VC Glitcher

Quick Start Guide

Disclaimer

Every effort has been made to make this documentation as a 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.

This tool must be used according to the 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.

Copyright

Manufactured by

Riscure BV

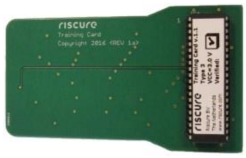
Delftechpark 49, 2628 XJ Delft, The Netherlands
Phone: +31 15 251 40 90, Fax: +31 15 251 40 99
Email: inforequest@riscure.com
Web: www.riscure.com

What is in the box

In the box you will find the VC Glitcher and all accessories to connect it to a computer and an oscilloscope.

Box content checklist

Qty	Description	Photo	Identifier (*)
1	VC Glitcher 2		VCG
1	Power supply unit, 15 V DC input 100 V to 240 V AC, 50 Hz to 60 Hz. Power cable included (country specific).		PSU
1	Communication cable: - USB, connectors USB-A to USB-B		USB
3	Signal cable: - BNC-SMB, coax, 50 Ω, 3 ft. BNC-male to SMB-female		BNC2SMB
1	Low-pass filter: - cut-off frequency, 1.9 MHz, 50 Ω BNC-male to BNC-female,		LPF1M9

Qty	Description	Photo	Identifier (*)
1	Impedance adapter: - 50 Ω, insert at 1 MΩ measurement input BNC-male to BNC-female		IMPA50
1	Smart card for testing and training purposes: - DES + PIN-verification in software		TC6
1	Extension board		
	This “VC Glitcher- Quick Start Guide”		

(*) The identifier is used for reference in this document only.

What does it do

The VC Glitcher is a plug and play smart card reader with Fault Injection (FI) capabilities. It executes programmable perturbation patterns on the card's power line or clock signal.

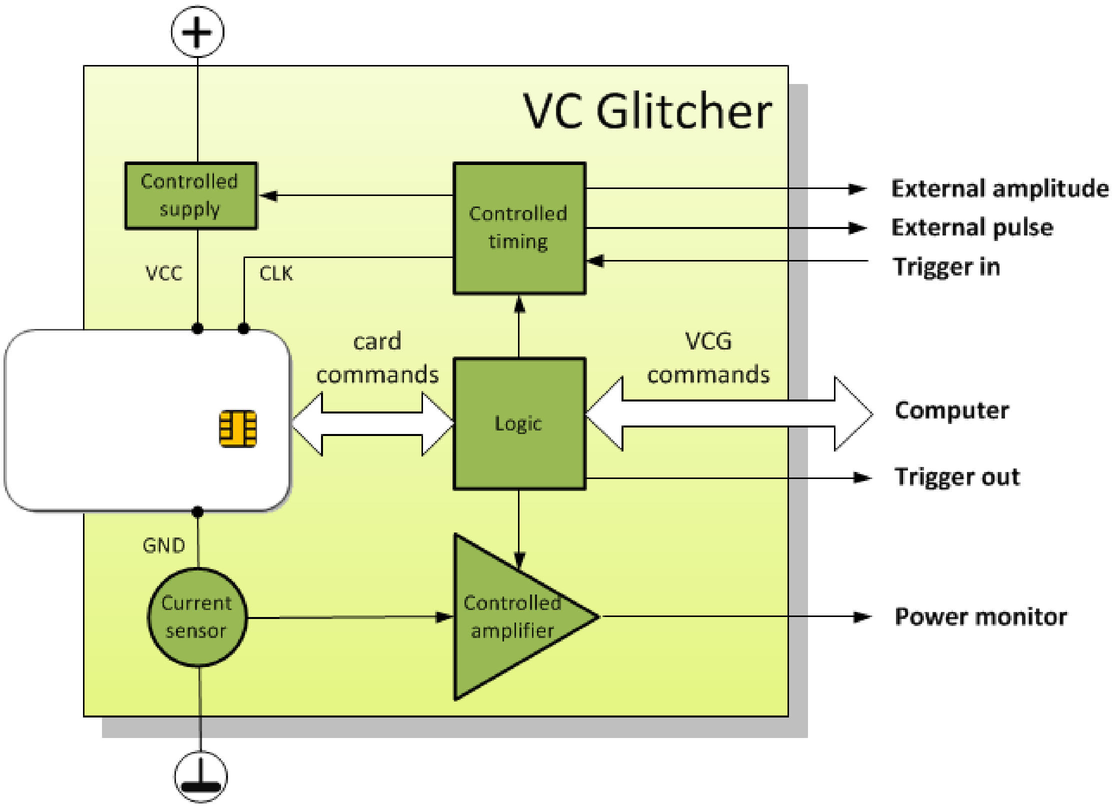


Figure 1 Functional overview of the VC Glitcher.

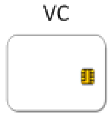
The perturbation signal is available to other types of fault injection devices such as lasers and electromagnetic pulse probes.

The VC Glitcher is normally used in combination with Inspector, the Riscure side channel software suite. You can also use the Software Development Kit (SDK) to developing custom applications that communicate with the VC Glitcher.

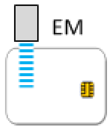
How to build a setup

The following sections describe common fault injection setups using the VC Glitcher.

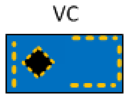
For a step-by-step connecting guide of the typical setup (Setup A), go to page 12.



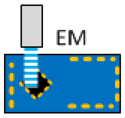
Setup A - Electric perturbation of a smart card (typical setup)



Setup B - Electromagnetic perturbation of a smart card



Setup C - Electric perturbation of an embedded target



Setup D - Electromagnetic perturbation of an embedded target

Setup A - Electric perturbation of a smart card

In this setup, the VC Glitcher submits the smart card to glitches on the power line or clock line, while the card is processing requests from the computer.

To see the card's power consumption and the appropriate timing for injection faults, connect an oscilloscope to the power monitor port.

Estimate the major glitch timing parameters: (a) offset from the start of target processing, (b) offset to the next clock transition, and (c) a glitch pattern.

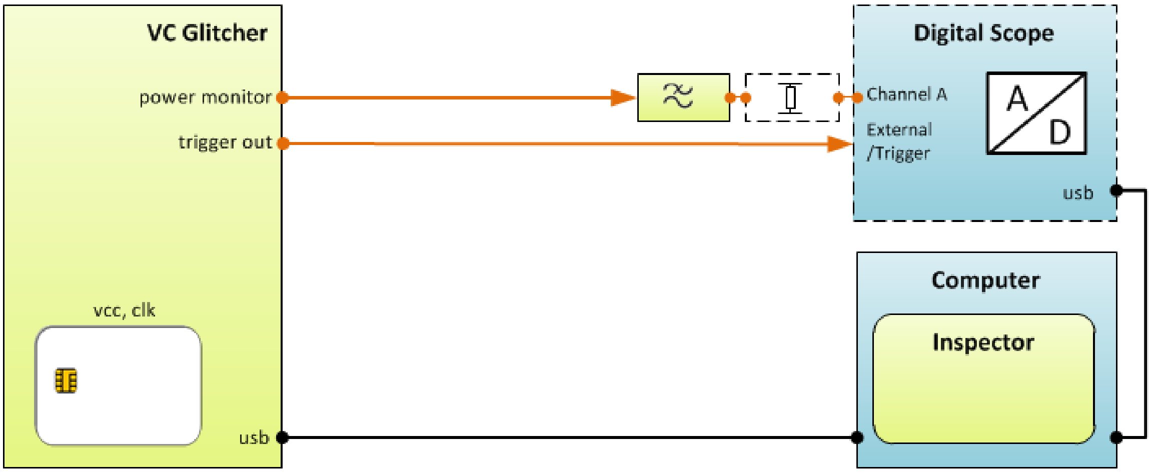


Figure 2 - Basic setup for the electrical perturbation of a smart card.

Setup B - Electromagnetic perturbation of a smart card

Additional products required: EM-FI Probe.

In this setup the VC Glitcher controls an external fault injector: the EM-FI probe. This probe sends electromagnetic (EM) pulses to a spot on the card in order to cause glitches.

The positioning of the EM-FI probe requires a high precision XYZ-motion platform, for example the EM Probe Station.

To see the card's power consumption and the appropriate timing for injection faults, connect an oscilloscope to the power monitor port.

Estimate the major glitch timing parameters: (a) offset from the start of target processing, (b) offset to the next clock transition, and (c) a glitch pattern.

Start a surface scan to find the best spot for glitching (hotspot). Fine-tune the glitch parameters on the hotspot to get the desired fault effects.

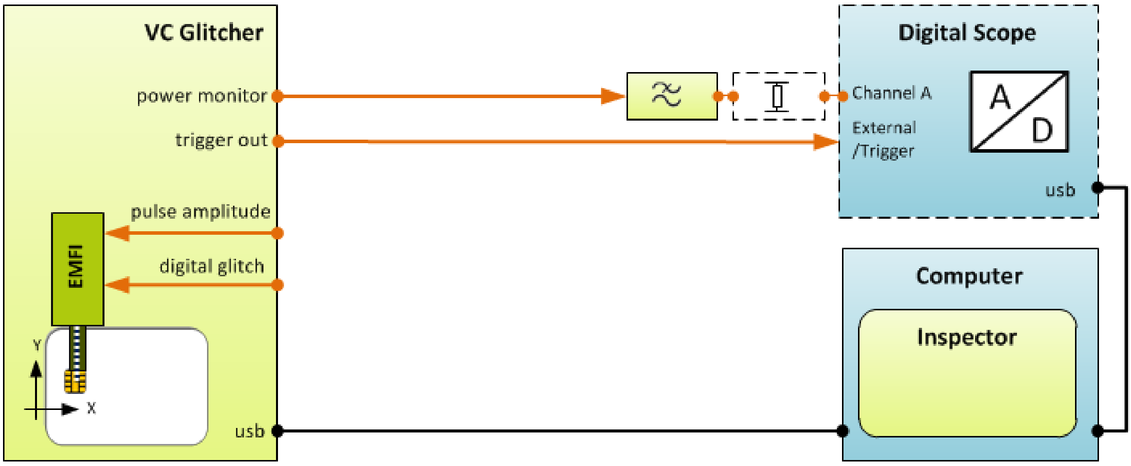


Figure 3 - Basic setup for the electromagnetic perturbation of a smart card.

Setup C - Electric perturbation of an embedded target

Additional products required: Glitch Amplifier, Current Probe

In this setup, the VC Glitcher submits an embedded target to glitches on the VCC supply line, while the target processes requests from the computer.

You need two extra components, the Glitch Amplifier and the Current Probe. The Glitch Amplifier amplifies the glitch and delivers the higher supply currents needed by the embedded target. The Current Probe picks up the power supply current to the embedded target.

Preconfigure the target to provide a trigger signal for the VC Glitcher. This signal serves as a timing reference for the perturbation program.

To find appropriate timing for fault injection, connect an oscilloscope to the Current Probe inserted in the VCC line and observe the power consumption of the target.

Estimate the major glitch timing parameters: (a) offset from the trigger instance, and (b) a glitch pattern.

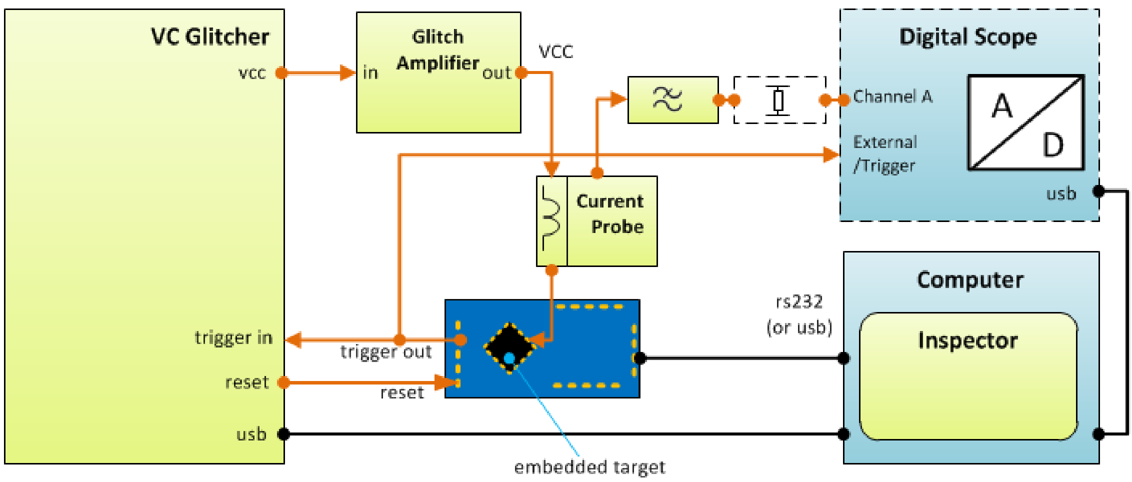


Figure 4 Setup for electric perturbation of an embedded target.

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

Do not glitch the circuitry of the RS232/USB communication peripherals!

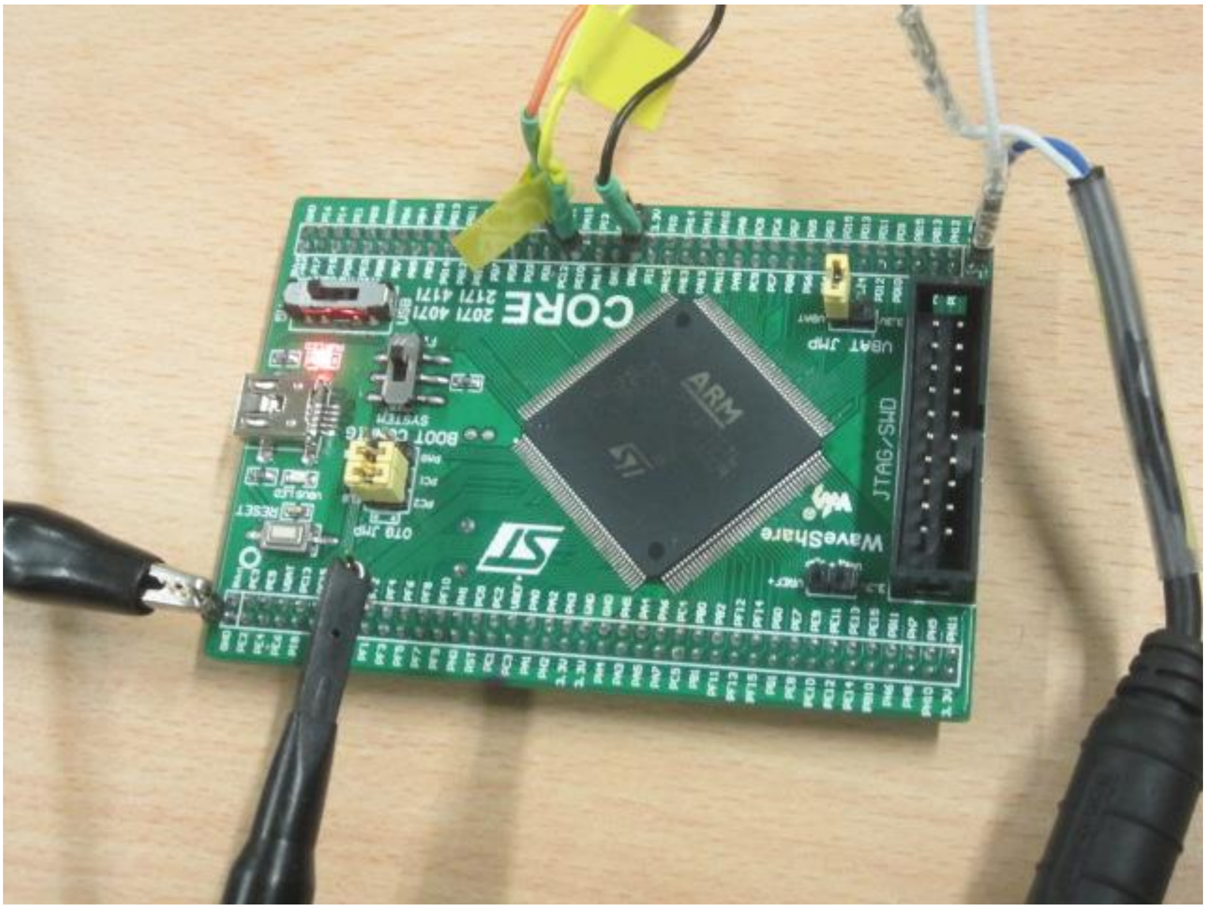


Figure 5 An example of custom wiring with an embedded target.

Setup D - Electromagnetic perturbation of an embedded target

Additional products required: EM-FI Probe, Current Probe

In this setup the VC Glitcher controls an external fault injector: the EM-FI probe. This probe sends electromagnetic (EM) pulses to a spot on the embedded target in order to cause glitches.

The positioning of the EM-FI Probe requires a high precision XYZ-motion platform, for example the EM Probe Station.

You need an extra component, the Current Probe. The Current Probe picks up the power supply current to the embedded target.

To find appropriate timing for fault injection, connect an oscilloscope to a Current Probe in the VCC line and observe the power consumption of the target.

Estimate the major glitch timing parameters: (a) offset from the trigger instance, and (b) a glitch pattern.

Start a surface scan to find the best spot for glitching (hotspot). Fine-tune the glitch parameters on the hotspot to get the desired fault effects.

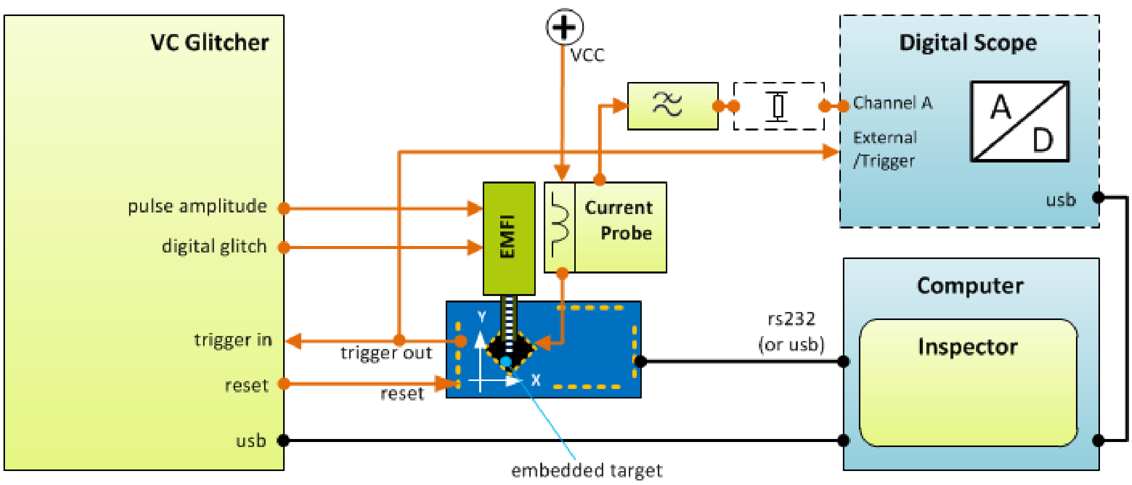


Figure 6 Setup for electromagnetic perturbation of an embedded target.

Connecting a typical setup

Preparation: Install Inspector first. This will also install the VC Glitcher USB drivers. (See Inspector manual for system requirements). Install the VC Glitcher SDK if you are developing or working without Inspector.

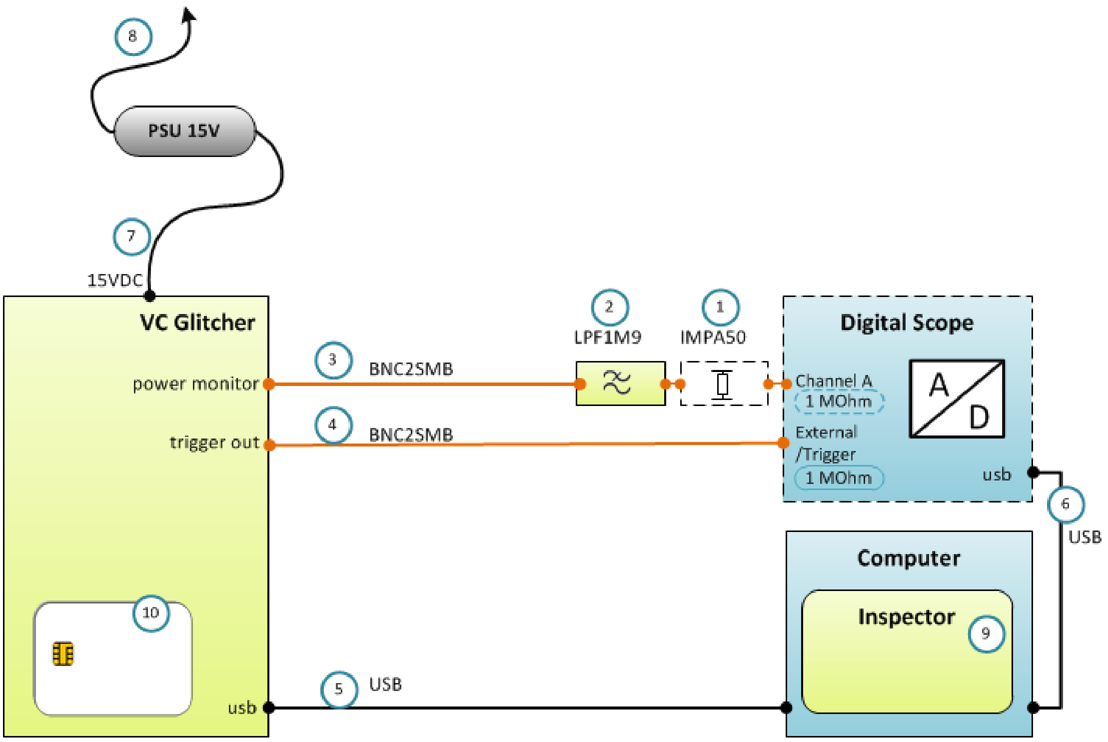


Figure 7 Order of connections for a typical VC Glitcher setup.

Take the following steps:

1. If the Channel A input impedance is 1 MΩ, add the impedance adapter IMPA50. Leave it out otherwise.
2. Connect filter LPF1M9 to the input channel (or IMPA50).
3. Connect **power monitor** of the VC Glitcher with a BNC2SMB cable to filter LPF1M9.
4. Connect **trigger out** of the VC Glitcher with a BNC2SMB cable to the **External** trigger channel.
5. Connect the VC Glitcher with a USB cable to the computer.
6. Connect the scope with a USB cable to the computer.

7. Plug the output of the PSU into the **15VDC** socket of VC Glitcher.
8. Plug the input of the PSU into a mains power socket.

▪ On the computer, Windows will detect the VC Glitcher and register it as plug and play USB device. Drivers will be installed if needed.

9. Start Inspector, if the application is not yet open.
   Inspector will recognize the VC Glitcher as a compound device.
   To verify this, select Tools >> Hardware Manager >>Devices >> Fragment glitcher, I/O devices, Raw I/O devices, VC Glitchers.

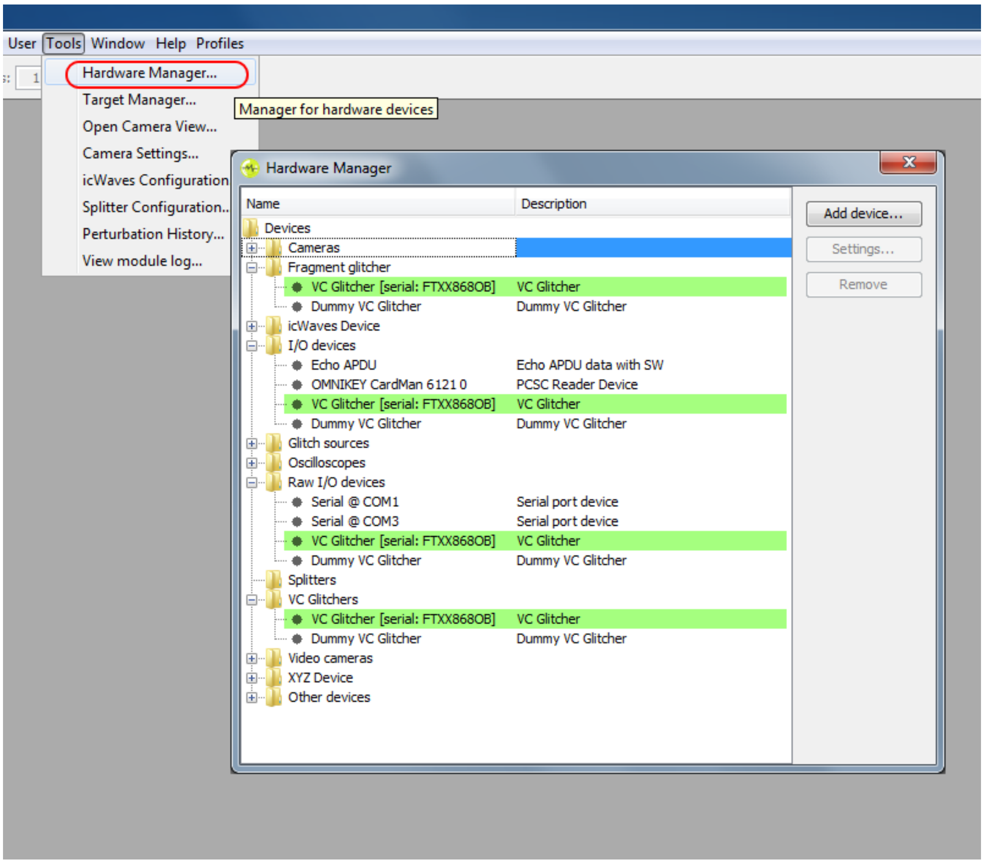


Figure 8 Highlighted references of device types registered for the VC Glitcher.

10. Insert a (training) smart card with contact pads forward and on bottom-side.

Your setup is now ready for configuring and executing perturbations!

A smart card can be safely inserted and removed while the VC Glitcher is powered.

Do not unplug the power or USB cable **while** the VC Glitcher is being initialized by Inspector.

When to apply an impedance adapter

Transfer of analog signals between devices are standardized using 50 Ω coax cables.

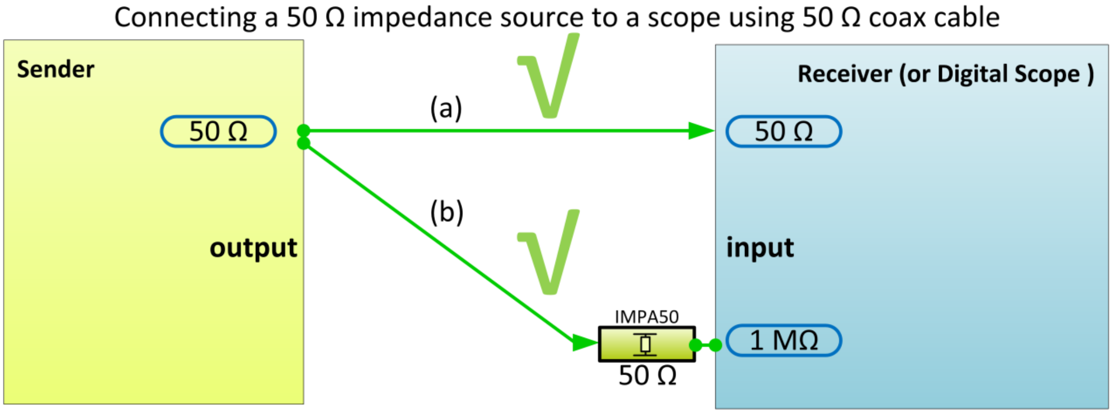


Figure 9 Connecting a 50 Ω source to a scope.

For the best quality of transfer, output and input must have a matching 50 Ω impedance (Figure 9, a). If the receiver only has a 1 MΩ input (Figure 9, b) and distortions or echoes aren't acceptable, then a 50 Ω impedance adapter must be prefixed to the input connector. Be aware that the received amplitude will now be **half of the sent amplitude**.

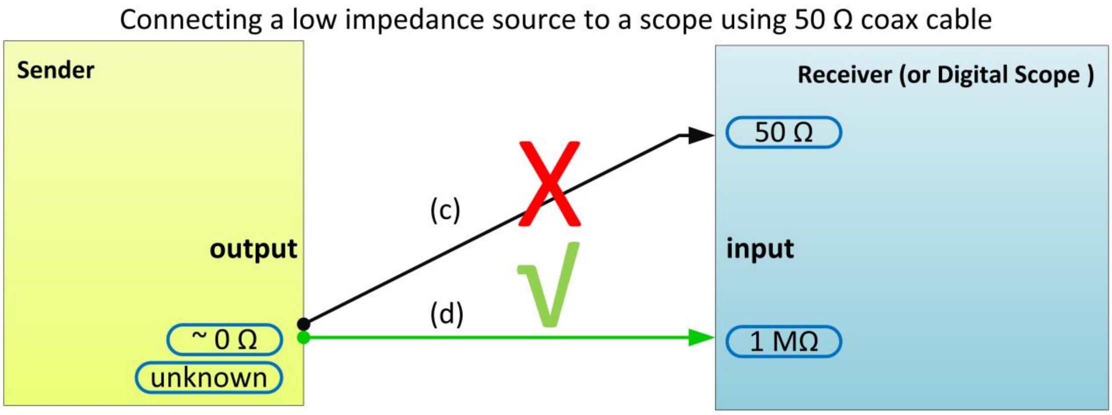


Figure 10 Connecting a low impedance source to a scope.

The 1 MΩ input is suitable for the accurate handling of rising/falling edges of digital signals.

Which low-pass filter to choose

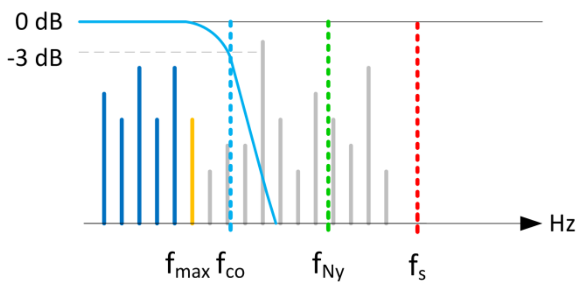
The goal of analog to digital conversion is a reliable representation of the measured analog signal. The quality of this representation is influenced by the sample rate and quantization precision.

The original signal can be reconstructed if the sample rate is at least **two times** the highest frequency present in the signal (Nyquist/Shannon-theorem).

Minimum and recommended sample rate

To speed up data analysis, the sample rate must be kept as low as possible. To be able to lower the sample rate, apply a low-pass filter. The filter removes unwanted high frequencies from the signal.

Physical low-pass filters however do not have an ideal cut-off characteristic. Sub-sampling artefacts will show up when the signal is sampled at the (theoretical) Nyquist rate. The recommended sample rate therefor is at least **four times** the LPF cut-off frequency.



f_{max} : highest frequency of interest
f_{co} : cut-off frequency of filter, $\leq f_{Ny}/2$
f_{Ny} : Nyquist frequency, $= f_S/2$
f_S : sampling frequency, $\geq 4\, f_{co}$

Choose combination f_{co}, f_s such that:
$f_{max} \leq f_{co} \leq f_S/4$

Figure 11 Balancing the filter cut-off frequency and the recommended sample rate.

Frequencies of interest are:

- The clock frequency of the central processor unit (CPU), usually defined by an internal clock.
- The clock frequency of crypto core(s), which could be different than those of the CPU.

Focus of interest	Clock frequency	Low-pass filter cut-off frequency (identifier)	Scope sample rate (recommended minimum).
Patterns in the overall operation, for example a crypto algorithm	1 MHz – 160 MHz	**1.9** MHz (LPF1M9) [1]	≥ 10 MSa/s
Details of a specific operation for example a crypto round	1 MHz – 40 MHz	**50** MHz (LPF50M) [2]	≥ 200 MSa/s
	40 MHz – 80 MHz	**90** MHz (LPF90M) [2]	≥ 400 MSa/s
	80 MHz – 160 MHz	**200** MHz (LPF200M) [2]	≥ 800 MSa/s

[1] There are cases you may desire to sample at a **lower rate** than the CPU clock frequency. This has consequences for the LPF. Use an LPF with a cut-off frequency ≤ ¼ of the desired sample rate!

[2] These filters are not supplied with the VC Glitcher.

How to verify your setup

To check whether your setup is correct, perform the next checks in order:

1. Is the VC Glitcher powered?
2. Is the VC Glitcher recognized by the computer?
3. Is the VC Glitcher responding to commands?

Please ensure that each step is successful, before proceeding to the next one. If not successful, refer to page 23 for solutions.

Check 1 - Is the VC Glitcher powered?

If the VC Glitcher is powered, the front LCD display lights up.

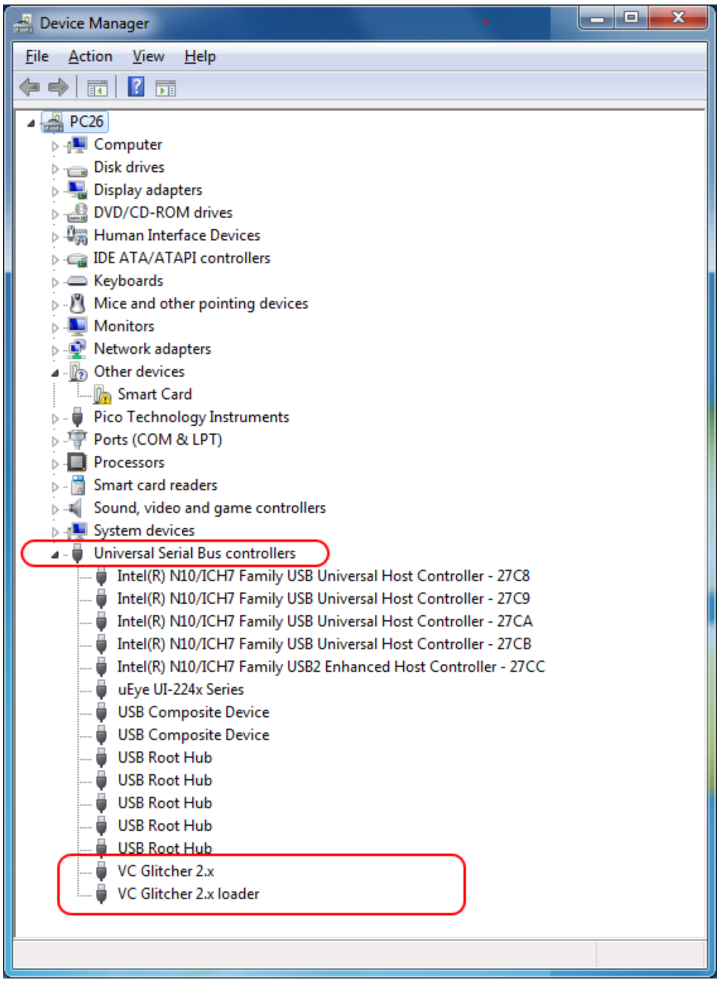
After power on, the LCD display shows a message with the VC Glitcher product version and copyright string.

Figure 12 Sample message after power on.

Check 2 - Is the VC Glitcher recognized?

1. To be recognized as plug and play product, the VC Glitcher device driver must have been registered with Windows. Driver registration is normally part of
   - the installation of Inspector;
   - the installation of the VC Glitcher SDK.
2. To verify VC Glitcher driver registration, follow the next steps
   - Open in Windows the Device Manager
   - Unfold category **Universal Serial Bus controllers**;

- Find driver entries with names starting with “VC Glitcher 2.x”.



Check 3 - Is the VC Glitcher responding to commands?

Preparation:

- Build the setup according to Figure 7.
- Insert training smart card **TC6**.

1. In Inspector, select **Perturbation** >> **Voltage/Clock** >> **Smart Card** >> **Protocol**.

   The SC Perturbation dialog opens.
2. Select tab **[General]**:
   - Set ‘Accept measurements with errors’ to **checked**;
   - Set ‘Limit errors’ to **unchecked**;

3. Select tab **[Measurement Setup]**:

   - From ‘Oscilloscope’ list, select **Sine Generator**;
   - Leave all other parameters as-is.

4. Select tab **[Glitch]**:

   - From ‘Glitcher’ list, select **VC Glitcher [*serial number*]**;
   - From ‘Glitch mode’ list, select **VCC**;
   - From ‘Clock speed’ list, select **1M** Hz;
   - Set ‘Number of Wait/Glitch sequences’ to **1**;
   - Set ‘Number of glitches per clock cycle’ to **1**.

5. Ignore settings in tab **[icWaves Setup]**.
6. Select tab **[Perturbation]**:

   - Set ‘Number of measurements’ to **Fixed**, **100**;
   - Set ‘Glitch voltage’ to **Fixed**, **-1.0** V;
   - Set ‘Vcc voltage’ to **Fixed**, **3.3** V;
   - Set ‘Clock high voltage’ to **Linked to VCC**;
   - Set ‘Clock low voltage’ to **Fixed**, **0** V;
   - Set ‘Wait cycles 1’ to **Fixed**, **After trigger**, and **1k** cycles
   - Set ‘Glitch cycles 1’ to **Fixed**, **10** cycles;
   - Set ‘Glitch offset 1’ to **Fixed**, and **20** cycles;
   - Set ‘Glitch length 1’ to **Fixed**, and **30** ns;

7. Select tab **[Target]**:

   - From ‘Protocol’ list, select **Training card 6** (as printed on the inserted card);
   - From ‘Data generator’ list, select **Fixed data**;
   - From ‘Trigger phase’ list, select **Crypto command**;
   - Set ‘Stop protocol after trigger’ to **unchecked**;
   - From Protocol settings ‘Algorithms’ list, select **DES**;
   - From ‘I/O device’ list, select **VC Glitcher [*serial number*]**;
   - Set ‘Low level communication logging’ to **checked**.

Summary of glitching settings:

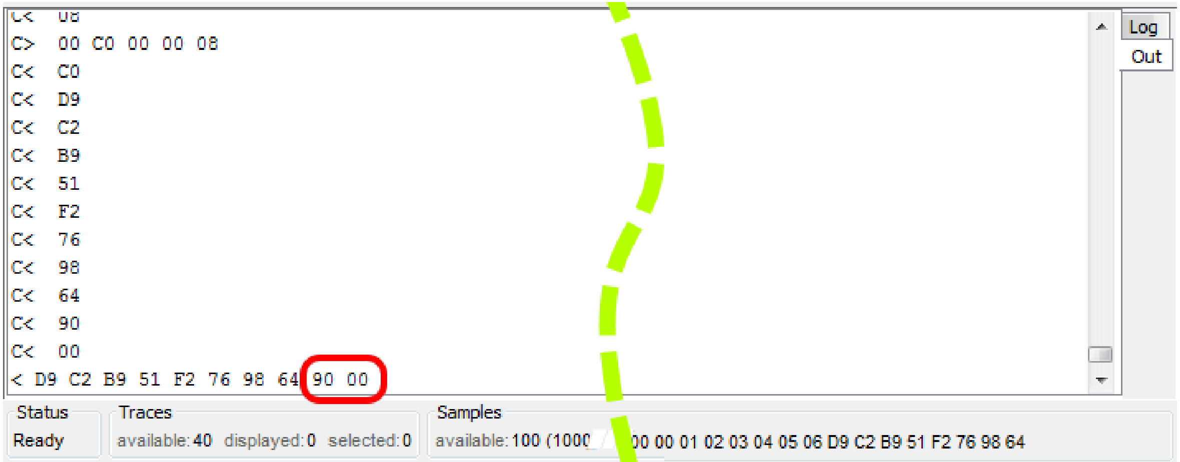
With the chosen card clock frequency of 1 MHz the perturbation program starts 1000 µs (= 1000 * 10^{-6} s/cycle) after receiving the trigger (training card 6 starts execution of crypto command). This program will fire in 10 consecutive clock cycles a 30 µs down-glitch of the Vcc with -1 V, each fired 20 ns after the rising edge of the card clock signal.

8. Press button ☑ to accept the values entered and close the dialog.
9. Inspector immediately starts the acquisition with sending a commands to the smart card. The acquisition is expected to complete within a few seconds.
10. A trace window opens and displays the simulated sine wave.
11. Observe panel **Out** at the bottom of the screen.

    The bytes exchanged with the smart card are listed as hexadecimal value pairs. Communication is indicated by direction arrows ">" (sent by Inspector) and "<" (received from smart card).

    Scroll down to the last line.

    The card should finish its response by sending bytes '**90 00**', indicating a successful completion of the command request.



How to control with custom applications

Setup for application development

Figure 13 Using the SDK to communicate with the VC Glitcher.

VC Glitcher SDK

Use the VC Glitcher Software Development Kit (SDK) if you want to communicate with the VC Glitcher in your own application.

The SDK is a software package containing code libraries that implement the VC Glitcher Application Programming Interface (API).

The API provides building blocks that enable your application to exchange data with the VC Glitcher and the smart card.

The SDK contains:

- Full documentation of the API;
- Header files and library files to be linked with your C/C++ source code;
- Python script files with examples of API usage;
- VC Glitcher USB device drivers.

The current Windows version supported by the SDK is Windows 7.

For more information, visit the Riscure Support Portal, https://support.riscure.com.

Help and troubleshooting

Common problems

Connecting USB cables	**First** connect the VC Glitcher with the USB cable to the computer, **then** power the VC Glitcher.
The LCD display shows full screen of white dots.	**CAUSE**: Occurrence of cable glitches when setting up the USB connection. **SOLUTION**: ▪ Unplug the PSU from the VC Glitcher. ▪ Re-seat the USB cable connectors ▪ Plug the PSU into the VC Glitcher.
Inspector - Module Execution Error: “CANNOT RUN MODULE <path>\ScopeAcquisition.class”	**CAUSE**: Card was inserted upside down. The acquisition module could not communicate with the card. **SOLUTION**: Re-insert the card with contact pads first and downwards.  *Figure 14 Correct insertion of a smart card*

VC Glitcher is not working. The display shows a full progress bar: 	**CAUSE:** The VC Glitcher has not been initialized correctly. This may happen when power or communication to the device is lost during the initialization. **SOLUTION**: The VC Glitcher needs to be re-initialized with factory settings. Please contact Riscure Support.

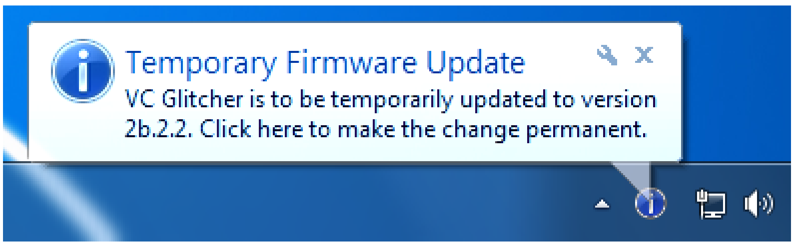
Interoperability issues

VC Glitcher 1.x	This generation of products is not capable of glitching embedded targets.

VC Glitcher initialization

Inspector tools and software are continuously improved. Newer Inspector versions expect certain parameters to be reported by old hardware too. This problem of backward compatibility is solved by a process called hardware initialization.

Consider the case when two or more versions of Inspector applications are open in Windows at the same time. Only one, the ‘active’ Inspector, is having the focus of user control. When this active Inspector is accessing a VC Glitcher for first use, its firmware will be temporarily updated by a process called ‘initialization’. Inspector requests the user to confirm the initialization and, unless explicitly making it permanent, the initialized state lasts until a power-off or a next initialization by one of the other Inspector applications. Windows notifies the user when an initialization process is ready to start.



An ongoing initialization process is visible on the LCD display by a progress bar, and usually takes only a few seconds to complete.

Do not unplug the power or USB cable while the VC Glitcher is being initialized!
An aborted initialization will corrupt the VC Glitcher and will make it inoperable.

Still have questions?

1. Go to the Inspector Help menu, and read detailed information on the VC Glitcher device.
2. Visit the Riscure Support Portal on the internet: https://support.riscure.com.

Technical specifications

Operational conditions

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

Do not block the ventilation holes of the VC Glitcher.
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 VC Glitcher is not required but recommended when not used for an extended period of time.

Power supply input

- 15 V DC
- Center-positive plug, inner-Ø 2.5 mm, outer-Ø 5.5 mm.

Use of a PSU other than supplied by Riscure is not supported.
Power spikes may cause internal damage and loss of accuracy.

Current measurement circuit

- Enabling general power consumption monitoring.
- Virtually zero-ohms for high bandwidth.
- Software configurable offset -30 .. 0 mA.
- Amplifier, low noise 26 pA / √Hz @ 100 kHz, high bandwidth -3 dB @ 1.5 GHz.

Internal logic

- Dedicated CPU (FPGA), 100 MHz

- 2 kB data memory (512 x 32 bits), smart card communication buffers and glitch parameters.
- 4 kB instruction memory (2k x 16 bits), glitch program.

Card power control

- Card power supply Vcc configurable 0.0 ... 6.6 V, default 3.3 V.

Card clock control

- Software configurable frequency 1 MHz, 2 MHz, 3 MHz or 4 MHz.
- Unsharpened square wave (low harmonics).
- High and low voltage level individually configurable 0.0 ... 6.6 V.

Glitch control

- One of three exclusive perturbation targets: VCC, CLK or OPT (external fault injector).
- Glitch amplitude programmable -7.4 V ... +4.2 V in 2 mV steps.
- Glitch width programmable 2 ns ... 2^{31} ns in 2 ns steps (for external glitch, minimum width 4 ns).

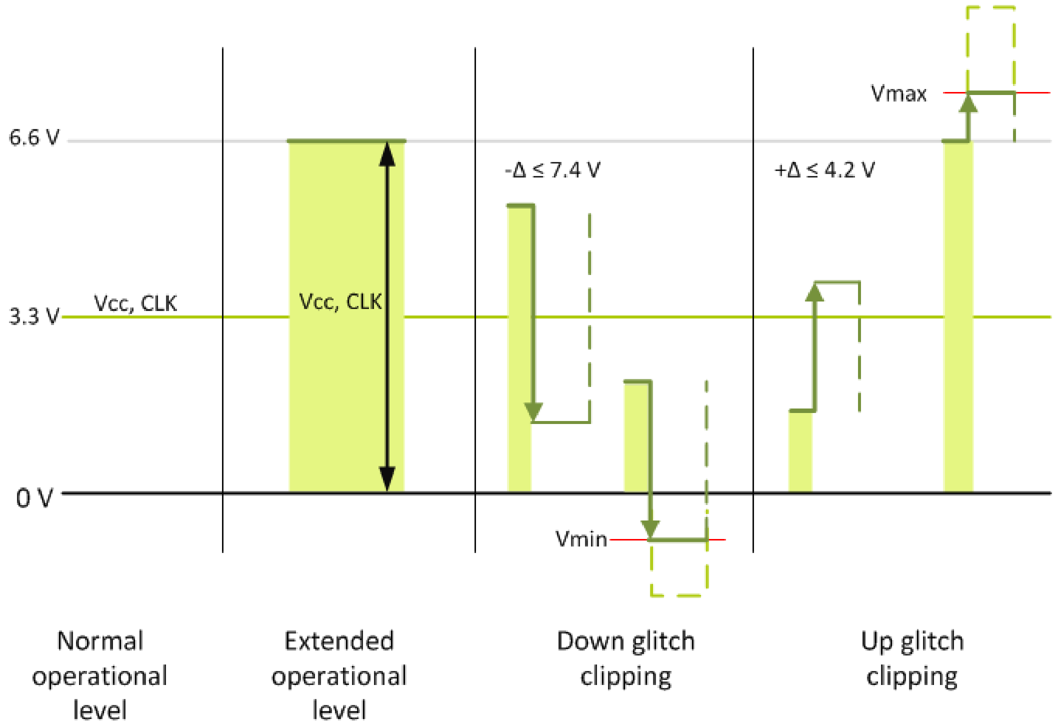


Figure 15 Operational voltage levels and the clipping of glitched signals.

Clipping level	Value	Condition (no card present)
VCC-glitching, Vmin	-1.00 V	@ VCC= 3.3 V, glitch= -7.4 V
VCC-glitching, Vmax	8.50 V	@ VCC= 6.6 V, glitch= +4.2 V
CLK-glitching, Vmin	-0.95 V	@ CLK-low= 3.3 V, glitch= -7.4 V
CLK-glitching, Vmax	8.00 V	@ CLK-high= 6.6 V, glitch= +4.2 V

Table 1 Hardware determined clipping levels measured in the unloaded case (no card present).

Product case

- Dimensions: 220.00 x 169.50 x 34.63 [mm], 8.661 x 6.673 x 1.363 [inch] (L x W x H).

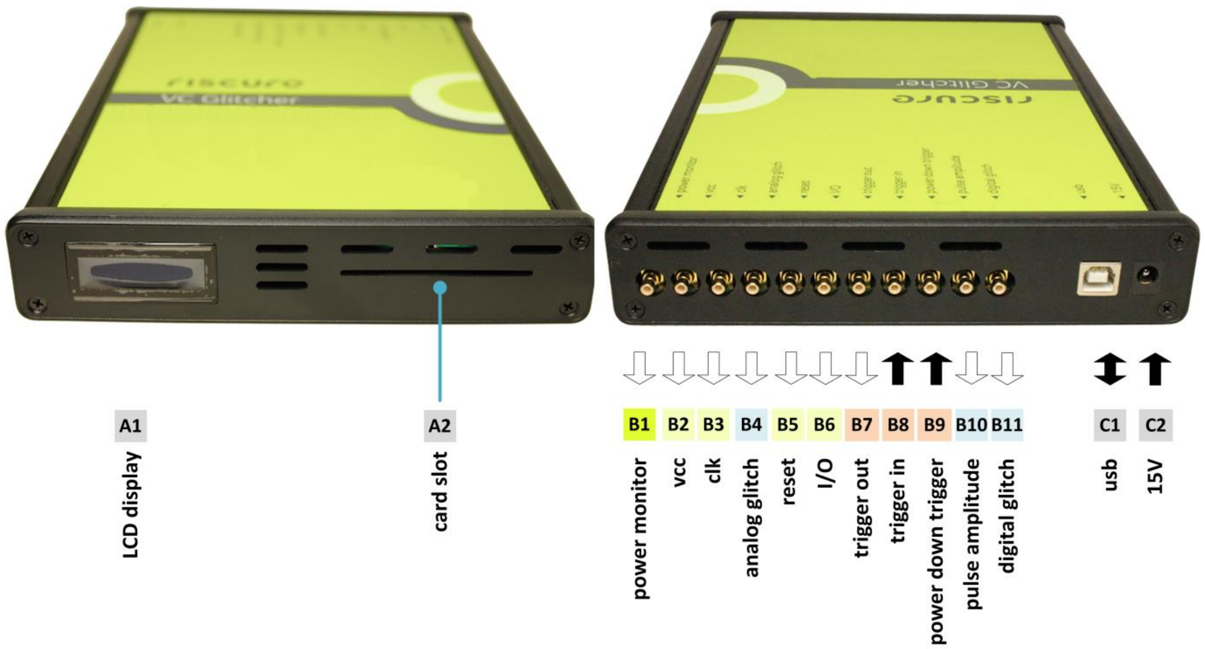


Table 2 Details of interfaces and functions.

Port	Label	Description
A1	-	LCD Display with two character rows
A2	-	Smart card slot
B1	**power monitor**	Signal proportional to the power consumption of the smart card.
B2	**vcc**	SMB. Buffered output. Linear signal (-1.0 ... 8.5 V) Duplicate of smart card pad VCC signal (glitches included).
B3	**clk**	SMB. Buffered output. Linear signal (-0.95 ... 8.0 V) Duplicate of smart card pad CLK signal (glitches included).
B4	**analog glitch** [1]	SMB. Buffered output. Linear signal (-1.0 ... 8.5 V) for an external fault injector combining pulse amplitude and digital glitch.

Port	Label	Description
B5	**reset**	SMB. Buffered output. Duplicate of smart card pad RST signal.
B6	**I/O**	SMB. Buffered output. Duplicate of smart card pad I/O signal.
B7	**trigger out**	SMB. Buffered TTL output. Binary timing reference signal for external hardware. A rising edge signals the completion of a command transfer to the smart card. This port is usually connected to the trigger port of an oscilloscope.
B8	**trigger in**	SMB. CMOS level input. Binary timing reference signal from an external source. The VC Glitcher can use the rising/falling edge to start execution of a perturbation program.
B9	**power down trigger** [2]	SMB. CMOS level input. Binary warning signal from an external source. The VC Glitcher can use the rising/falling edge to stop all interaction with the target immediately.
B10	**pulse amplitude**	SMB. Buffered output. Linear signal (0.0 ... 3.3 V) for an external fault injector defining the glitch amplitude: 0 V = 0% power, 3.3 V= 100% power.
B11	**digital glitch**	SMB. Buffered output. Binary switch signal for an external fault injector to activate the glitch while the signal level is high (≥ 2.4 V).
C1	**usb**	USB 2.0 port. Type USB-B. Communication link with a computer.
C2	**15V**	15 V DC. Power supply input.

[1] This is a legacy device signal. Transient effects, especially overshoot, make it not appropriate for controlling perturbance power. External fault injectors must be controlled exclusively by the **pulse amplitude** and **digital glitch** signals.

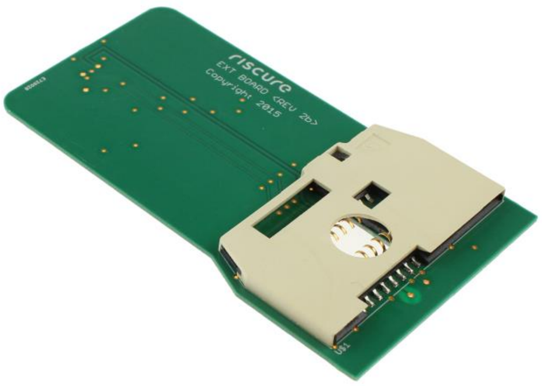
[2] The power down trigger (PDT) is used to prevent the target from getting into a state where it would trigger certain countermeasures e.g. wipe keys or apply

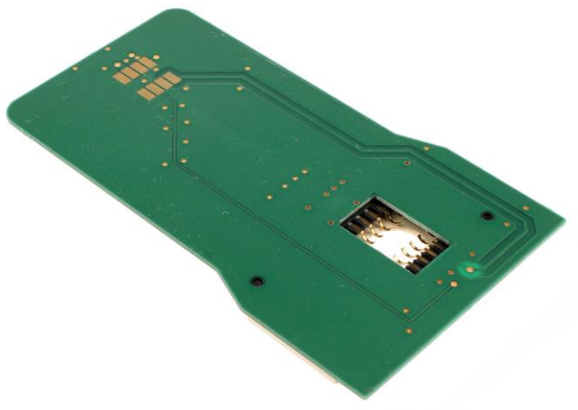
damage to itself. A PDT signal can be produced by a pattern recognition device e.g. icWaves from Riscure.

Figure 16 Top view of the VC Glitcher

Extension board

The VC Glitcher comes with a smart card extension board (thickness 0.8 mm). This board can carry the smart card and can be inserted into the card slot. The board enables (EM) probing experiments which require physical access to the smart card.





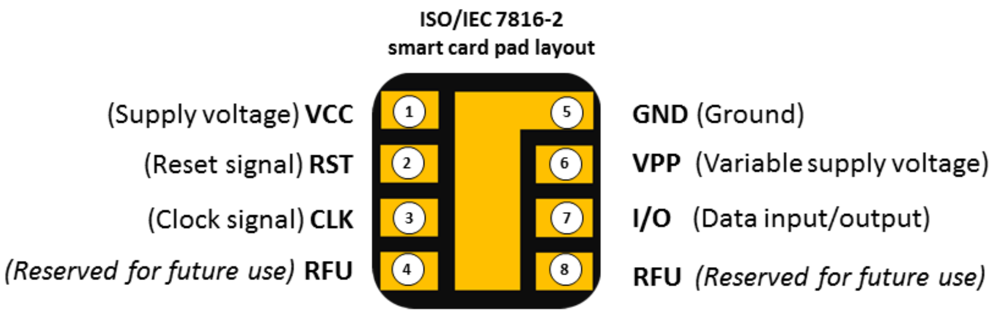


Figure 17 Numbering and function of smart card pads.

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)

VC Glitcher

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-VC Glitcher.

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

F. de Beer

Signature of representative

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