riscure

Glitch Amplifier 2

datasheet
v1

Contents

The product

Why we started it

Observations

Fault Injection attacks become more popular and as a result real world examples of devices and chips being hacked with this technology are seen regularly.

This increases the need for chip and embedded system vendors to have devices which they can use to efficiently test their products and implemented counter measures against fault injection vulnerabilities.

One of the fault injection methods often being used is voltage glitching where the attacker tries to influence device behavior by changing the voltage provided to the target for a very short timeframe (microseconds).

This is exactly what the glitch amplifier 2 can do. Controlling the power line of a device and produce fast and sharp voltage glitches (positive and negative) to test the device on vulnerabilities for these kind of attacks.

We decided to upgrade the Glitch Amplifier to a more accurate version that can produce faster and sharper glitches as ever before and at the same time include additional functionality as requested by users.

Improvements of the Glitch Amplifier 2

1. Increased glitch success rate because of sharper glitches.
2. Integrated current and power monitor
3. Easy to position closely above your target
4. Easy connection to your target via one of the three output connectors that Glitch Amplifier 2 offers.
5. Can be used in combination with EM probe station baseplate. Glitch Amplifier 2 exactly fits to the baseplates grid.

The challenge it solves

Challenges that are solved with Glitch Amplifier 2:

1. Sharper and faster glitches

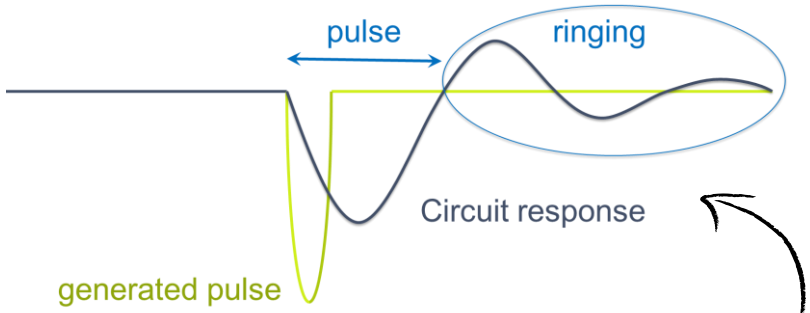
   Glitch Amplifier 2 internals are optimized to produce voltage glitches at target's power pin which are just as fast and sharp as the pulses from pulse generator. Same pulse strength and the same pulse duration. This dramatically increases the glitch success rate.

2. Position close to the target to optimize glitch performance and minimize ringing

   Long wires between the glitch amplifier and the target have a bad effect on the desired glitch shape due to added inductance between Glitch Amplifier and target. Glitch Amplifier 2 can be positioned very close to the target and comes with special coper strips that can be soldered on to minimize this effect and as a result maximizes results.

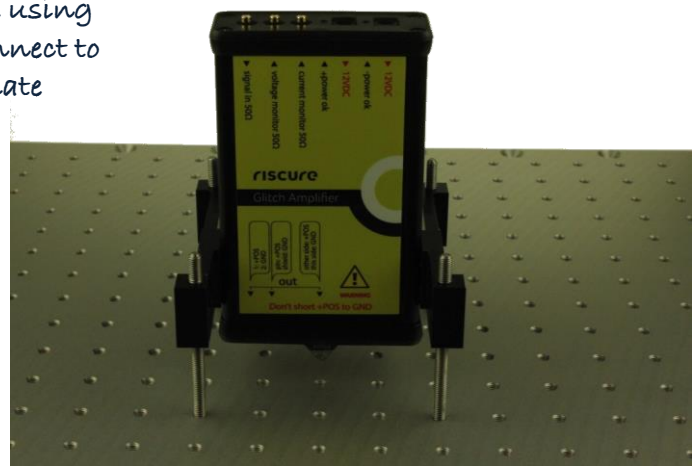
3. Directly see how the voltage glitch performs on the target

   Usually you want to see the effect that the voltage glitch has on the target and for this a current probe can be added to the setup. Drawback of this is that adding a current probe to the setup has a negative effect on the speed and sharpness of the glitch. To overcome this, Glitch Amplifier 2 has integrated measurement circuits that give you an insight in the glitch without influencing it.



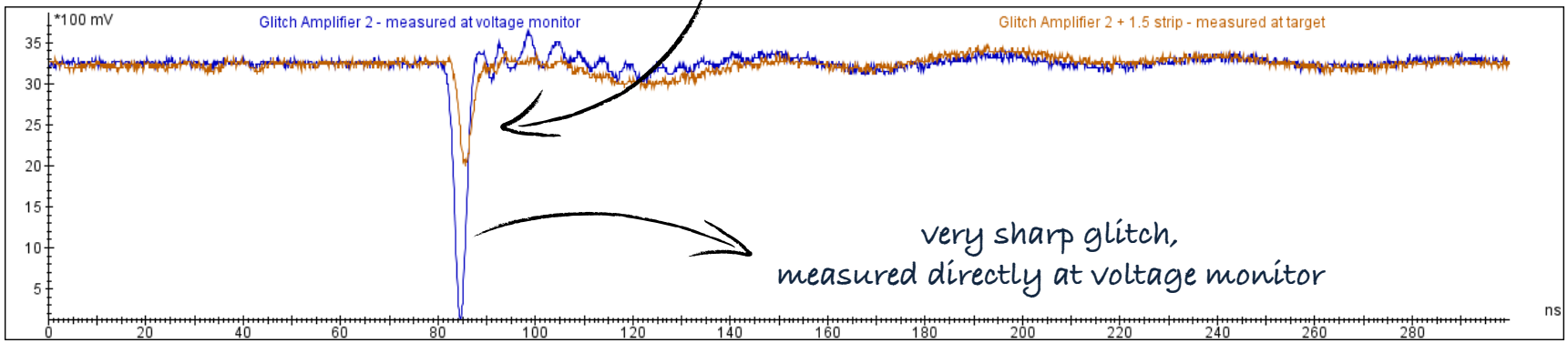
Closer positioning to target and using shorter wires results in sharper glitches and less ringing

Use Glitch Amplifier 2 stand alone using the foots or connect to XY base plate



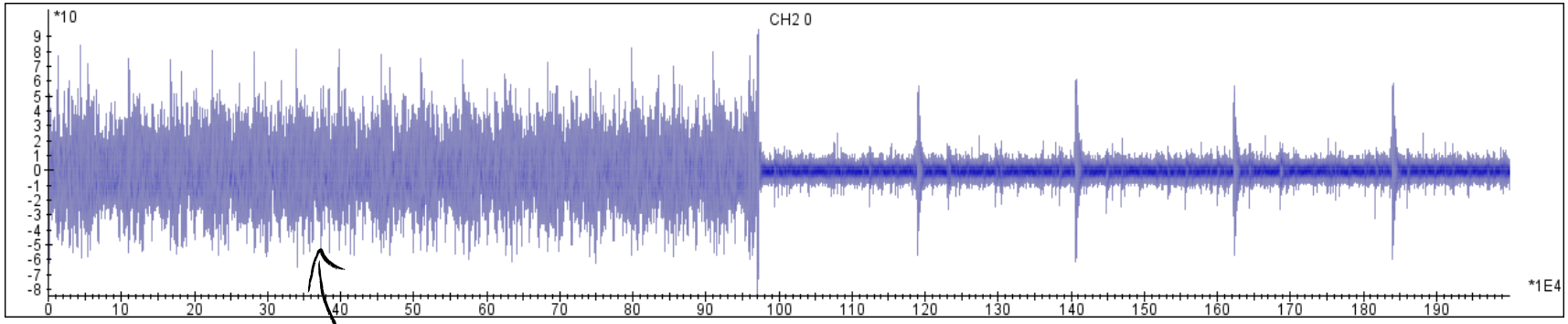
Unique selling points

sharp glitch,
measured at target



very sharp glitch,
measured directly at voltage monitor

Current monitor



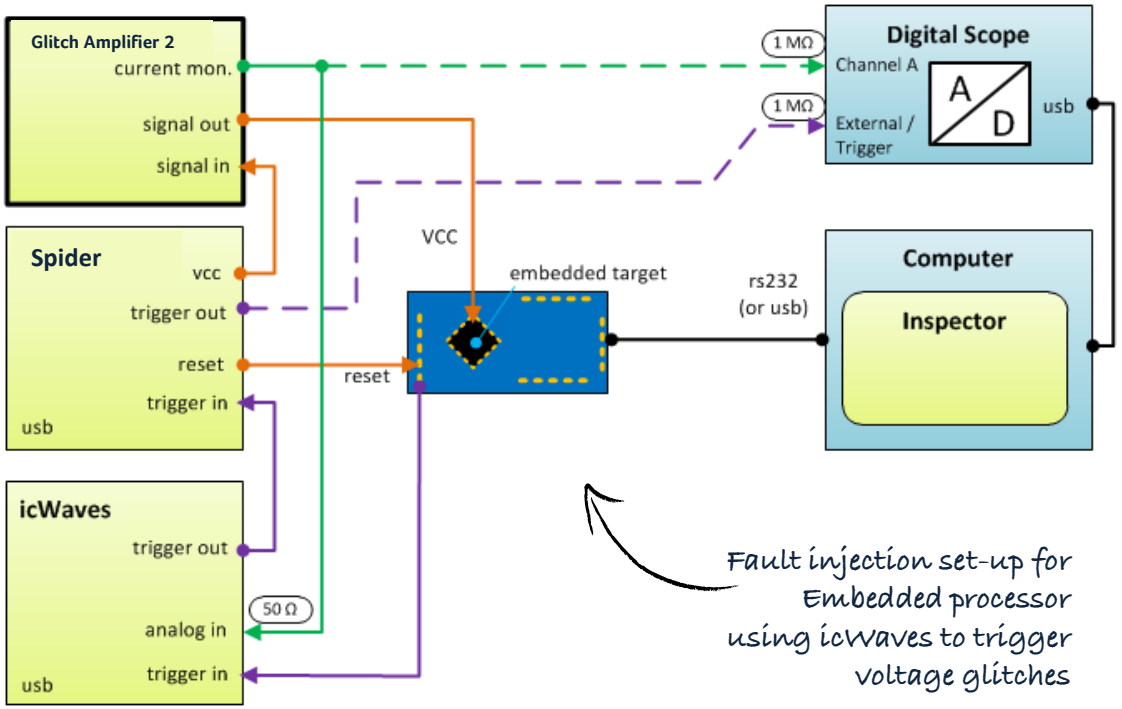
Integrated current and voltage monitors enable to see the glitch effect on the target without adding additional measurement devices. This works efficient and increases the glitch success rate of the setup

Example use case

Use case – Voltage glitching on Embedded Processor

The test scenario

1. Connect Spider to Glitch Amplifier 2 for voltage glitch generation
2. Feed Glitch Amplifier 2 current monitor signal to oscilloscope for analysis and to icWaves for pattern detection
3. Use icWaves for analog pattern based fault triggering
4. Inspector communicates to target over USB, rs 232 and collects measurement results



Technical details

Technical specifications

Specs

Signal in

- Input impedance 50 Ω.
- Max. voltage range: -0.5 V .. +2 V.
- 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 is compensated by a 2x amplification.

Out

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

Current monitor 50 Ω

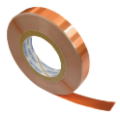
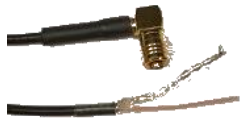
- Impedance 50 Ω
- Enabling detailed power consumption monitoring
- Spectrum: 1 MHz – 1000MHz
- Output voltage: -400 mV .. +400 mV
- Oscilloscope with 50 Ω input impedance must be connected via 50 Ω cable.

Voltage monitor 50 Ω

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

Package

Qty	Description	
1	Glitch Amplifier 2	
2	Power supply units (Phisong) 12V DC 0A .. 3A Input 100 V .. 240 V AC, 50 .. 60 Hz. Power cable (country specific) included.	 
10	Jumper wires: Male - Female	

Qty	Description	
1	Signal cable: - SMB-SMB, coax, 50 Ω, 3 ft.	
2	Signal cable: - BNC-SMB, coax, 50 Ω, 3 ft.	
2 X 3ft	Soldering copper	
1	Target supply cable - custom 2-pin connector	
1	Quick Start Guide	

Please contact Riscure for more information.

You can reach us by email : inforequest@riscure.com,

by phone : +31 15 251 4090 US: +1 650 646 9979

Or on the web: riscure.com.

riscure