	Kerberos, Ultimate-Line
KER-SUP	Support + Updates (yearly)

Kerberos Extended Functions

Order Ref.	Description
KER-LAN	LAN Events + Event Log
KER-PTP	IEEE 1588-2019 PTP
KER-CHN	VXI-11 and HiSlip1.0/2.0