Keysight Glitch Amplifier Needle

DS1322A Glitch Amplifier Needle

KEYSIGHT

USER MANUAL

Notices

Trademark Acknowledgments

Manual Part Number

DS1322-90002

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/DS1322A/glitch-amplifier-needle.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 Glitch Amplifier and all accessories to connect it to an oscilloscope.

Quantity[1]	Description	Photo	Identifier[2]
1	Glitch Amplifier		
2	12 DC Power Supply Unit, Input 100 - 240V, AC 50- 60 Hz		PSU
-	Power cable (included with PSU)	 Country-specific	
10	Jumper wires: Male - Female		
2	Signal cable: - BNC –SMB, 50 **Ω**, coaxial, 3 ft		BNC2SMB
1	Signal cable: SMB –SMB, 50 **Ω**, coaxial, 3 ft		SMB2SMB
1	Target supply: - custom 2-pin connector		
2	Bracket		

8	Hex Screw M3		Hex Screw
2	Copper Strip, 3ft		
1	Hex Key		
4	Feet		
4	Screw thread		
1	Glitch Amplifier Needle — Glitch Amplifier Needle Box — Glitch Amplifier Needle — SMB –SMB, 50 **Ω**, coaxial, 3 ft		
Optional	3D probe positioner: — Probe holding arm — Holding arm base — Mount to base plate with 2 M5 knurled knob	 	
	This “Glitch Amplifier Needle User Manual”		

1. Quantity of items registered in the package.
2. Identifier used in references in this document.

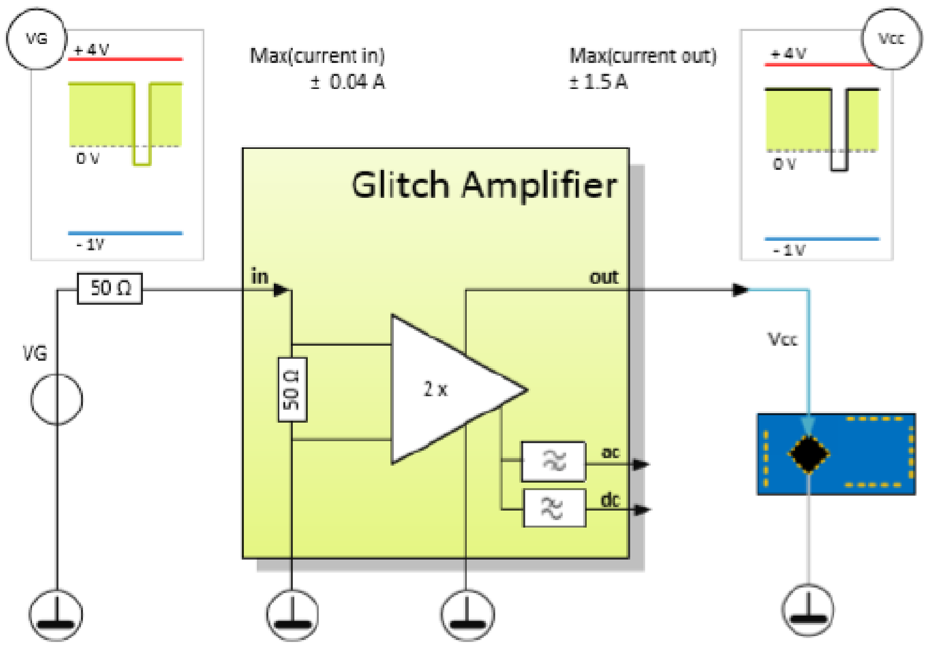
What It Does (Glitch Amplifier)

The Glitch Amplifier is device to power embedded targets, for example FPGAs or SOCs.

The Glitch Amplifier is capable of inserting high-speed glitches in the supply voltage while handling supply current.

A pulse generator like Smartcard Voltage and Clock Glitcher or Glitch Pattern Generator can generate the signal for glitching.

Figure 1 **Functional overview of Glitch Amplifier Needle**



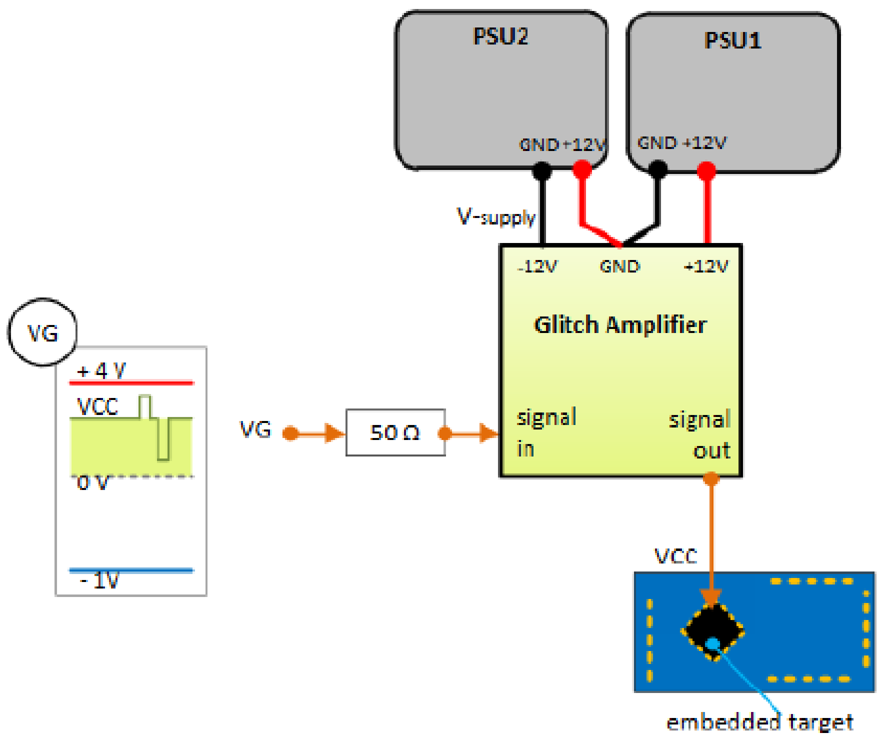
The Glitch Amplifier has a voltage monitor output to verify the shape of the glitched signal with an oscilloscope.

The Glitch Amplifier has DC and AC monitor outputs with a signal proportional to the target's current consumption. These outputs can be used by pattern recognition devices like Keysight Pattern Based Trigger Generator to implement dynamic glitching attacks.

Basic setup

The power of the Glitch Amplifier is supplied by two **identical** PSUs in a cascaded configuration.

Figure 2 Basic setup of Glitch Amplifier



How to Build a Setup

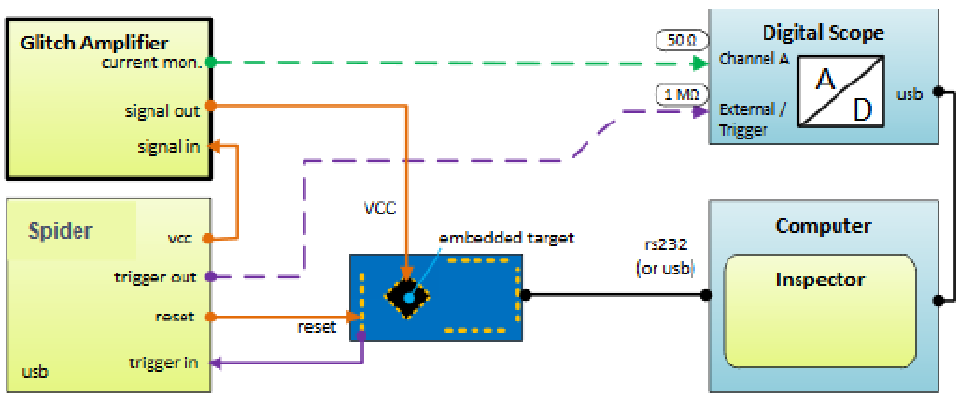
Setup for static power glitching

Additional products used: Glitch Pattern Generator

In this setup, Glitch Amplifier powers the target and transfers voltage glitches. The Supply voltage level (vcc) and voltage glitches are generated by Glitch Pattern Generator.

The digital oscilloscope is optionally used to observe the patterns in power consumption.

Figure 3 Perturbation of the power supply line with static timing



NOTE

You may want to remove the power supply capacitors on the embedded target to get better power consumption readings and better glitch effects.

NOTE

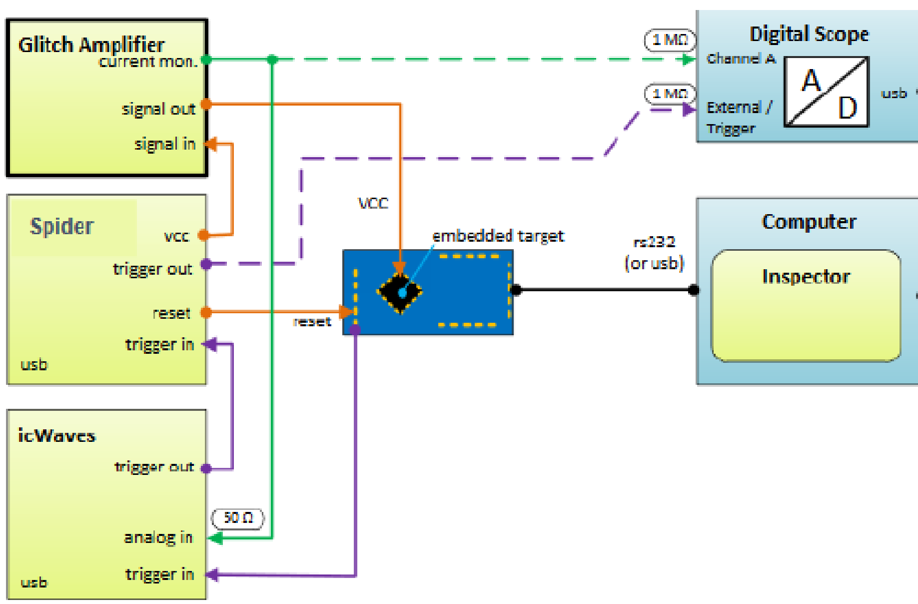
Keep the wiring between the Glitch Amplifier and the target as short as possible. For the best results use short copper strips soldered from the Glitch Amplifier to the target. Both copper strips have a low inductance providing better power consumption readings and better glitch effects.

Setup for dynamic power glitching

Additional products used: Glitch Pattern Generator, Pattern Based Trigger Generator

This setup has a target with variable clock frequency countermeasures to make synchronization difficult. The variability in timing is captured by triggering on a preselected wave fragment in the power consumption. Recognition of this fragment is performed by the Pattern Based Trigger Generator using the Glitch Amplifier current monitor signal.

Figure 4 **Perturbation of the power supply line with dynamic timing**



The power signal is connected to the high impedance input of the scope to prevent loss of signal quality for the Pattern Based Trigger Generator.

NOTE The analog input of Pattern Based Trigger Generator 3 has software selectable impedance 50 Ω / 1M Ω. Configure it for 50 Ω.

How to Mount the Glitch Amplifier

The Glitch Amplifier can be horizontal or vertically mounted.

This enables a short path from the Glitch Amplifier to the target’s voltage lines.

Figure 5 **Horizontal and vertical positioning of the Glitch Amplifier**

Position adjustment

Adjustment for horizontal or vertical position is done by rotating the two brackets 90 degrees.

Place the four M3 hex screws into the screw holes of the bracket.

Figure 6 **Mounting bracket**

Position the Glitch Amplifier and bracket so the hex screws align with the screw holes of the Glitch Amplifier.

With the hex key fasten the hex screws until they keep the bracket in place. Repeat these steps for the other side of the Glitch Amplifier.

Height adjustment

Use the supplied screw threads to adjust the height of the Glitch Amplifier.

Place the screw threads inside the bracket’s corner holes.

Adjust them by hand, the screw thread will go through the bracket.

The optimal height of the Glitch Amplifier is determent by target position.

Feet or base plate

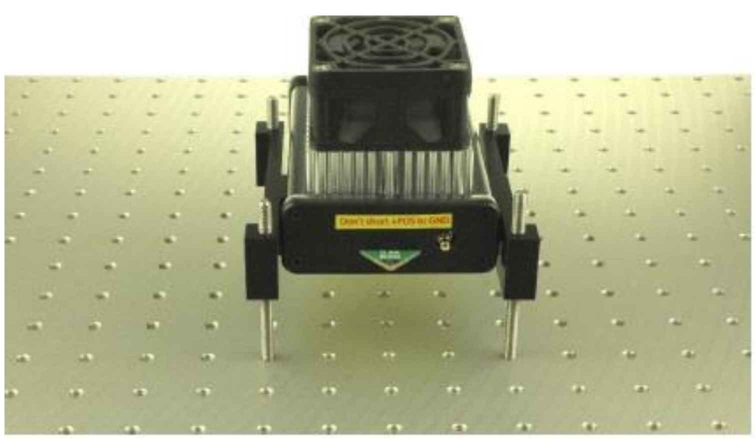
The Glitch Amplifier package contains feet that prevent any short when mounting on a PCB.

Figure 7 **Glitch Amplifier feet**

If you have a Keysight base plate (from the EM-Probe station or Precision XYZ stage), you will be able to mount the Glitch Amplifier directly to the base plate.

The screw threads will align with the base plate so that the Glitch Amplifier can be fastened easily and positioned accurately above your target.

Figure 8 **Glitch Amplifier on base plate**



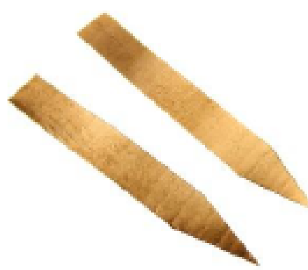
Using the Copper Strips

Preparing the copper strips

Cut a piece of copper strip of the length you might need.

Cut that piece in half so that you have two thin pieces of copper.

On one edge of each copper strip, cut an arrow like shape.

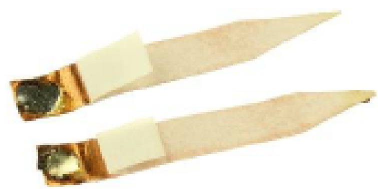


Turn the copper strip around and lift off a small portion of the isolation material.

Apply a bit of solder past to the exposed copper part.

Be sure the solder paste is applied to the copper and not the adhesive layer.

Solder this side of each copper strip to the Glitch Amplifier.



Turn the copper strips around and apply solder past on the point of the arrow.

Solder this part of each copper strip to the target. One strip to the voltage line and the other strip to ground.

What It Does (Glitch Amplifier Needle)

The Glitch Amplifier Needle, driven by the Glitch Amplifier, is capable of inserting high-speed glitches on embedded targets without having to alter the target power supply.

By connecting the Glitch Amplifier “out” SMB to the Glitch Amplifier Needle, it is possible to inject faults by placing the Needle on the target VCC pin and connecting the ground clip to the target ground without having to use the Glitch Amplifier as a power supply for the target.

Use this method if altering the power supply of the target is not possible.

NOTE **For the best result, use the 3ft. SMB cable supplied with the Glitch Amplifier Needle. The Glitch Amplifier Needle has a spring-loaded tip for easy positioning.**

Figure 9 Glitch Amplifier Needle attached with 3ft SMB cable

Glitch Amplifier Needle Setup

Figure 10 Perturbation of the VCC pin using Glitch Amplifier Needle

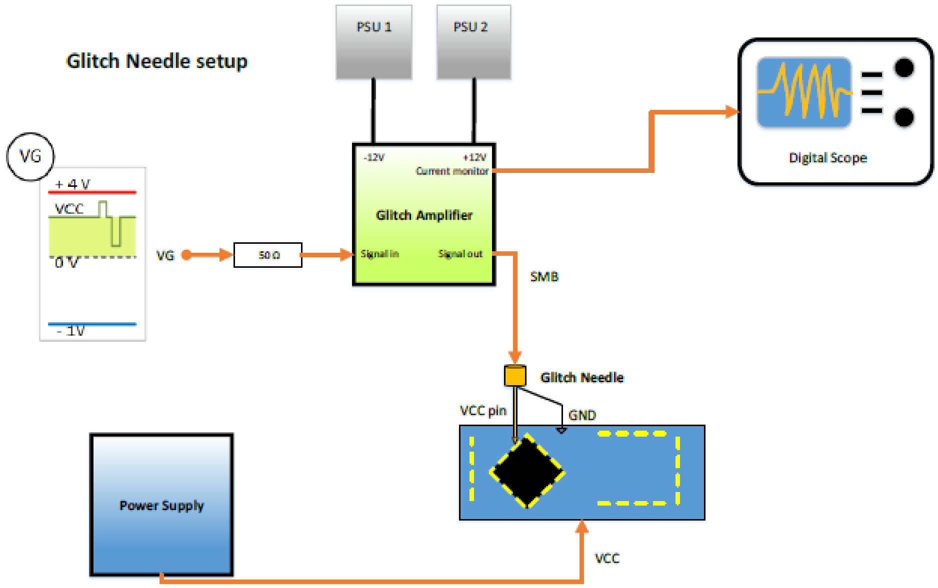


Figure 11 Glitch Amplifier Needle setup on a Crypto Training Target using a Keysight Precision XYZ Stage and 3D positioner

Figure 12 Close-up of Glitch Amplifier Needle on Crypto Training Target pin

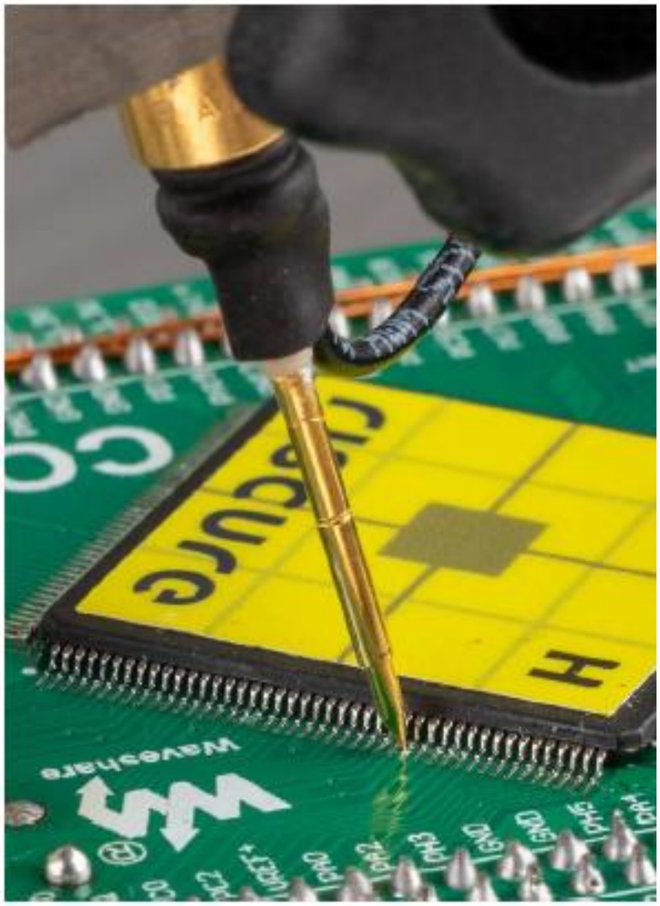


Figure 13 Crypto Training Target AES target measured with Glitch Amplifier Needle on the current monitor port of Glitch Amplifier Needle

How to Mount the Glitch Amplifier Needle

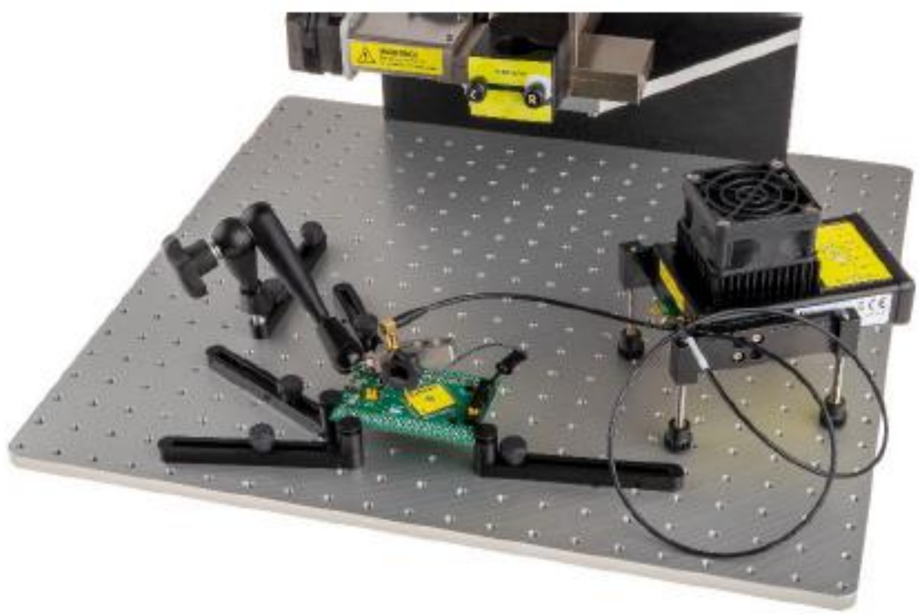
There are multiple ways of mounting Glitch Amplifier Needle on the target.

– Mounting with 3D positioner:

Figure 14 **Glitch Amplifier Needle using a 3D positioner**

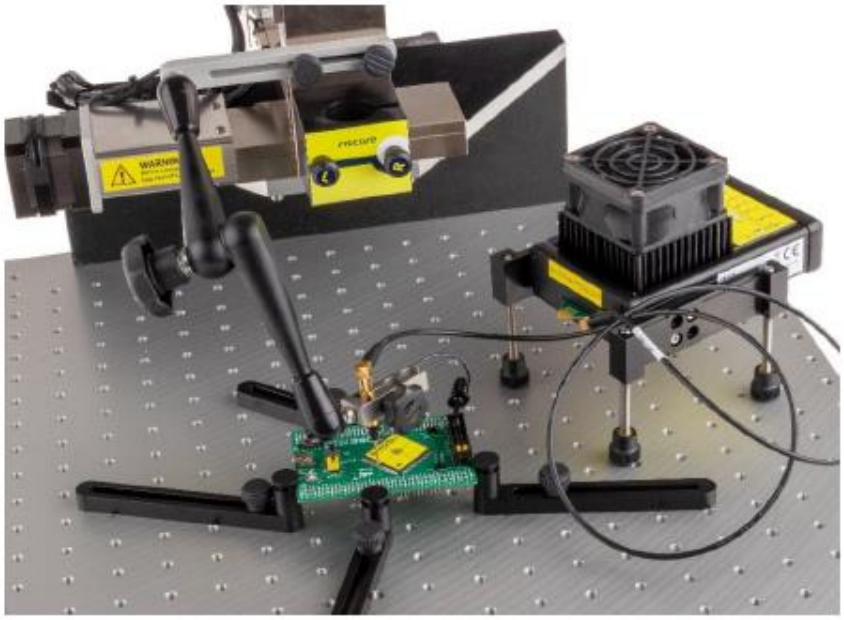
– Mounting with XYZ-base plate:

Figure 15 **Glitch Needle using a XYZ-base plate**



– Mounting with Precision XYZ-Stage:

Figure 16 **Glitch Amplifier Needle using a Precision XYZ-Stage**



– Mounting directly on Glitch Amplifier:

Figure 17 **Glitch Amplifier Needle directly mounted on Glitch Amplifier**

Still have questions?

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

Technical Specifications

Operational conditions

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

WARNING

Do not block the ventilation holes of the Glitch Amplifier.

A blocked airflow may cause malfunction or break down.

NOTE

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

NOTE

Turning off the Glitch Amplifier is recommended when not used for an extended period.

Power supply input

– Positive DC supply, fixed at +12 V.

– Negative DC supply, fixed at -12 V.

WARNING

Power supplier is protected against over current at 3A.

Signal input

– Input impedance 50 Ω.

– Max. voltage range measured between output impedance of Pulse Generator and input impedance of Glitch Amplifier: -0.5 V... +2V.

– Pulse Generator with 50 Ω output impedance must be connected via 50 Ω cable. As a result, ‘signal in 50 Ω’ voltage will be half of generator voltage. This compensated by a 2x amplification.

Out

- Max. voltage range -1V... +4V.
- Low noise < 10mV.
- Amplification: 2x. As a result 'out' voltage will match generator voltage.
- Bandwidth: DC... 300Mhz @ -3dB.
- Capable of sourcing and sinking up to 1.5 A and 1A continuously.
- Connection cable between 'out' and target must be as short as possible (low Inductance).

Current monitor signal

- Impedance 50 Ω.
- Enabling detailed power consumption monitoring.
- Spectrum: 1 MHz -1000 MHz.
- Output voltage: -400 mV... +400 mV.
- Current monitor with 50 Ω output impedance must be connected via 50 Ω cables to 50 Ω input impedance of oscilloscope.

Voltage monitor

- 50 Ω tap on the out-port for connection to an oscilloscope.
- Enabling detailed monitoring of the voltage glitch.
- Voltage monitor with 50 Ω output impedance must be connected via 50 Ω Cables to 50 Ω input impedance of oscilloscope. As a result, 'Voltage monitor 50 Ω' signal will be half of 'out' voltage.
- Output voltage: -0.5 V... +2V.

Voltage protection

- Power supply inputs have NO overvoltage protection and rely on the external power supply.
- Signal out is NOT short circuit protected.

Heat protection

– Internal power dissipation is handled by the ventilator blowing the generated air into the heat sink.

Port	Label	Description
A1	Signal out	PCB connector to solder copper strips.
A2	Signal out	SMB connector to connect target.
A3	Signal out	Female-header connector to connect target.
B1	PSU1	12V DC Power supply input.
B2	-power ok	-12V Power status LED.
B3	PSU2	12V DC Power supply input.
B4	+power ok	+12V Power status LED.
B5	Current Monitor 50 Ω	SMB, 50 Ω analog output.
B6	Voltage Monitor 50 Ω	SMB, 50 Ω analog output.
B7	Signal in 50 Ω	SMB, 50 Ω analog input, -0.5... +2 V Controls the voltage at signal out.

KEYSIGHT

Edition 1, October 2024

DS1322-90002

www.keysight.com