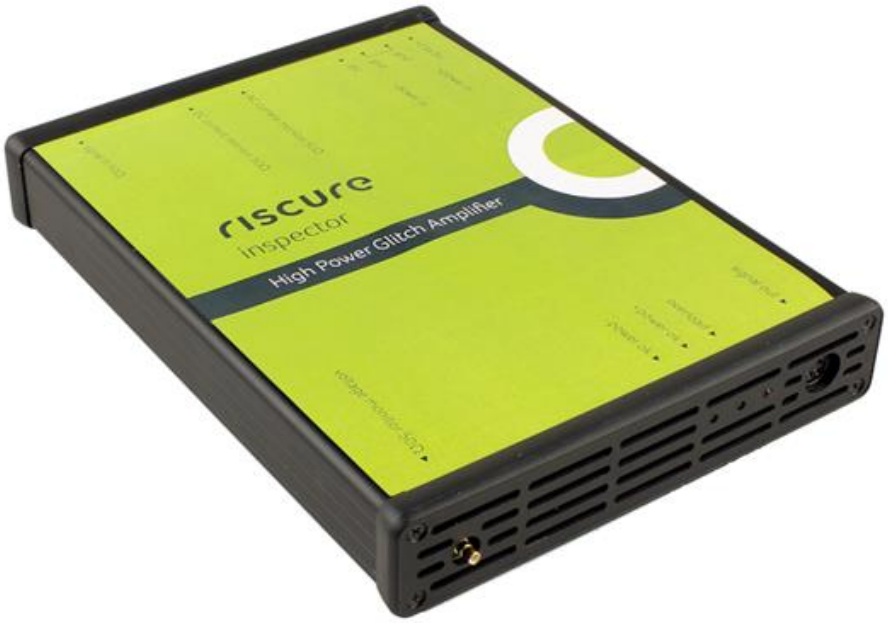
High Power Glitch Amplifier

Quick Start Guide



What is in the box

In the box you will find the High Power Glitch Amplifier and all accessories to connect it to an embedded target and a glitch generator.

Box content checklist

Qty [1]	Description	Photo	Identifier [2]
1	High Power Glitch Amplifier		HPGA
2	Power supply unit (Agilent E3633A or Keysight E3633A). Input 100 V .. 240 V AC, 50 .. 60 Hz. Power cable (country specific) included.	 	PSU1, PSU2
1	Signal cable: - BNC-SMB, coax, 50 Ω, 3 ft.		
1	Signal cable: - SMB-SMB, coax, 50 Ω, 3 ft.		

Qty [1]	Description	Photo	Identifier [2]
4	Power supply cable - red/black, banana plugs ø 4 mm, gold, max. 32 A		
1	Target supply cable - custom 4-pin connector to red/black twisted wires		
	This “High Power Glitch Amplifier- Quick Start Guide”		

[1] Qty = Quantity, the number of units in the box

[2] The identifier is used for reference in this document only.

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 does it do

The High Power Glitch Amplifier (HPGA) is a device to power a target with a high power consumption, for example an embedded processor.

While mainstream power supplies are designed to stabilize the voltage and thus suppress high frequency noise, the HPGA is capable of applying high speed glitches in the supply voltage line while the target consumes a current up to 10 A.

The signal for glitching can be generated by a pulse generator like Riscure's VC Glitcher.

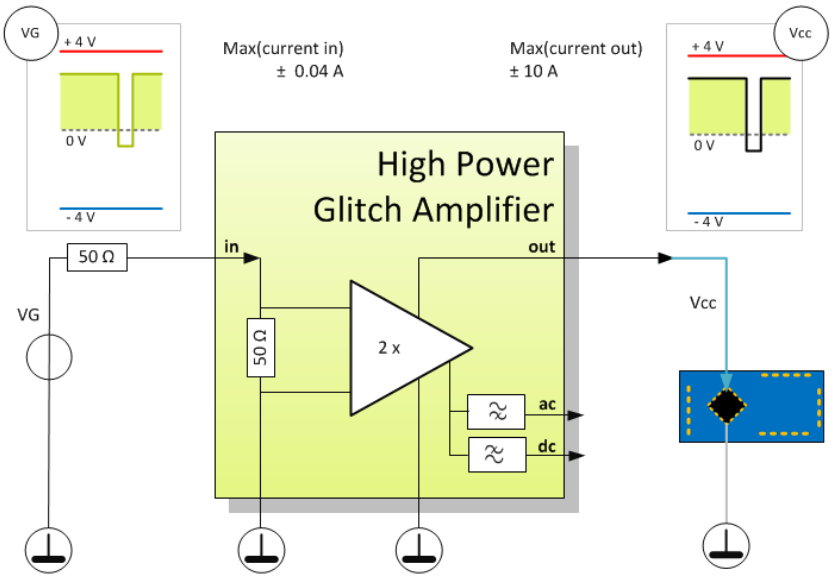


Figure 1 Functional overview of the High Power Glitch Amplifier.

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

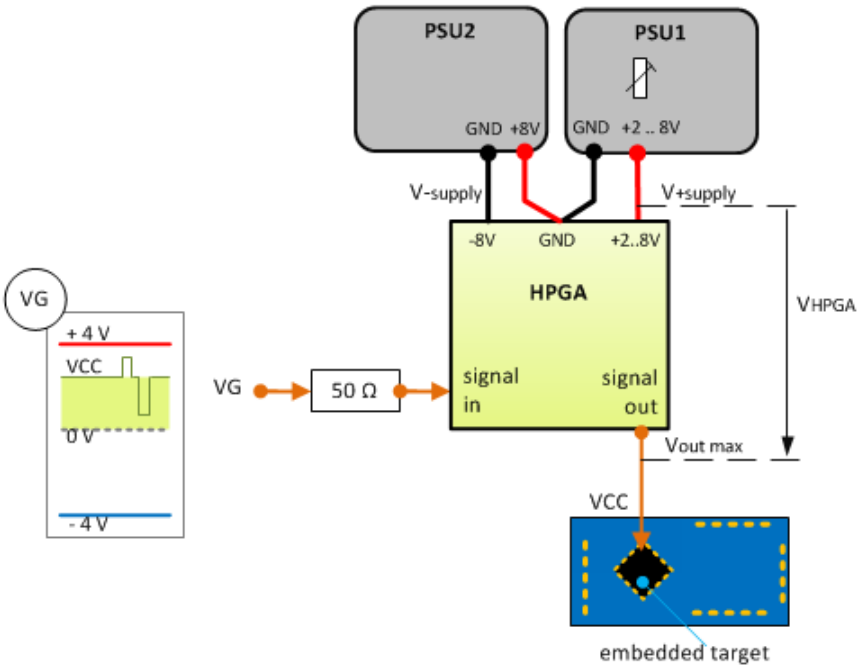
The HPGA has DC and AC monitor outputs with a signal proportional to the target's current consumption. These outputs can be used by pattern recognition devices to implement dynamic glitching attacks.

The High Power Glitch Amplifier is a stand-alone device. It is normally used in combination with Inspector and a VC Glitcher.

How to build a setup

Basic setup

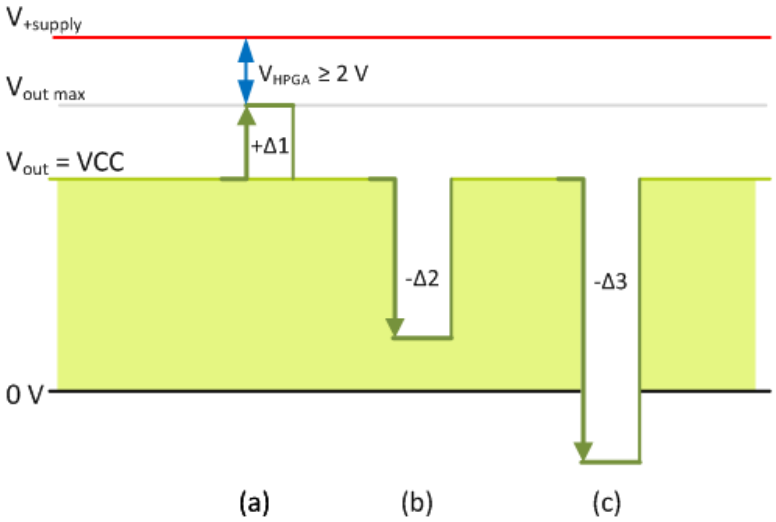
The power for the HPGA is supplied by two **identical** PSU's used in a cascaded configuration.



The HPGA has the following operational limits.

- $V_{HPGA} = V_{+supply} - V_{out\ max}$, $V_{HPGA} \geq 2$ V
  to provide sufficient voltage drop over the amplifier.
- $P_{HPGA} = I_{+supply} * V_{HPGA}$, $P_{HPGA} \leq 50$ W
  to limit internal power dissipation.

To use the HPGA within its operational limits, the user must tune the positive supply voltage $V_{+supply}$ on PSU1. $V_{+supply}$ and $I_{+supply}$ are read from the PSU display.



Two situations:

- (a) If the glitch voltage is positive then $V_{out\ max}$ equals VCC + glitch voltage.
- (b),(c) If the glitch voltage is negative then $V_{out\ max}$ equals VCC.

Example

Your target needs to run at 1.2 V and consumes 8 A. You want to apply negative voltage glitches of 1.5 V.

In the Inspector perturbation module dialog, you configure ‘vcc’ (VG) to 1.2 V and ‘glitch voltage’ to ‘-1.5 V’. Now $V_{out\ max}$ equals vcc = 1.2 V. Then $V_{+supply}$ needs to be at least 1.2 + 2 = 3.2 V. The power dissipation by the HPGA equals 8 A * 2 V = 16 W, which is okay because it is below the limit of 30W.

Summary of PSU configuration

Both PSU's are identical. Assign one as PSU1 ($V_{+supply}$) and the other as PSU2 ($V_{-supply}$).

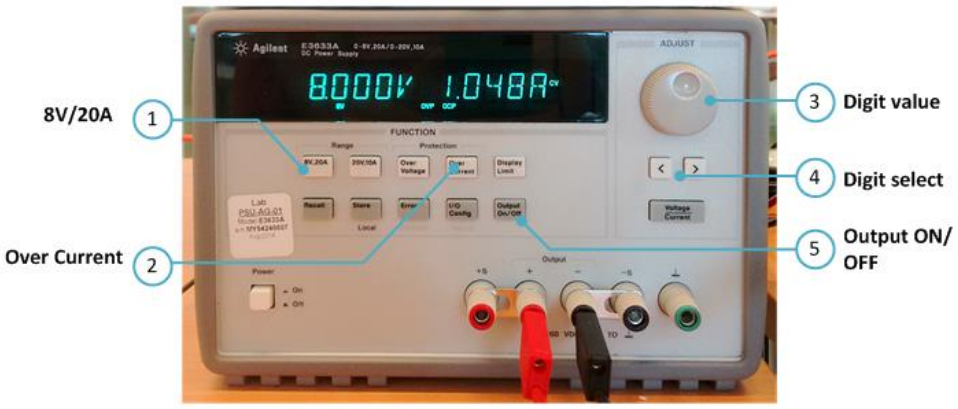
PSU1 is set to range 8V/20A, and voltage may be tuned 2.0 .. 8.0 V.

PSU2 is set to range 8V/20A, and voltage is kept at 8.0 V.

Both PSU's have the overcurrent protection set to 12 A.

Do not apply a higher voltage than **8 V!**
The HPGA is not guarded by an overvoltage protection on positive and negative supply inputs.

Always use the HPGA with both PSU's switched on.



How to configure the PSU

Before making any changes, deactivate the power supply to the HPGA:

- Press button (5) **Output On/Off**. The display changes to "OUTPUT OFF".

Set the PSU to 8V control mode:

- Press button (1) **8V/20A**.

- Optionally lower the voltage by using dial (3) and buttons (4).

Protect the HPGA by limiting the maximum current to 12A:

- Press button (2) **Over Current** protection. The display changes to “LEVEL xx.xx A”, and a digit is flashing.
- Use buttons (4) to select a digit, and use dial (3) to choose its decimal value. Set the value to **12.00** A.
- Press button (2) **Over Current** again to acknowledge the protection level. The display shows “OCP ON” and changes after a few seconds to “OUTPUT OFF” again.

Activate the power supply to the target again:

- Press button (5) **Output On/Off**.
  The display changes to “OUTPUT ON”, and after a few seconds shows the measured voltage and current.
  A small sign “**ocp**” is lit to show the over-current protection is active.

Use the Store and Recall buttons to save settings.
See the PSU manual.

Setup for static power glitching

Additional products used: VC Glitcher.

In this setup, the High Power Glitch Amplifier powers the target and transfers voltages glitches. The supply voltage level (vcc) and voltage glitches are generated by a VC Glitcher.

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

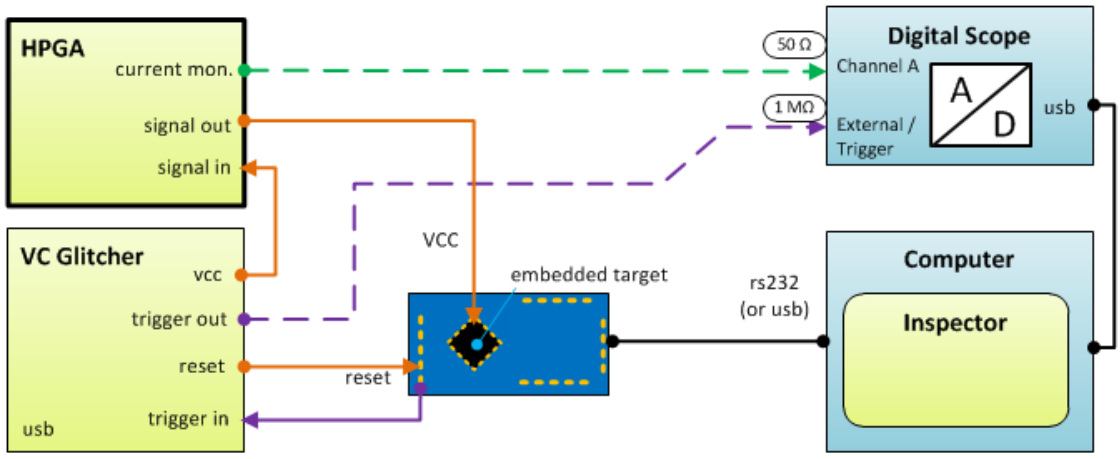


Figure 2 Perturbation of the power supply line with static timing.

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 High Power Glitch Amplifier and the target as short as possible. Both wires should be close together or even better be twisted.
Short and twisted cables have a low inductance providing better power consumption readings and better glitch effects.

Setup for dynamic power glitching

Additional products used: VC Glitcher, 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 AC (or DC) HPGA current monitor signal.

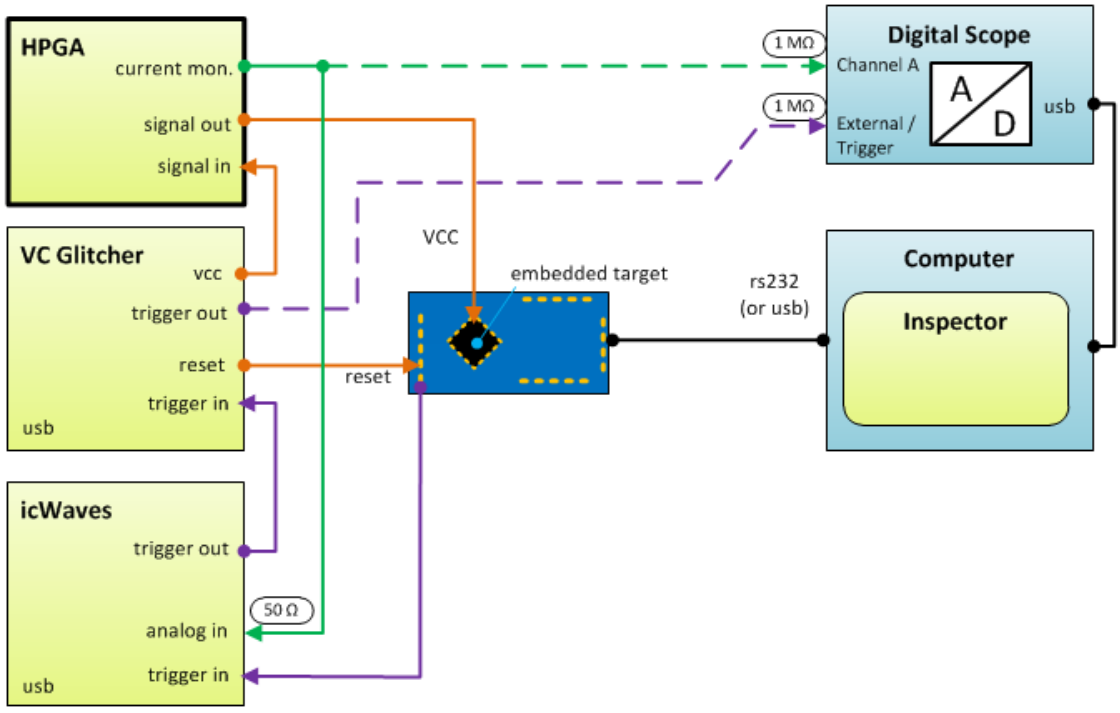


Figure 3 Perturbation of the power supply line with dynamic timing

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

The analog input of icWaves 3 has software selectable impedance 50 Ω / 1 MΩ. Configure it for 50 Ω.

Help and troubleshooting

Common problems

Signal/Behavior	Cause/Solution
Red overload LED is flashing	**Cause**: The HPGA has become too hot. **Solution**: ▪ Ensure that $V_{-supply}$ is ON (drives the cooling fans). ▪ Disconnect the target. Wait until the HPGA has cooled down. ▪ Do not block the ventilation vents. ▪ Lower the $V_{+supply}$.  Reconsider the current load conditions of your target.
Red overload LED is ON	**Cause:** The power supply voltage is unsufficient for the HPGA to control. **Solution:** Set $V_{+supply}$ to a value above 2 V.
Green LED is OFF	**Cause**: Power supply input is not active because related PSU is in “OUTPUT OFF” mode. **Solution**: Press button OUTPUT ON/OFF on related PSU.
Different intensity of green LEDs	The intensity is proportional to the supply voltage. So a difference between LED’s means the $V_{+supply}$ and $V_{-supply}$ have been set tot different values.

Still have questions?

Visit our Riscure Support Portal: https://support.riscure.com.

Technical specifications

Operational conditions

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

Do not block the ventilation holes of the High Power Glitch Amplifier. A blocked air flow may cause malfunction.

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

Turning OFF the High Power Glitch Amplifier is not required but recommended when not used for an extended period of time.

Power supply

- Positive DC supply, adjustable +2 .. 8 V
- Negative DC supply, fixed at -8 V
- Both supplies are capable of driving 11 A (HPGA consumption 1 A + target consumption 10 A)

High Power Glitch Amplifier is not protected against over voltage. Supply voltage should not exceed 8 V at any time.

Signal input

- Input impedance 50 Ω.
- Max. voltage range: -2 V .. +2 V.
- Source must be connected with 50 Ω cable.

Signal output

- Output impedance: < 30 mΩ.

- Amplification: 2 x
- Bandwidth: DC .. 50 MHz @ -3dB, 100 MHz @ -6dB
- Capable of sourcing and sinking up to 10 A.
- Slew rate: > 600 V/µs @ 10 A, glitch -4.8 V
- Short circuit protected.

DC Power plug 4-pin layout. Each pin capable of handling currents of 7.5 A. (e.g. model KPPX-4P manufactured by Kycon).

DC Current monitor signal

- Impedance 50 Ω
- Intended for low frequency, long duration overview traces
- Spectrum: DC – 1 MHz
- Output voltage: nominal 100 mV/A

AC Current monitor signal

- Impedance 50 Ω
- Enabling detailed power consumption monitoring.
- Intended for high frequency, short duration traces.
- Spectrum: 1 MHz - 1000 MHz
- Output voltage: -400 mV.. +400 mV

Voltage monitor

- 50Ω Tap on the signal out-port for connection to an oscilloscope.
- Enabling detailed monitoring of the voltage glitch.

This output should be loaded by 50Ω input impedance of oscilloscope for best quality view of the glitch. Keep in mind, the measured voltage will be **signal out / 2**.

Voltage Protection

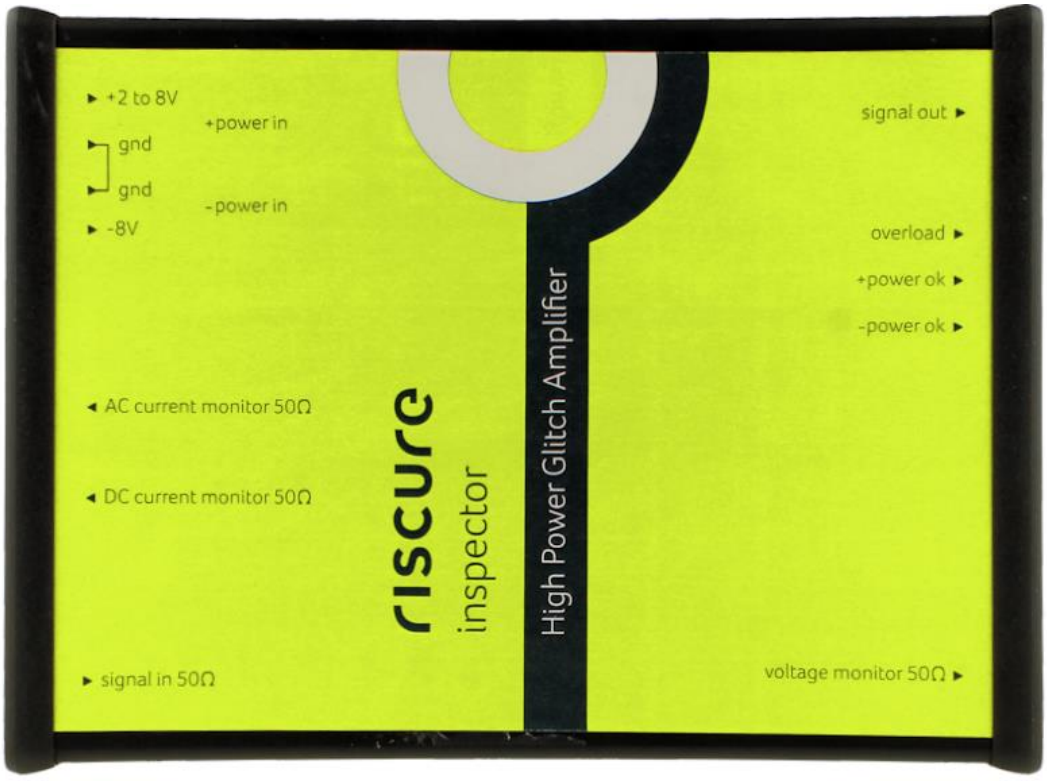
- Power supply inputs have NO overvoltage protection, and rely on the external power supply.
- Signal out is short-circuit protected.

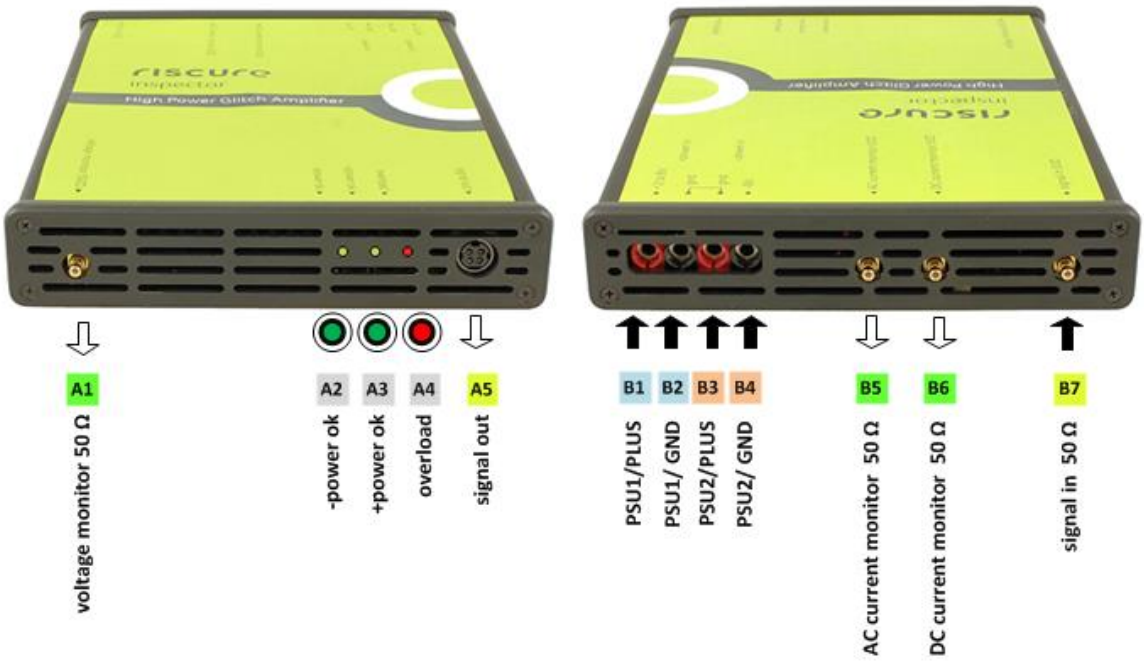
Heat Protection

- Internal power dissipation is handled by built-in ventilators to blow the generated hot air out of the housing.
- If the HPGA gets overheated, a thermal protection will activate which causes the output voltage to drop and the overload LED to be flashing.
  The thermal protection will deactivate automatically when the temperature has sufficiently dropped.

Product case

Dimensions (L x W x H): 220 x 170 x 35 [mm], 8.66 x 6.67 x 1.36 [inch]





Port	Label	Description
A1	**voltage monitor 50 Ω**	SMB, 50 Ω, analog output, -4 V .. +4 V Tap on signal out port to connect with an oscilloscope.
A2	**-power ok**	Green LED. ON = $V_{-supply}$ present. OFF = no power.
A3	**+power ok**	Green LED. ON = $V_{+supply}$ present. OFF = no power.
A4	**overload**	Red LED. ON = HPGA overheated. OFF = normal operation.
A5	**signal out**	SMB, ≤ 30 mΩ, analog output, -4 V .. +4 V DC Voltage proportional to 2x signal in.
B1	**+2 to 8V**	Banana plug connector, $V_{+supply}$. Connected to positive outlet (red) of PSU1.
B2	**gnd**	Banana plug connector. Connected to ground outlet (black) of PSU1.
B3	**gnd**	Banana plug connector, $V_{-supply}$. Connected to positive outlet (red) of PSU2.
B4	**-8V**	Banana plug connector. Connected to ground outlet (black) of PSU2.
B5	**AC current monitor 50 Ω**	SMB, 50 Ω, analog output
B6	**DC current monitor 50 Ω**	SMB, 50 Ω, analog output
B7	**signal in 50 Ω**	SMB, 50 Ω, analog input, -2 .. +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)

High Power 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-High Power 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: 13 / 05 / 2015

Signature of representative

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