Keysight Transceiver

DS1001A Transceiver

KEYSIGHT

USER MANUAL

Notices

Trademark Acknowledgments

Manual Part Number

DS1001-90002

Edition

Edition 1, October 2024

Published by:
Keysight Technologies
1400 Fountain Grove Parkway
Santa Rosa, CA 95403

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS," AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT WILL CONTROL.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at

https://www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, browse to one of the following URLs, according to the name of your product:

https://www.keysight.com/us/en/product/DS1001A/transceiver.html

To receive the latest updates by email, subscribe to Keysight Email Updates at the following URL:

https://support.keysight.com

Information on preventing instrument damage can be found at:

https://www.keysight.com/find/PreventingInstrumentDamage

Is your product software up-to-date?

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates for your product, go to the Keysight Technical Support website at:

https://www.keysight.com/find/techsupport

Product and Solution Cybersecurity

Keysight complies with multinational regulations for the cybersecurity of its own products and is committed to providing information to assist you in protecting your products and solutions from external cyber threats. For more information, see:

https://www.keysight.com/us/en/about/quality-and-security/security/product-and-solution-cyber-security.html

Keysight also recommends that you secure your IT environments using appropriate third-party tools. For instruments that run the Microsoft Windows operating system, Keysight concurs with Microsoft's recommendations for ensuring that the instrument is protected:

- Get the latest critical Windows updates
- For network-connected instruments, use an Internet firewall (in Keysight instruments, Windows Firewalls enabled by default)
- For network-connected instruments, use up-to-date antivirus and anti-spyware software

Responsible Disclosure Program

Keysight recommends that security researchers share the details of any suspected vulnerabilities across any asset owned, controlled, or operated by Keysight (or that would reasonably impact the security of Keysight and our users) using this form:

https://www.keysight.com/us/en/contact/responsible-disclosure-program.html

Report a Product Cybersecurity Issue

If you discover a cybersecurity issue that you suspect may involve Keysight's proprietary software, or third-party software supplied by Keysight as part of a product, or that may affect the operation of Keysight products, we encourage you to report it to us using this form:

https://www.keysight.com/us/en/about/quality-and-security/security/product-and-solution-cyber-security.html

Contents

What’s in the Box?

The box contains the Transceiver and all accessories to connect it to a computer and an oscilloscope.

Qty[1]	Description	Photo	Identifier[2]
1	Transceiver		TCV
1	12V DC power supply unit (PSU), input 100 - 240 V, AC 50 - 60 Hz with country-specific power cable	 	PSU
1	Ethernet cable		
1	SFP+ to Ethernet adapter		
2	SMA (Plug) to BNC (Jack) adapter		
2	SMA (Plug) to SMB (Plug) adapter		

1	64 GB Flash Stick	
1	10dB attenuator	
1	20dB attenuator	
1	SMB to SMB cable, 3 feet	
1	SMB to BNC cable, 3 feet	
1	USB 3.0 to Ethernet adapter	
1	This “DS1001A Transceiver User Manual”	

1. The amount or number of registered items (quantity, Qty)
2. Identifier used in this document to refer to the item

WARNING

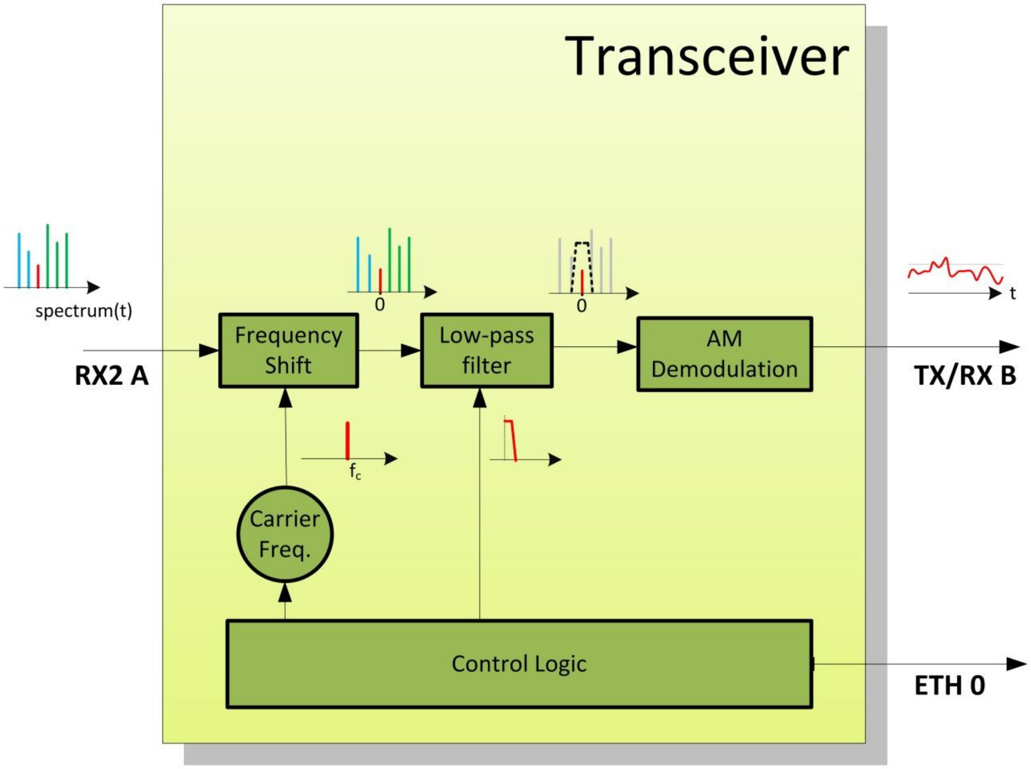
Do not reflash the Transceiver Field-Programmable Gate Array (FPGA) bitstream. Transceiver has been flashed with Keysight bitstream and functionality will be lost after reflashing with another bitstream.

Please contact https://support.keysight.com if Transceiver is not functional.

What It Does

The Transceiver is a professional, high-performance software defined radio (SDR) device for application in side channel attacks on wireless communication systems.

Figure 1 Functional overview of Transceiver



The Transceiver can be tuned to a specific frequency on range 10 MHz .. 6 GHz, and outputs the modulation energy of signals on that frequency. That energy can be recorded with a digital oscilloscope for performing a Simple Power Analysis / Differential Fault Analysis (SPA/DPA) in Inspector.

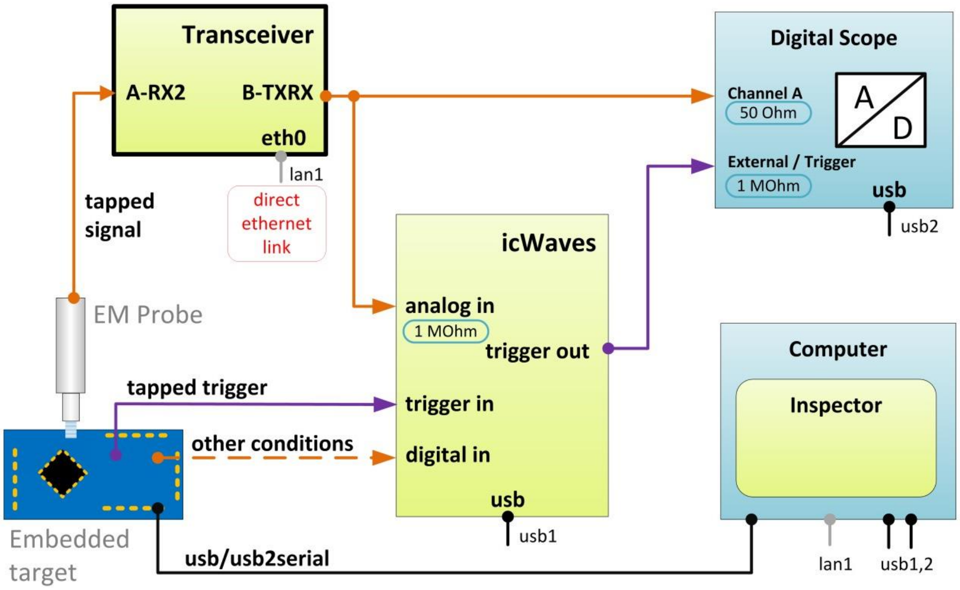
The input signal can come from an EM Probe, and the output signal can also be sent to a pattern recognition product like the DS1002A Pattern Based Trigger Generator.

How to Build a Setup

Typical side channel analysis setup

An EM Probe picks up the radio frequency (RF) signal and feeds the Transceiver. The Transceiver extracts the modulation signal from a configured carrier frequency and feeds the Pattern Based Trigger Generator. The Pattern Based Trigger Generator triggers measurements after the occurrence of a trained modulation pattern, gated by a trigger from the embedded target.

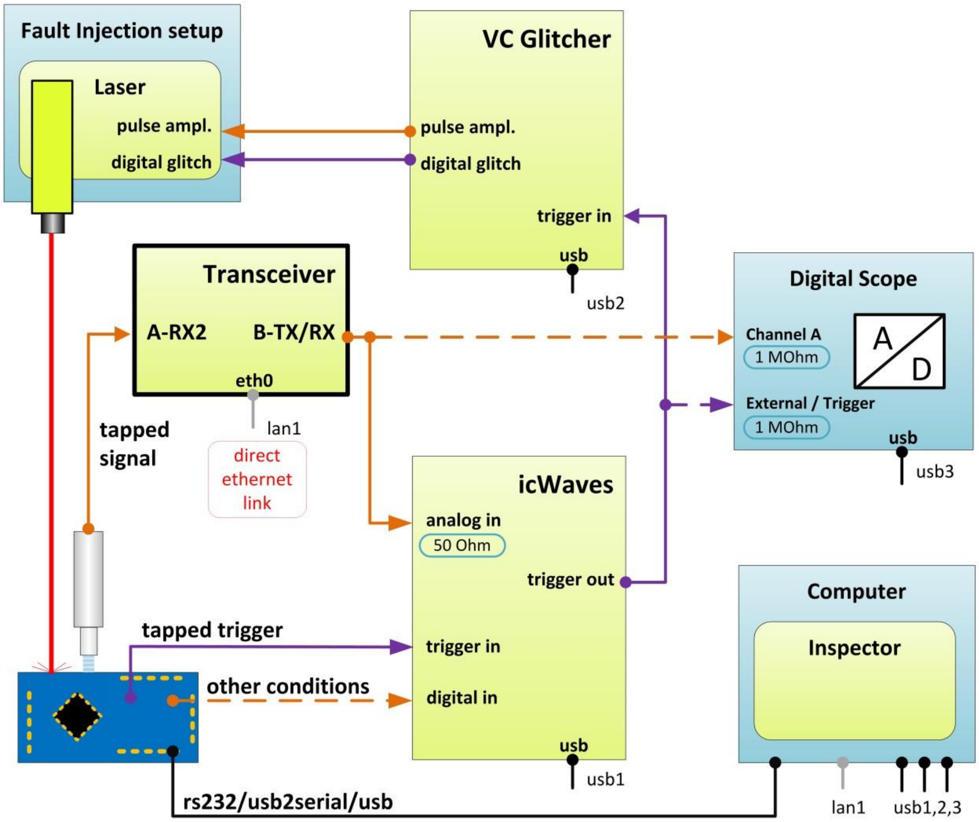
Figure 2 Typical use of the Transceiver in an RF side channel analysis setup



Typical fault injection setup

An EM Probe picks up the RF signal from the target and feeds the Transceiver. The Transceiver extracts the modulation signal from a configured carrier frequency and feeds the Pattern Based Trigger Generator. The Pattern Based Trigger Generator conditionally triggers the DS1160A Smartcard Voltage and Clock Glitcher on trained modulation patterns. The DS1160A Smartcard Voltage and Clock Glitcher fires the laser with a configured energy level and burst pattern.

Figure 3 Typical use of the Transceiver in a fault injection setup



How to set the Transceiver tuning frequency

The GNURadio application enables configuration of all Transceiver parameters.

1. Install the Virtual Linux machine containing GNURadio from the 64GB flash disk, following the installation guide document.
2. Connect the Transceiver with a LAN cable directly to the computer.

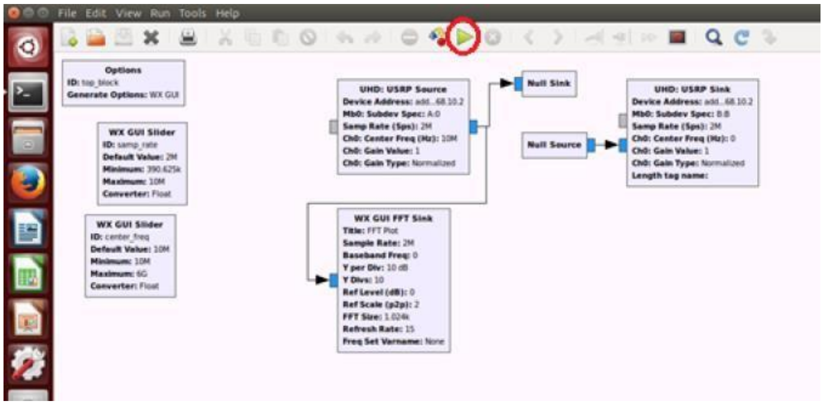
NOTE

Intel Virtualization Technology (also known as Intel VT) must be enabled in the BIOS of your PC to run the Linux Virtual Machine successfully.

For users with AMD processors, AMD-V support must be enabled in the BIOS of your PC.

3. On the computer, start the supplied Linux virtual machine.
4. Click on the "Teminal" icon to launch the GNURadio.

5. Click the "Run" button to execute the default template.



Options
ID: top_block
Generate Options: WX GUI

WX GUI Slider
ID: samp_rate
Default Value: 2M
Minimum: 390.625k
Maximum: 10M
Converter: Float

WX GUI Slider
ID: center_freq
Default Value: 10M
Minimum: 10M
Maximum: 6G
Converter: Float

UHD: USRP Source
Device Address: add...68.10.2
Mb0: Subdev Spec: A:0
Samp Rate (Sps): 2M
Ch0: Center Freq (Hz): 10M
Ch0: Gain Value: 1
Ch0: Gain Type: Normalized

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 2M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

Null Sink

Null Source

UHD: USRP Sink
Device Address: add...68.10.2
Mb0: Subdev Spec: B:0
Samp Rate (Sps): 2M
Ch0: Center Freq (Hz): 0
Ch0: Gain Value: 1
Ch0: Gain Type: Normalized
Length tag name:

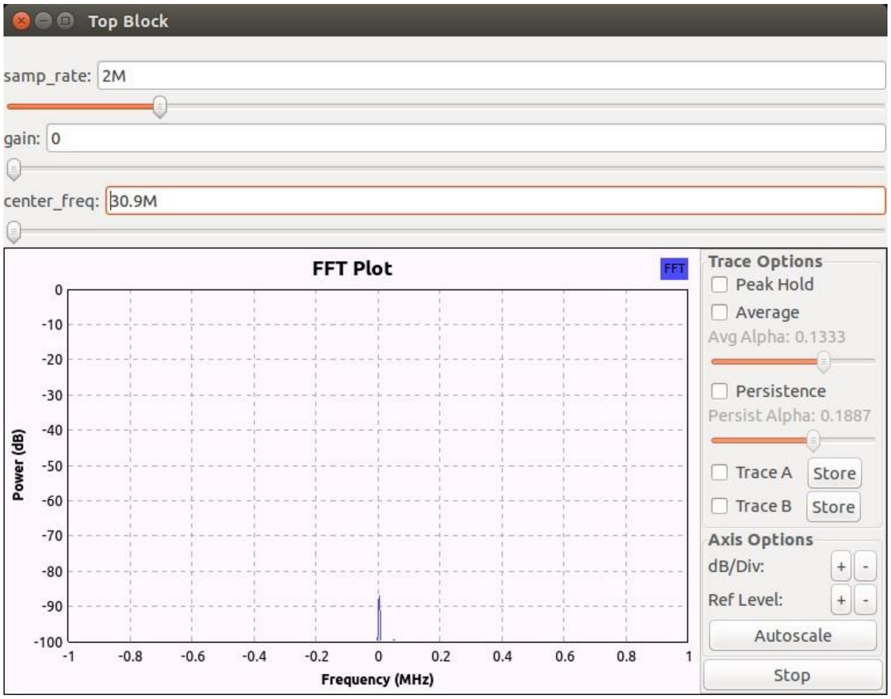
6. In the toolbar, press the Run icon (the green triangle).

7. A tuning dialog opens showing the FFT Plot view and three main controls:

samp_rate

center_freq.

gain



samp_rate: 2M

gain: 0

center_freq: 30.9M

Avg Alpha: 0.1333

Persist Alpha: 0.1887

8. Move the top slider, or enter a value, for the samp_rate in Samples/sec. This value defines the bandpass filter width in the Transceiver. Enter a value that is 2x the highest modulation frequency of interest to you (Nyquist theorem).

9. Move the bottom slider, or enter a value, for center_freq in Hz.
   This will tune the Transceiver to the specified carrier frequency. The FFT Plot is instantly updated with the extracted energy of frequency components around this center frequency.

10. Fine-tune the Transceiver for best reception by sliding the center-freq such that the peak of the carrier frequency occurs at position 0 MHz in the FFT Plot.

11. The gain parameter can be used to tune the output signal amplitude.

Verification of the Setup

Follow the next checks to verify a correct setup:

12. Is the Transceiver powered?

13. Is the Transceiver recognized?

14. Is the Transceiver responding to commands?

Please ensure that a check is successful before going to the next one. If a check is unsuccessful, refer to the section “Help and Troubleshooting” for solutions.

Check 1: Is the Transceiver powered?

The Transceiver is powered when the LED in the PWR button is ON.

Check 2: Is the Transceiver recognized?

1. Connect the Transceiver with a LAN cable directly to a computer.
2. Switch the Transceiver ON.
3. Set the host machine IP to 192.168.10.1, with subnet mask of 255.255.255.0
4. Open any terminal.
5. Type: `ping 192.168.10.2`

The Transceiver is reachable and recognized when ping reports low response time values (typically < 5 ms).

Check 3: Is the Transceiver responding to commands?

Preparation: Start the Linux virtual machine with the GNURadio application.

1. Use the shortcut on the desktop to start GNURadio.
2. On the toolbar, press Run-icon.
3. Set samp_rate to 2M
4. Move the center_freq slider.

If a clear peak can be found in the FFT Plot, then the Transceiver is working.

Help and Troubleshooting

Common problems

Signal or behavior	Table Heading
The Output Signal is too weak	Configure the gain parameter with a higher value.
Cannot find the login password to the Linux VM	Search for “password” in the document VirtualMachine_Installation_Guide.pdf. It can be found under the Documentation folder of the USB stick.

Still have questions?

Visit the Keysight Support Portal at https://support.keysight.com

Technical Specifications

The Transceiver is a software customized version of the high-end Ettus Research USRP X310 product.

The Transceiver is configured with the GNURadio application, provided as a ready-to-run Linux virtual machine.

Operational conditions

- Room temperature 20 – 30 °C, (68 – 86 °F)

CAUTION

Do not block the ventilation holes. A blocked air flow may cause malfunction or breakdown.

NOTE

Maintain stable environmental conditions (temperature, humidity, airflow, etc.) to reliably repeat tests and compare test results.

Power supply input

- 12 V DC, max 45 W

Networking

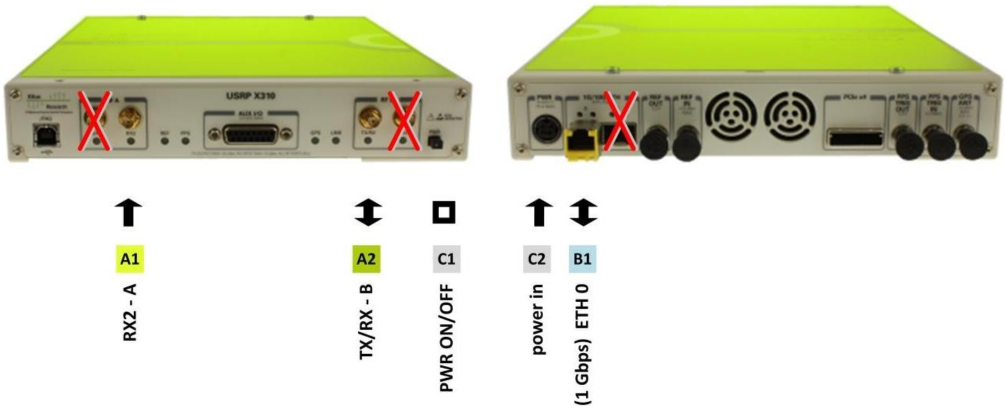
- RJ45, LAN
- Fixed static IP-address, 192.168.10.2
- For direct connection to client computer

Tuning characteristics

- Carrier frequency, software adjustable, 10 MHz .. 6000 MHz
- Filter bandwidth, software adjustable, 0.4 MHz .. 160 MHz

Product case

- Dimensions L x W x H: 277 x 218 x 39 [mm], 8.661 x 6.673 x 1.363 [inch]



Port	Label	Description
A1	RX2 – A	SMB. 50 Ω. Analog input. Input for radio frequent signal
A2	TX/RX - B	SMB. 50 Ω. Analog output Output of AM demodulated signal
C1	PWR	Power switch ON/OFF with built-in status LED
C2	Power in	15 V DC Power supply input
B1	ETH 0	RJ45 LAN connector, port 0 (1 Gbps) Connection with computer for configuration tasks (Remove the yellow-edged SFP-to-RJ45 adapter) NOTE: You cannot use the ETH 1 (10 Gbps) port

KEYSIGHT

This information is subject to change without notice

Edition 1, October 2024

DS1001-90002

www.keysight.com