Glitch Amplifier

Quick Start Guide

What is in the box **3**

What does it do **6**

How to build a setup **8**

How to mount the Glitch Amplifier **10**

Using the Copper strips **13**

Glitch Needle **15**

Glitch needle setup **17**

Mounting Glitch Needle **19**

Technical specifications **22**

Declaration of conformity **27**

Disclaimer

Every effort have been made to make this document as complete and as accurate as possible, but no warranty of fitness is implied. The information is provided on an as-is basis. Riscure shall have neither liability nor responsibility to any person or entity with respect to any loss or damage arising from the information contained in this documentation.

The information contained in this document is subject to change without notice.

The Glitch Amplifier must be used according to the Glitch Amplifier user guide. Any operation related to maintenance, repair or calibration must be carried out by qualified personnel. Consequently, in case of failure, contact Riscure to find out about the procedure to follow.

Manufactured by

Riscure BV

Delftechpark 49, 2628 XJ Delft, The Netherlands
Phone: +31 15 251 40 90, Fax: +31 15 251 40 99

Email: inforequest@riscure.com
Web: www.riscure.com

What is in the box

The box contains the Glitch Amplifier and all accessories to connect it to an oscilloscope.

Box content checklist

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

Quantity [1]	Description	Photo	Identifier [2]
2	Copper Strip, 3ft		
1	Hex Key		
4	Feet		
4	Screw thread		
1	Glitch Needle: - Glitch Needle Box - Glitch 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- Quick Start Guide”		

[1] Quantity of items registered in the package

[2] Identifier used in references in this document.

What does it do

The Glitch Amplifier is device to power embedded targets, for example, FPGA's of SOC's.

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

A pulse generator like Riscure VC-Glitcher or Spider can generate the signal for glitching.

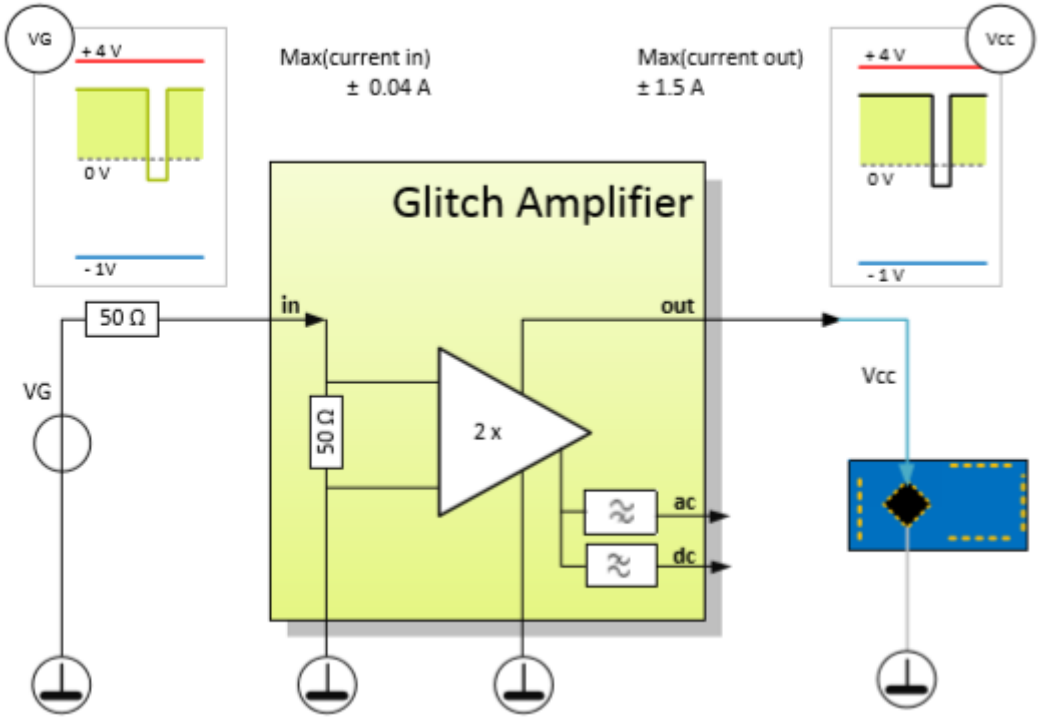


Figure 1 Functional overview of Glitch Amplifier.

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 Riscure icWaves to implement dynamic glitching attacks.

Basic setup

The Power of the Glitch Amplifier is supplied by two **identical** PSU's in a Cascaded configuration.

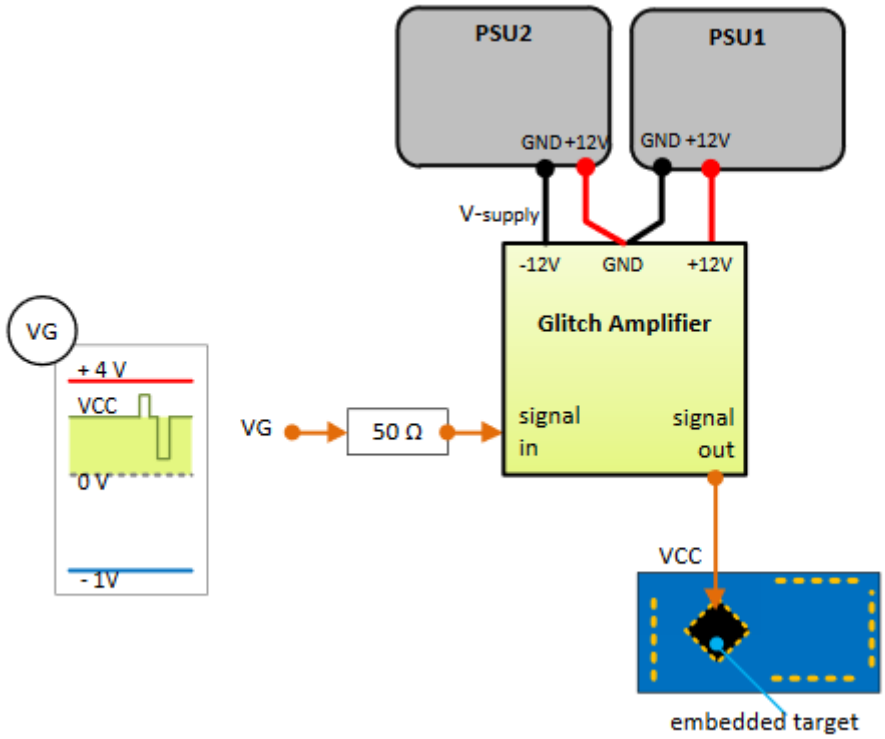


Figure 2 Basic setup of Glitch Amplifier.

How to build a setup

Setup for static power glitching

Additional products used: Spider.
In this setup, Glitch Amplifier powers the target and transfers voltage glitches.
The Supply voltage level (vcc) and voltage glitches are generated by Spider.

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

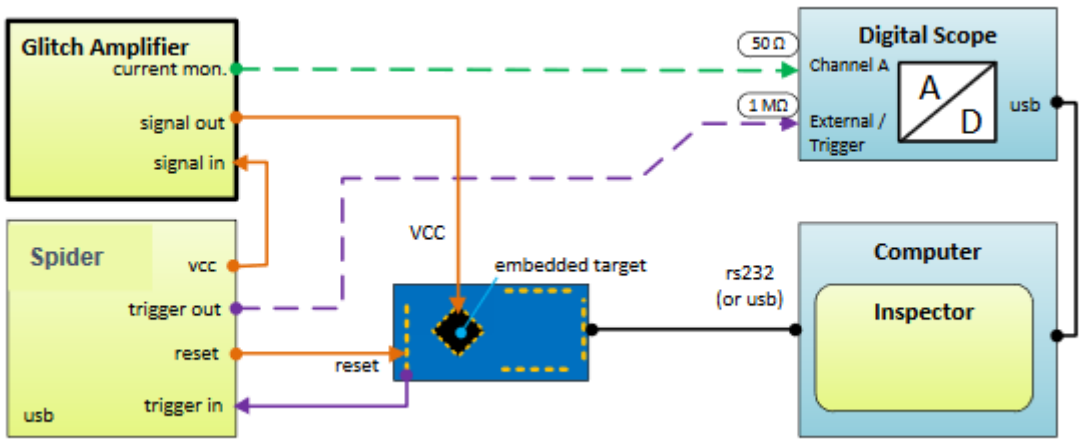


Figure 3 Perturbation of the power supply line with static timing.

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

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: Spider, icWaves.
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 icWaves using the Glitch Amplifier current monitor Signal.

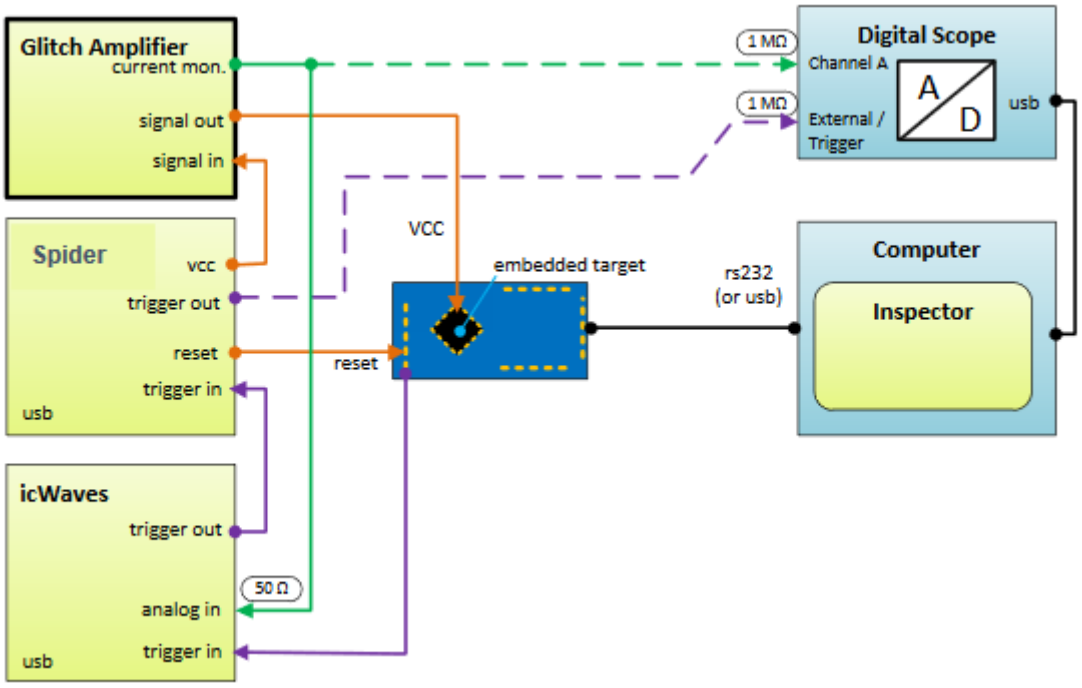


Figure 4 Perturbation of the power supply line with dynamic timing

The power signal is connected to the high impeddance input of the scope to prevent loss of signal quality for the icWaves.

The analog input of icWaves 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 in to the screw holes of the bracket.

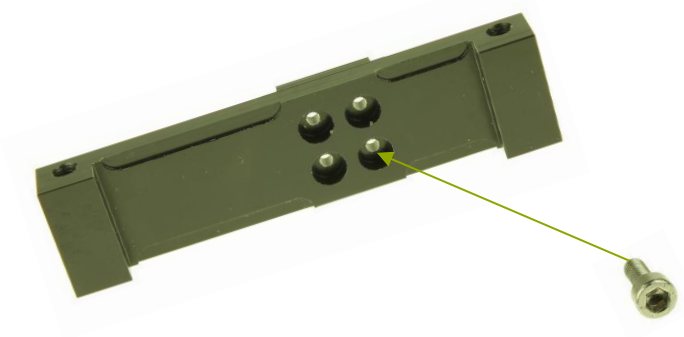


Figure 6 Mounting bracket.

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 thread's to adjust the height of the Glitch Amplifier.
Place the screw thread's inside the bracket's corner holes.
Adjust them by hand, the screw thread will go thru 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 Riscure base plate (from the EM-Probe station or 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.

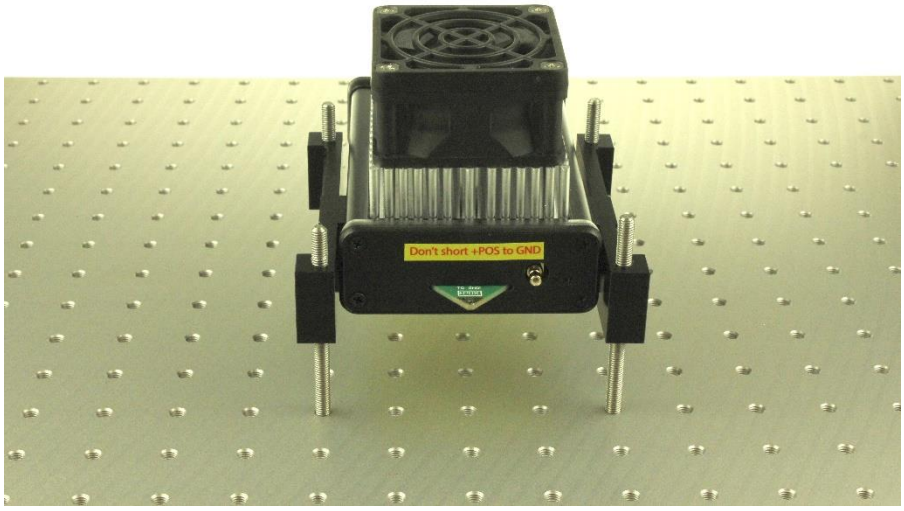


Figure 8 Glitch Amplifier on Base plate.

Using the Copper strips

Prepairing 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 adheasive slayer.

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.

Glitch Needle

What does it do

The Glitch 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 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.

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

Figure 9 Glitch Needle attached with 3ft SMB cable.

Glitch needle setup

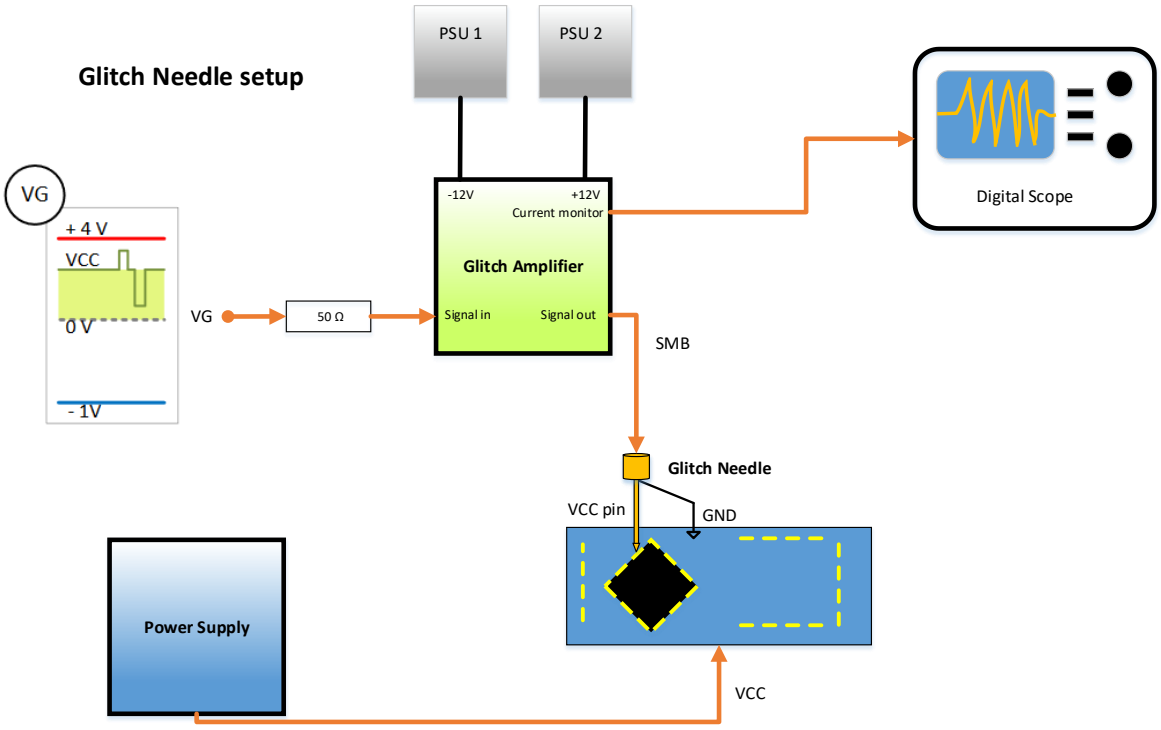


Figure 10 Perturbation of the VCC pin using Glitch Needle.

Figure 11 Glitch Needle setup on a Piñata target using a Riscure XYZ Stage and 3D positioner.

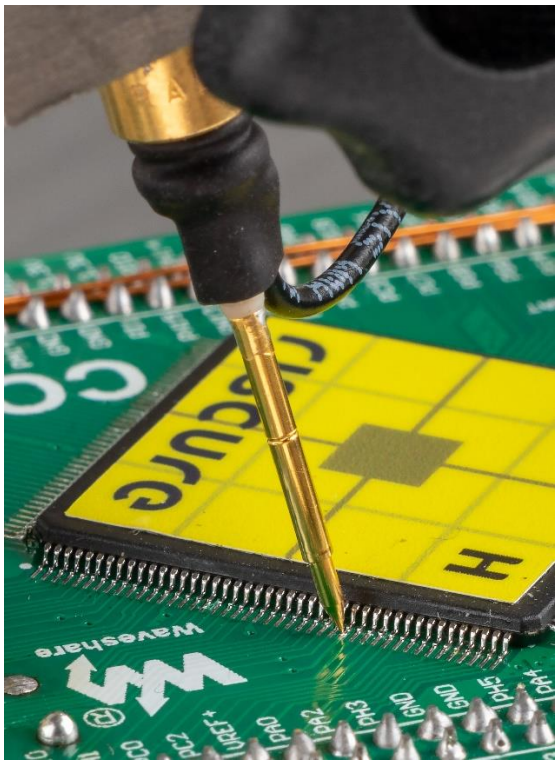


Figure 12 Close-up of Glitch Needle on Piñata target pin

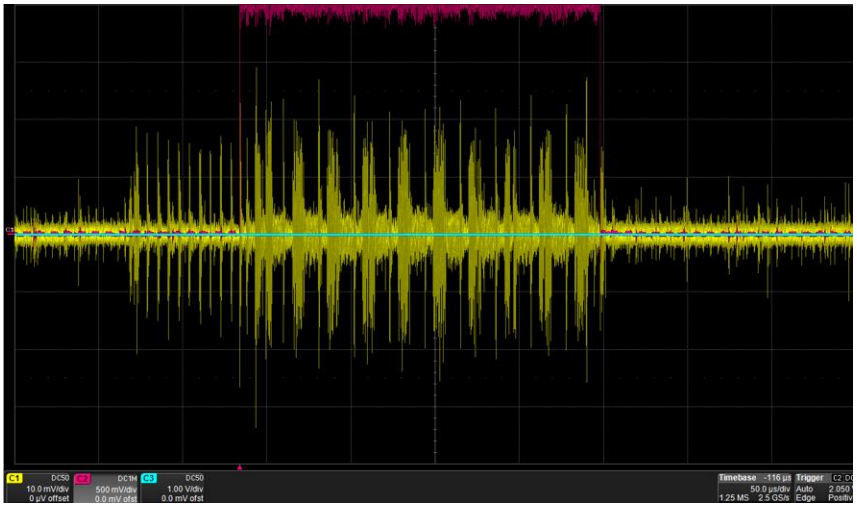


Figure 13 Piñata AES target measured with Glitch Needle on the current monitor port of Glitch Amplifier.

Mounting Glitch Needle

Mouting

There are multiple way’s of mounting Glitch Needle on the target.

- Mountting with 3D positioner

Figure 14 Glitch Needle using a 3D positioner

- Mounting with XYZ-base plate

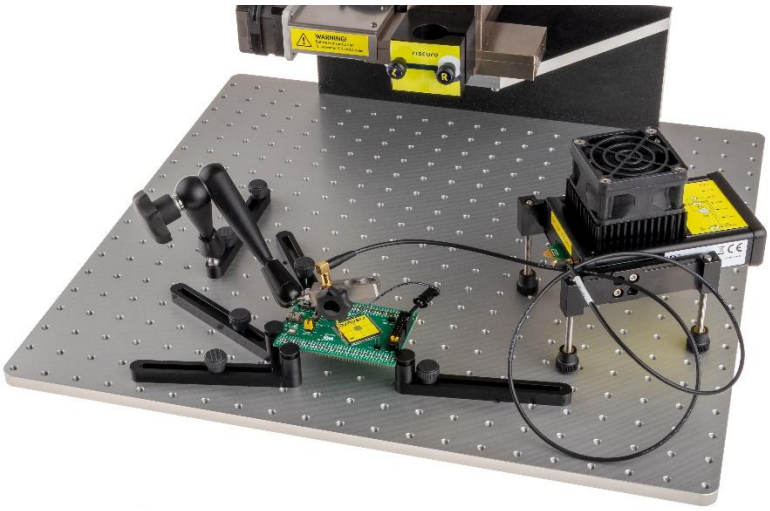


Figure 15 Glitch Needle using a XYZ-Base plate

- Mounting with XYZ-Stage

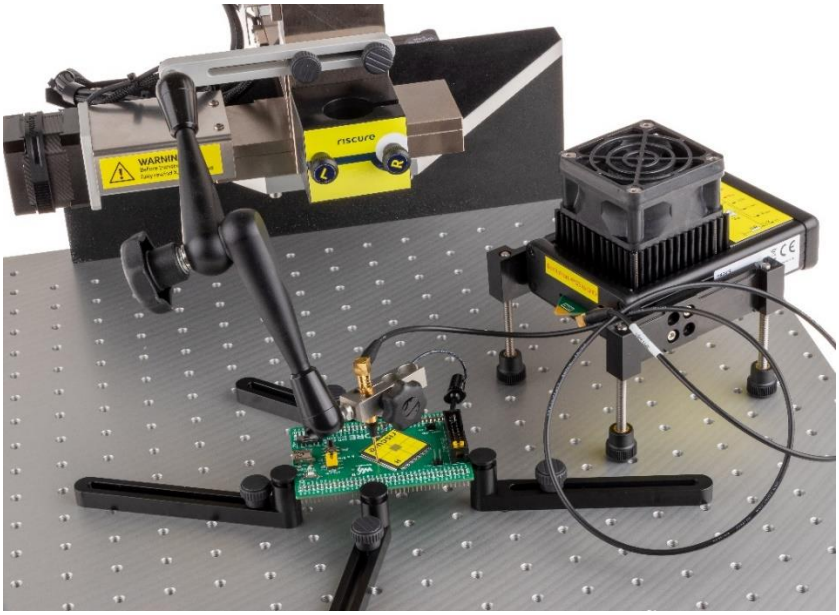


Figure 16 Glitch Needle using a XYZ-Stage

- Mounting directly on Glitch Amplifier

Figure 17 Glitch Needle Directly mounted on Glitch Amplifier

Still have questions?

1. Visit the Riscure Support Portal: http://support.riscure.com.

Technical specifications

Operational conditions

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

Do not block the ventilation holes of the Glitch Amplifier.
A blocked airflow may cause malfunction or break down.

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

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

Power supplier are 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.

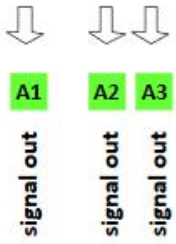
Voltage Protection

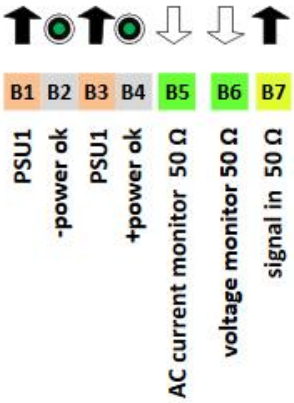
- Power supply inputs have NO overvoltage protection, and relay on the external Power supply.
- Signal out is NOT short circuit protected.

Heat Protection

- Internal power dissipation is handled by the ventilator blowing the generated air In too the heat sink.


Don't short +POS to GND


A1
A2
A3
signal out
signal out
signal out


B1
B2
B3
B4
B5
B6
B7
PSU1
-power ok
PSU1
+power ok
AC current monitor 50 Ω
voltage monitor 50 Ω
signal in 50 Ω

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.

Declaration of conformity

EC-DECLARATION OF CONFORMITY

Suppliers Details

Name
Riscure B.V.
Address
Frontier Building, Delftechpark 49, 2628 XJ Delft, The Netherlands

Product Details

Product Name
Inspector
Model Name(s)
Glitch Amplifier
Trade Name
Riscure

Applicable Standards Details

Directives:
- LVD (2006/95/EC) - EMC directive (2004/108/EC)

Standards:
- IEC 60825-1; IEC 320 C8; IEC 60950-1; 21 CFR 1040; ANSI/ESD S20.20:2007; BS EN 61340-5-1:2007; EN55022-B; EN61000-4-2, 4-5; CISPR 11; CISPR22-B; UL 1950

Supplementary Information

The appliance fulfils the relevant requirements of the EMC-directive and the LVD-directive according to our technical documentation TCD-Glitch Amplifier.

Declaration

I hereby declare under our sole responsibility that the product(s) mentioned above to which this declaration relates complies with the above mentioned standards and Directives

Name: Dr.ir. F.G. de Beer / Technical Director
Issued Date: 02 / 05 / 2013

Signature of representative

Riscure B.V.
Frontier Building
Delftechpark 49
2628 XJ Delft
The Netherlands
Tel.nr.: +31 (0) 15 251 4090