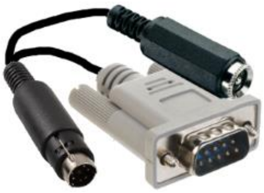
Power Tracer

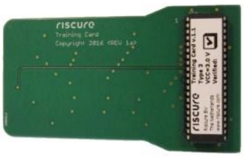
Quick Start Guide

What is in the box

The box contains the Power Tracer and all accessories to connect it to a computer and an oscilloscope.

Box content checklist

Quantity	Description	Photo	Identifier (*)
1	Power Tracer 4		
1	Power Supply Unit 15 V DC - input 100 V to 240 V AC, 50 .. 60 Hz		PSU
	Power cable (included with PSU)	 Country specific	
2	Signal cable: - BNC to BNC, 50 Ω, coaxial		BNC50
1	Proprietary split cable: - PS2 to RS232/Probe-power.		PS2PRB
1	Communication cable: - USB, USB-A to USB-B		USB

Quantity	Description	Photo	Identifier (*)
1	Low-pass filter: - 50MHz, 50 Ω, BNC male-to-female		LPF50
1	Low-pass filter: - 90MHz, 50 Ω, BNC male-to-female		LPF90
1	Impedance adapter: - 50 Ω, BNC to BNC		IMPA50
1	Smart card for training purpose: - 3DES in software		TC2
1	Smart card for training purpose: - AES in software		TC3
1	Smart card for training purpose: - ECC in software+ DES in hardware		TC8
1	Extension card		
	This “Power Tracer - Quick Start Guide”		

(*) Identifiers are used in references in this document.

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 does it do

The Power Tracer is a plug and play smart card reader with Side Channel Analysis (SCA) capabilities. It can measure the power consumption of the smart card with a high sensivity.

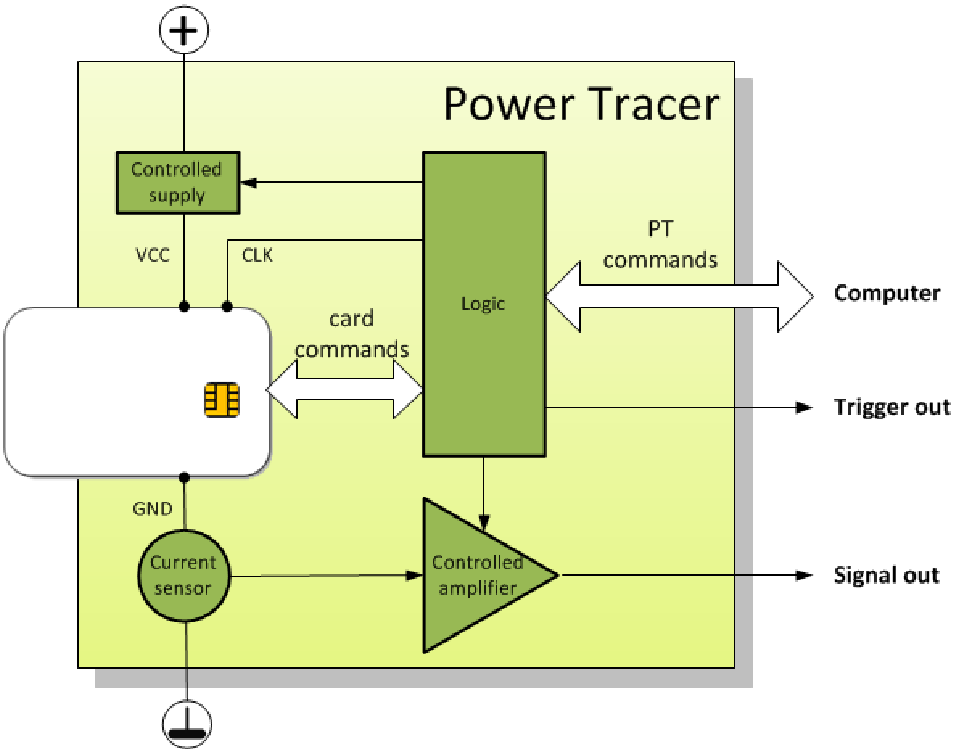


Figure 1 Functional overview of the Power Tracer.

The Power Tracer produces a trigger out signal when the smart card is going to execute a command. This signal is useful for synchronization of other measurement devices.

The Power Tracer enables the tuning of the card’s power supply, the card’s clock frequency, and the offset and gain of the current amplifier.

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

How to build a setup

Typical setup with a digital storage scope

In this setup the power consumption of the smart card, when it is executing a cryptographic command, is measured and digitized by the digital oscilloscope.

After a trigger out event, the scope records a configured number of samples into a trace. Inspector retrieves and stores these traces.

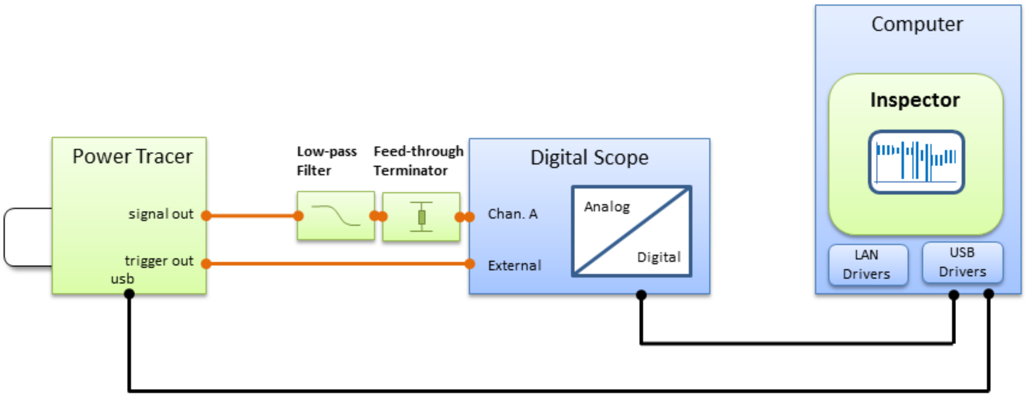


Figure 2 Power Tracer setup with a digital storage scope.

How to connect a typical setup

Preparation: Install the Inspector application (or the Power Tracer SDK) to provide for the Power Tracer USB drivers.

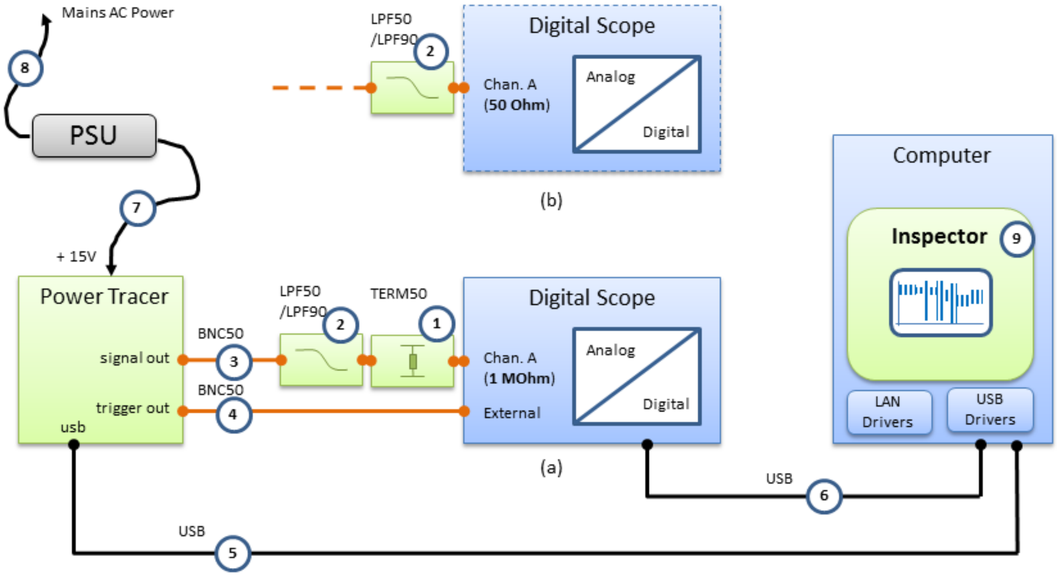


Figure 3 Step-wise connecting a setup with the Power Tracer.

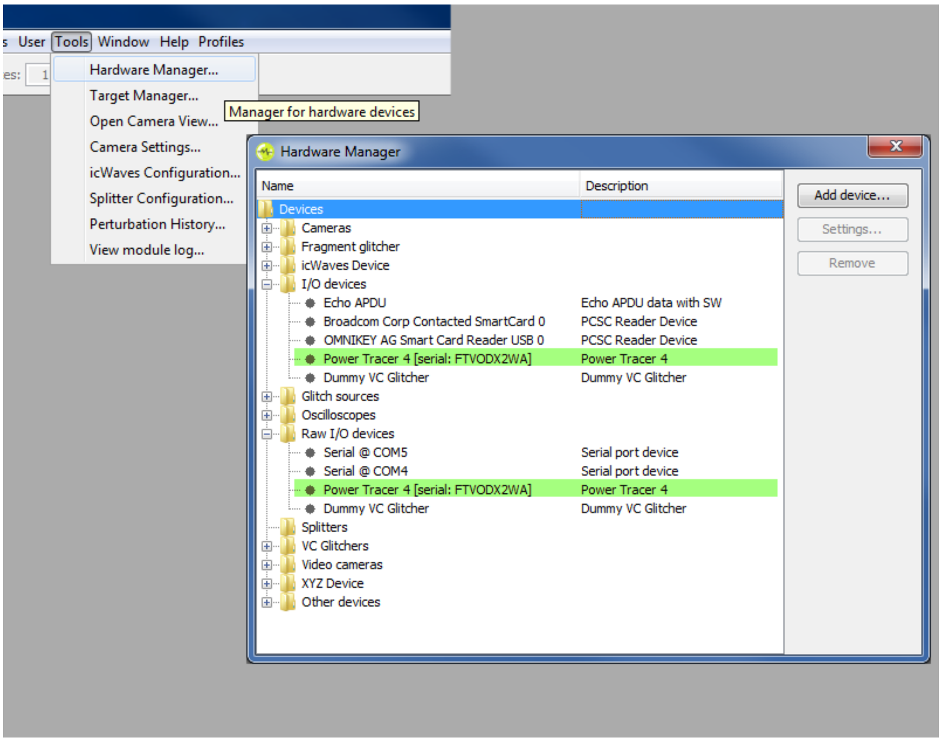
Take the following steps:

- (1) Connect the adapter **IMPA50**, if needed, to Channel A of the scope (For guidance, see next section).
- (2) Choose a low-pass filter **LPF50** or **LPF90** and connect it to the **IMPA50** (For guidance, see next section).
- (3) Connect **signal out** of the Power Tracer with a BNC50 cable to the LPF.
- (4) Connect **trigger out** of the Power Tracer with a BNC50 cable to the **External** trigger channel of the scope.
- (5) Connect **usb** of the Power Tracer with the USB cable to the computer.
- (6) Connect the scope with the USB cable to the computer.
- (7) Insert the power supply plug of the PSU into the **+15V** port of the Power Tracer.
- (8) Plug the PSU into a mains power wall socket.

- On the computer, the Power Tracer is detected and registered as plug and play device. Drivers will be installed if needed.
- (9) Inspector will automatically record the Power Tracer as I/O device. Verify the presence of the Power Tracer in the hardware manager
  Select Tools >> Hardware Manager,

  See branch **I/O Devices.**

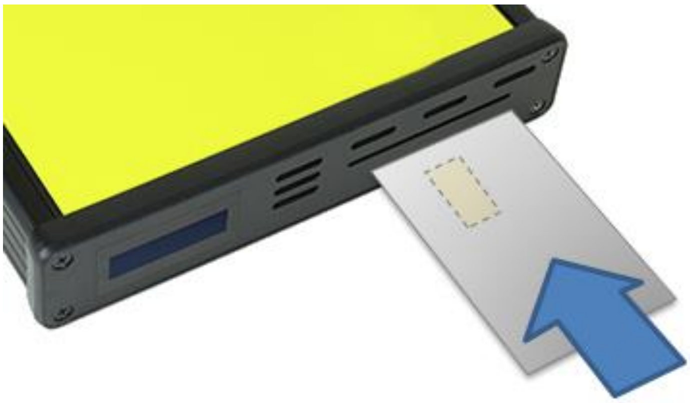
  See branch **Raw I/O Devices.**



Name	Description
Devices	
Cameras	
Fragment glitcher	
icWaves Device	
I/O devices	
Echo APDU	Echo APDU data with SW
Broadcom Corp Contacted SmartCard 0	PCSC Reader Device
OMNIKEY AG Smart Card Reader USB 0	PCSC Reader Device
Power Tracer 4 [serial: FTVODX2WA]	Power Tracer 4
Dummy VC Glitcher	Dummy VC Glitcher
Glitch sources	
Oscilloscopes	
Raw I/O devices	
Serial @ COM5	Serial port device
Serial @ COM4	Serial port device
Power Tracer 4 [serial: FTVODX2WA]	Power Tracer 4
Dummy VC Glitcher	Dummy VC Glitcher
Splitters	
VC Glitchers	
Video cameras	
XYZ Device	
Other devices	

Figure 4 The Power Tracer 4 registered in the Hardware Manager.

- Insert a training card (or your own smart card).



The Power Tracer display message changes from “NO CARD INSERTED” to “CARD NOT POWERED”.

Your setup is now ready for measurement!

ℹ A smart card can be safely inserted and removed when the Power Tracer is powered.

⚠ Do not unplug the power or USB cable while the Power Tracer is being initialized by Inspector.

When to apply an impedance adapter?

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

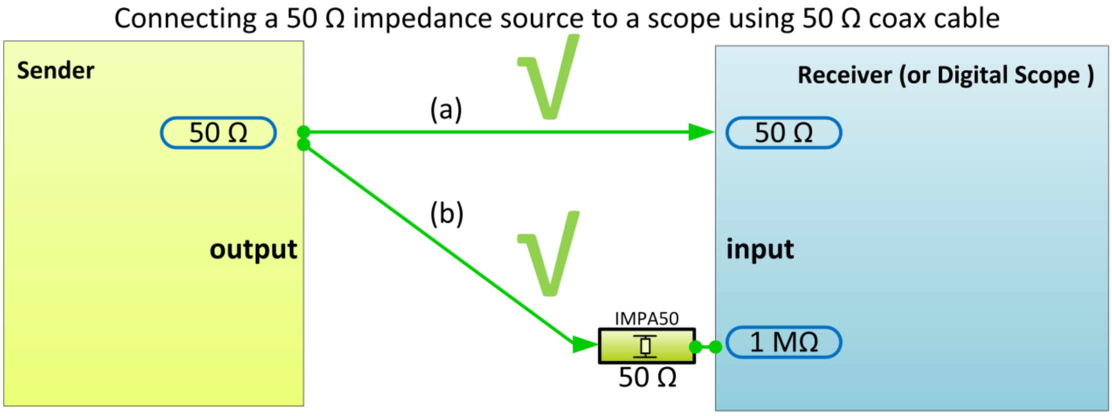

Connecting a 50 Ω impedance source to a scope using 50 Ω coax cable
Sender
50 Ω
output
(a)
√
(b)
√
IMPA50
50 Ω
Receiver (or Digital Scope)
50 Ω
input
1 MΩ

Figure 5 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 5, a). If the receiver only has a 1 MΩ input (Figure 5, b) and distortions or echos 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**.

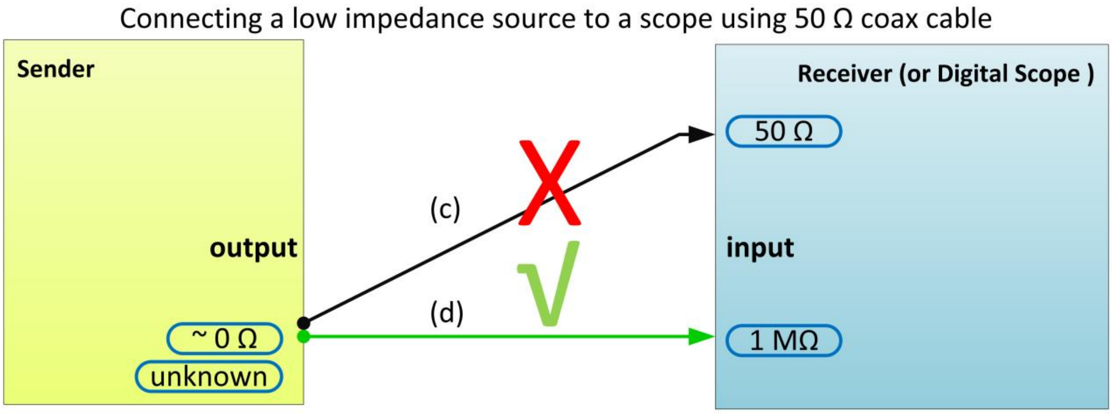

Connecting a low impedance source to a scope using 50 Ω coax cable
Sender
output
~ 0 Ω
unknown
(c)
X
(d)
√
Receiver (or Digital Scope)
50 Ω
input
1 MΩ

Figure 6 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?

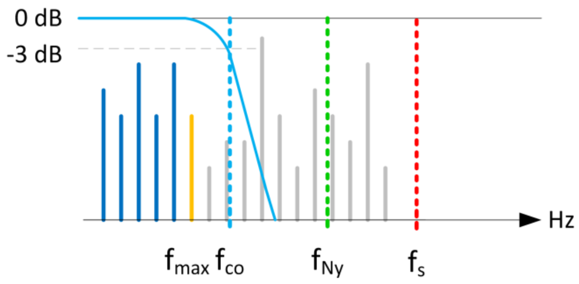
The goal of analog to digital conversion is a reliable representation of the measured analog signal. The quality of this representation is influenced by the sample rate and quantization precision.

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 7 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.

Table 1 Recommended combinations of low-pass filter and sample rate.

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][2]	≥ 10 MSa/s
Details of a specific operation for example a crypto round	1 MHz – 40 MHz	**50** MHz (LPF50M)	≥ 200 MSa/s
	40 MHz – 80 MHz	**90** MHz (LPF90M)	≥ 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 Power Tracer.

How to verify your setup

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

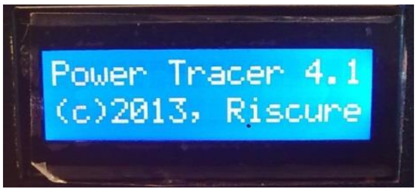
1. Is the Power Tracer powered?
2. Is the Power Tracer recognized by the computer?
3. Is the Power Tracer responding to commands?

Please ensure that each procedure is successful, before proceeding to the next one. If not successful, refer to page 18 for a solution.

1 - Is the Power Tracer powered?

If the Power Tracer is powered, the front display lights up.

After power on, the display shows a message with the Power Tracer version and a copyright string.



```
Power Tracer 4.1
(c)2013, Riscure
```

Figure 8 Initial Power Tracer display after power on.

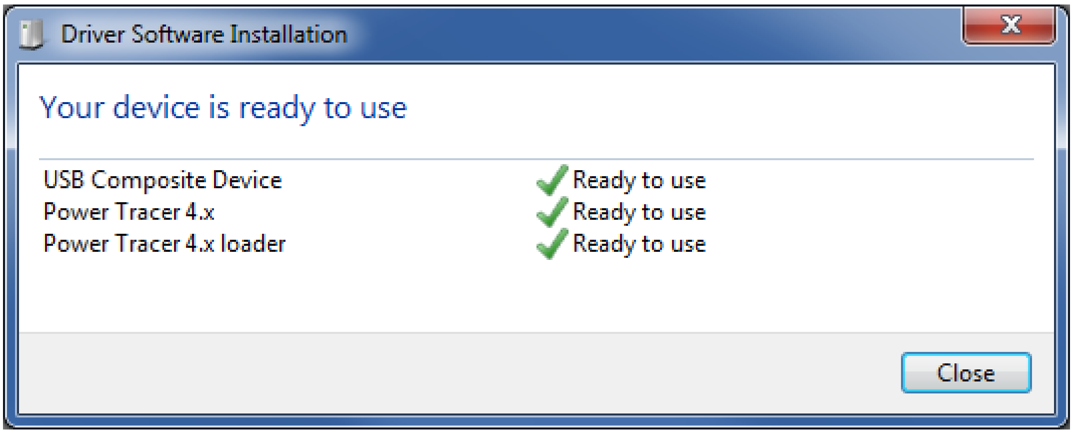
After establishing communication with Inspector (and no card inserted), the displayed message changes to:
“NO CARD INSERTED”.

When a card is inserted, the displayed message changes to:
“CARD NOT POWERED”

When the card is removed, the displayed message changes to:
“CARD NOT INSERTED”

2 - Is the Power Tracer recognized?

1. To control the Power Tracer from a computer, it must be recognized as a USB device. The device driver for the Power Tracer is included in the installation of the Inspector application and is available for Windows only.
2. Windows will automatically recognize the Power Tracer when it is plugged into a USB port.



Driver Software Installation

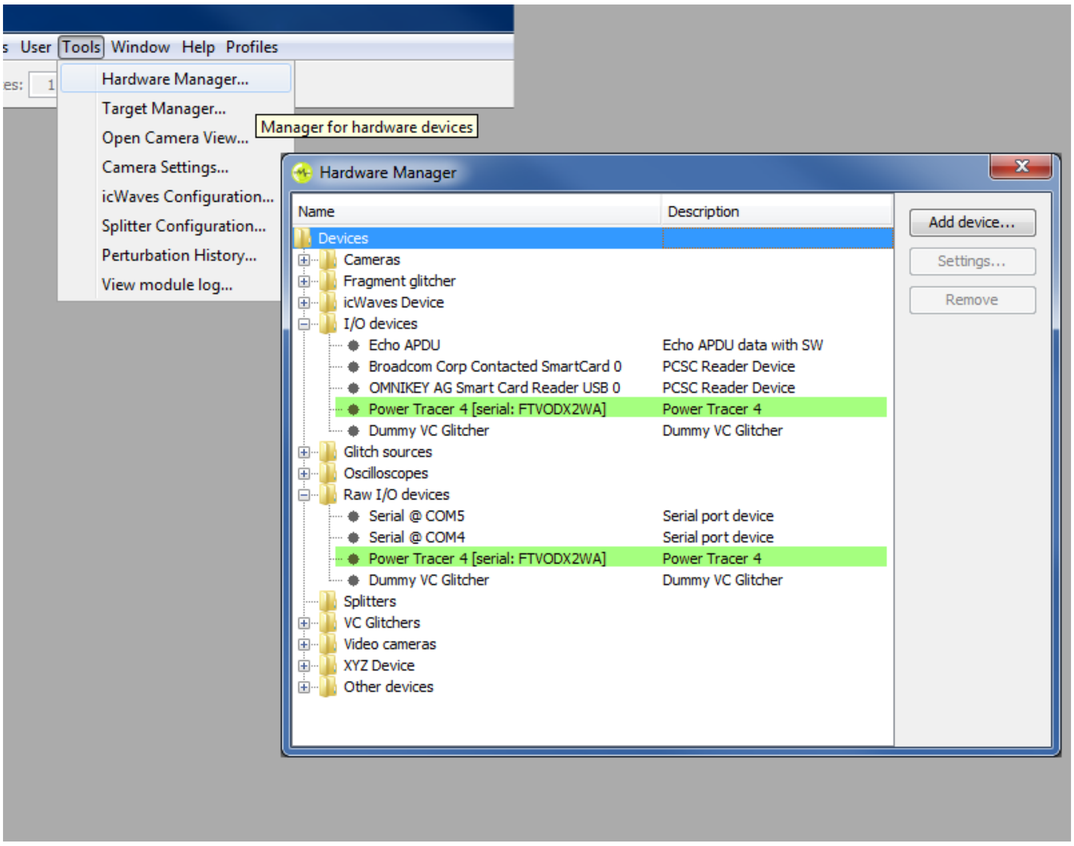
Your device is ready to use

USB Composite Device ✓ Ready to use
Power Tracer 4.x ✓ Ready to use
Power Tracer 4.x loader ✓ Ready to use

Figure 9 Automatically installing the USB device driver for the Power Tracer 4.

3. At startup, Inspector searches for available Power Tracer devices and lists them in the Hardware manager.
   To open the Hardware Manager:

select Tools >> Hardware Manager



Name	Description
Devices	
Cameras	
Fragment glitcher	
icWaves Device	
I/O devices	
Echo APDU	Echo APDU data with SW
Broadcom Corp Contacted SmartCard 0	PCSC Reader Device
OMNIKEY AG Smart Card Reader USB 0	PCSC Reader Device
Power Tracer 4 [serial: FTVODX2WA]	Power Tracer 4
Dummy VC Glitcher	Dummy VC Glitcher
Glitch sources	
Oscilloscopes	
Raw I/O devices	
Serial @ COM5	Serial port device
Serial @ COM4	Serial port device
Power Tracer 4 [serial: FTVODX2WA]	Power Tracer 4
Dummy VC Glitcher	Dummy VC Glitcher
Splitters	
VC Glitchers	
Video cameras	
XYZ Device	
Other devices	

3- Is the Power Tracer responding to commands?

Preparation: Insert training smart card **TC8** into the Power Tracer, with the contact pads down.

1. In Inspector, select Acquisition >> Scope – Protocol.

   The Scope Acquisition dialog opens.

2. Select tab **[General]**

   - enter **10** in ‘Number of measurements’
   - mark checkbox ‘Accept measurements with errors’
   - unmark checkbox ‘Limit errors’

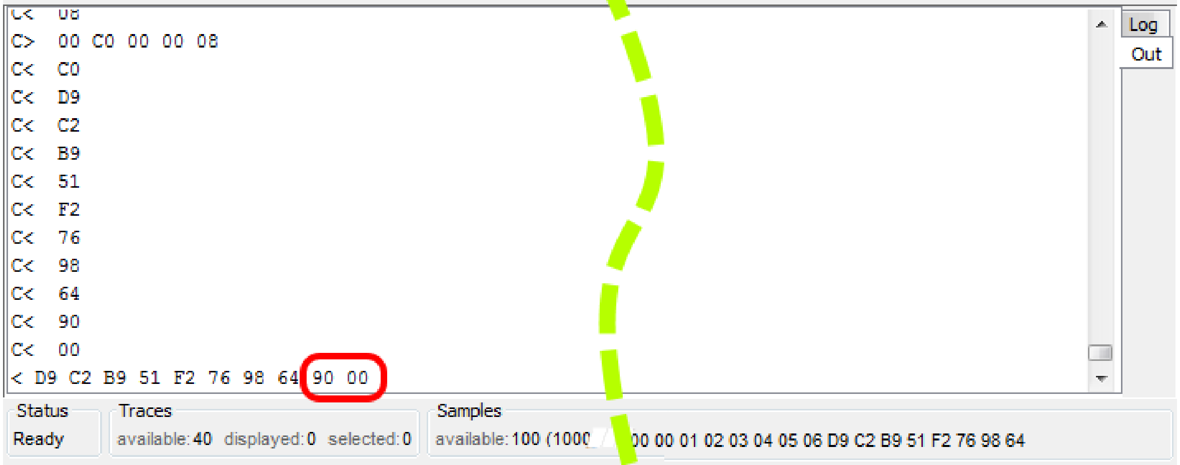
3. Select tab **[Measurement Setup]**:

   - from Oscilloscope list, select **Sine Generator**.

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

- from Protocol list, select **Training card 8** (choose id of inserted smart card)
- from Trigger phase list, select **Crypto command**
- unmark checkbox ‘Stop protocol after trigger’
- in Protocol settings, from Algorithms-list, select **DES**.
- in I/O device list, select **Power Tracer 4**
- mark checkbox ‘Use low noise power supply’
- mark checkbox ‘Low level communication logging’

5. Press button ☑ accept the values entered and to close the dialog.
6. Inspector starts the acquisition by exchanging data with the Power Tracer and with the smart card. The acquisition will complete within a few seconds.
7. A trace window opens and displays the simulated sine wave.
8. Observe the **Out panel** 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 with bytes ‘**90 00**’, indicating a successful completion.



```
C<  08
C>  00 C0 00 00 08
C<  C0
C<  D9
C<  C2
C<  B9
C<  51
C<  F2
C<  76
C<  98
C<  64
C<  90
C<  00
< D9 C2 B9 51 F2 76 98 64 90 00
```

Status: Ready

Traces: available: 40 displayed: 0 selected: 0

Samples: available: 100 (1000 … 00 00 01 02 03 04 05 06 D9 C2 B9 51 F2 76 98 64

How to control with custom applications

Setup for application development

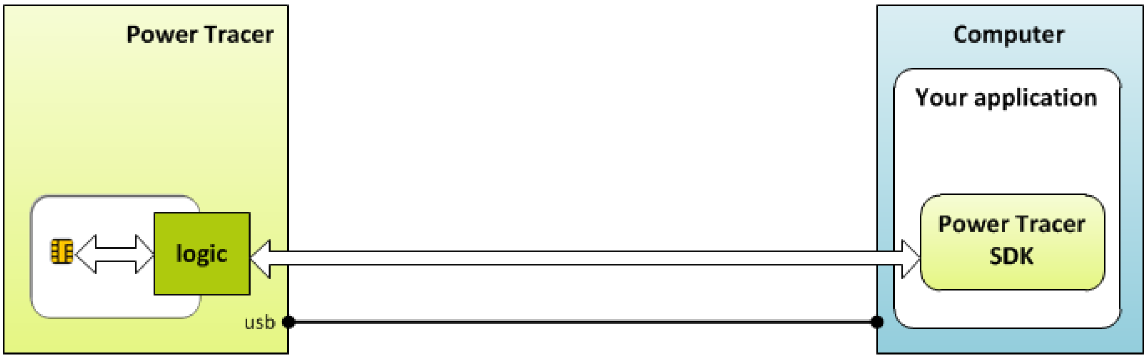


Figure 10 Using the SDK to communicate with the Power Tracer.

Power Tracer SDK

A software development kit (SDK) is available to build custom applications for the Power Tracer. This SDK implements the Power Tracer application programmer interface (API) and enables you to exchange data with the Power Tracer and the smart card.

The SDK contains:

- Header and library files to be linked with your C/C++ source code;
- Documentation on the API;
- USB drivers for the Power Tracer;
- Example python script files on how to use the API and verify the Power Tracer connection.

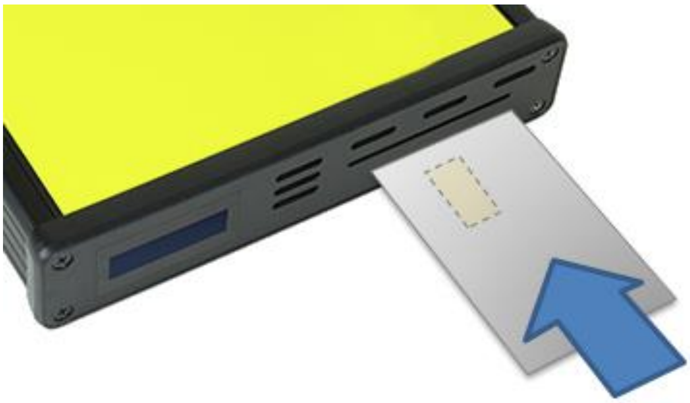
Current Windows version supported by the SDK is Windows 7.

For more information, visit Riscure Support (http://support.riscure.com).

Help and troubleshooting

Common problems

ℹ Order of connecting a USB cable	**First** fully connect the USB cable with the computer at both ends, **then** power the Power Tracer.
The Power Tracer LCD display shows a full screen of white dots.	**CAUSE**: Occasional glitches have occurred when setting up the USB connection. **SOLUTION**: ▪ Unplug the PSU from the Power Tracer. ▪ Re-insert the USB connector ▪ Reconnect the PSU to the Power Tracer.
The Power Tracer LCD displayed shows: "NO CARD INSERTED".	**CAUSE 1**: No smart card present. **SOLUTION**: Insert a smart card. **CAUSE 2**: Smart card inserted wrong. **SOLUTION**: Insert smart card with contact pads down. **CAUSE 3**: Smart card is not fully inserted. **SOLUTION**: Gently push smart card until blocked.
The Power Tracer LCD displayed shows: "CARD NOT POWERED",	**CAUSE**: This is not a problem, but reflects the status when no command is sent to the card. The card will be powered when measurements starts from Inspector.

Inspector - Module Execution Error: “CANNOT RUN MODULE <path>\ScopeAcquisition.class”	**CAUSE**: The acquisition module could not establish communication because card is inserted upside down. **SOLUTION**: Re -insert it with contact pads down.  *Figure 11 Correct orientation to insert a smart card*
Power Tracer is not working. The Power Tracer LCD display shows a full progress bar: 	**CAUSE:** The Power Tracer is not successfully initialized. This may happen when power or communication to the device was lost during the initialization. **SOLUTION**: The Power Tracer needs to be re-initialized with factory settings. Please visit http://support.riscure.com.

Interoperability issues

Inspector 4.6 only	An update is required for the Power Tracer 4 SDK.

Power Tracer initialization

Inspector tools and software are continuously improved. On your Windows desktop there can be different versions of Inspector applications open at the same time, but only one is the ‘active’ application having the focus of user control.

To maintain interoperability, the ‘active’ Inspector will temporarily initialize the Power Tracer when it is selected as I/O device for first use. This initialization state is lost after a power-off or after a re-initialization of the Power Tracer. An ongoing initialization is visible by a progress bar on the Power Tracer display, and usually takes a few seconds.

⚠ Please do not unplug the power or USB cable when the Power Tracer is being initialized! An aborted initialization will corrupt the Power Tracer and make it inoperable.

Still have questions?

1. Go to the Inspector Help menu, and read detailed information about the Power Tracer device.
2. 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 Power Tracer. A blocked air flow may cause malfunction or break down.

ℹ Maintain a stable and identical environment in order to reliably repeat tests.

ℹ Unplugging the PSU from the Power Tracer is not required but recommended when not used for an extended time.

Power supply input

- 15 V DC, max 800 mA
- 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.

Clock generation for smart card

- Software adjustable [1 .. 10 MHz], default 4 MHz.
- Unsharpened square wave (low harmonics), buffered.

Current measurement circuit

- Amplifier, low noise (26 pA / √Hz @ 1 MHz), high bandwidth (-3 dB @ 1.5 GHz).
- Virtually zero-ohms for high bandwidth.
- Isolated electrically from digital control circuit for low-noise signal.

- Fed by capacitors during measurement for low-noise signal.
- Software configurable gain 100 % .. 200 %.
- Software configurable offset 0 .. -30 mA.
- Software configurable smart card voltage 1.8 .. 6.0 V.

USB connector:

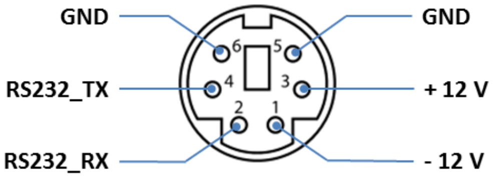
- USB 2.0, type USB-B, connection to PC.

BNC output connectors:

- **trigger out**, TTL-level triggering, 1 µs trigger delay resolution, active rising edge, pulse duration ~10 µs, trigger generated at completion of request block transfer to smart card.
- **clock out**, buffered TTL output, square wave oscillator, synchronous to smart card clock.
- **reset out**, buffered TTL output, the signal from smart card reset pad.
- **IO out**, buffered TTL output, the signal from smart card IO pad.
- **signal out**, impedance 50 Ω, buffered output, the analog signal proportional to smart card power consumption.
- Output range ± 4V for 1MΩ oscilloscope input impedance.
- Output range ± 2V for 50Ω oscilloscope input impedance.

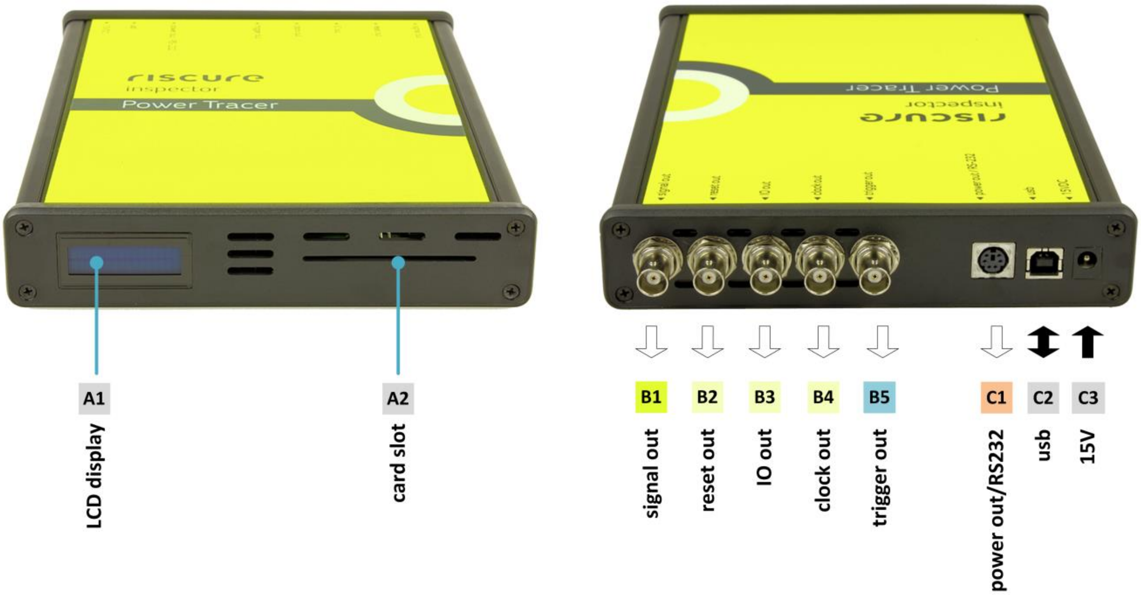
Power/RS232:

- Proprietary use of PS/2 connector to support probe hardware.



Product case

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

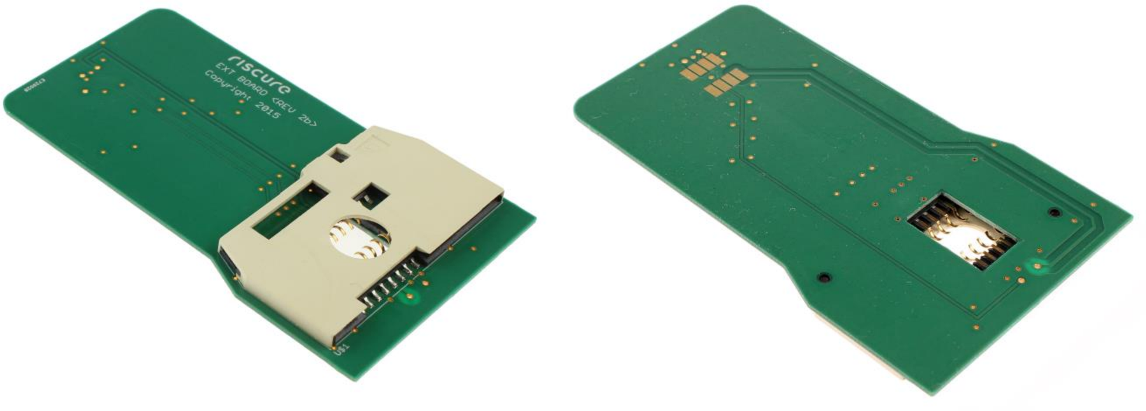


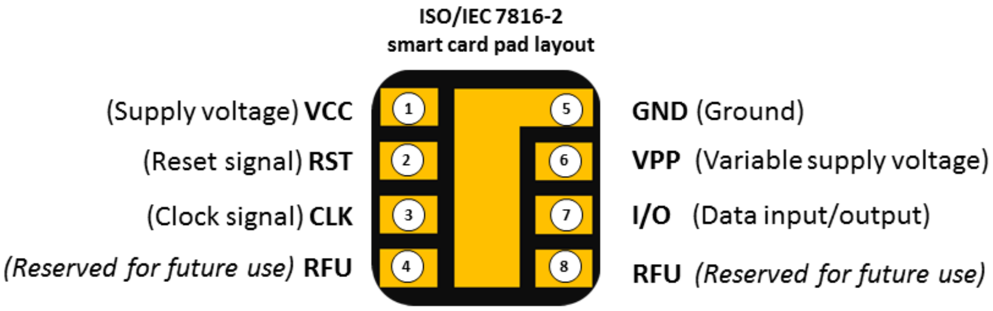
Port	Label	Description
A1	-	LCD display, 2 lines of text for messages.
A2	-	Smart card slot.
B1	**signal out**	BNC, Buffered output. Power consumption read-out. Usually connected to a channel on a digital storage scope.
B2	**reset out**	BNC, Buffered output. Duplicated signal from smart card pad 2. Optionally connected to a channel on a scope for preview.
B3	**IO out**	BNC, Buffered output. Duplicated signal from smart card pad 7. Optionally connected to a channel on a scope for preview.
B4	**clock out**	BNC, Buffered output. Duplicated signal from smart card pad 3. Optionally connected to a channel on a scope for preview.

Port	Label	Description
B5	**trigger out**	BNC, Buffered output. Configurable synchronization signal. Usually connected to a trigger port on a digital storage scope.
C1	**power out / RS-232**	PS2. Proprietary port for probe hardware.
C2	**usb**	Control connection with computer.
C3	**15VDC**	Power supply in.

Extension board

The Power Tracer 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.





Legacy interface

For backward compatibility, the Power Tracer has a PS2 port with proprietary wiring for attaching a 12 V probe power supply and a serial communication connection.

The Power Tracer can pass commands from USB port to the target on the RS-232 port.

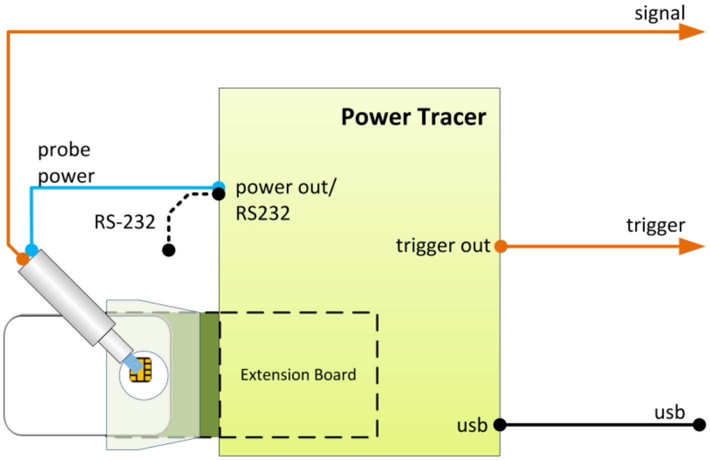


Figure 12 Probing a smartcard while not using the RS232 interface.

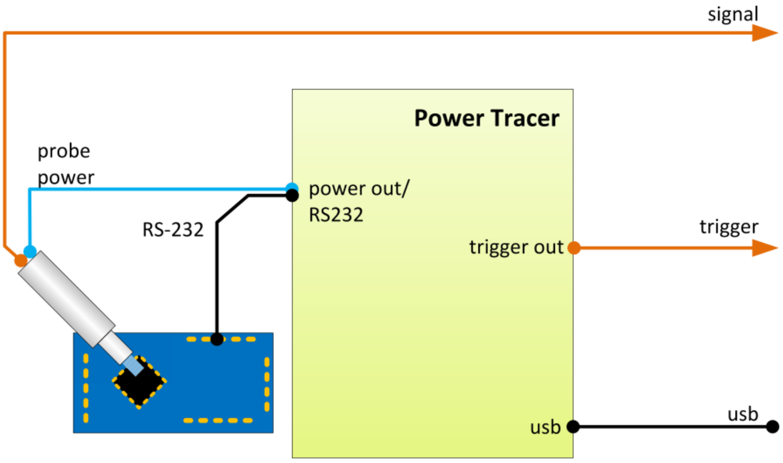
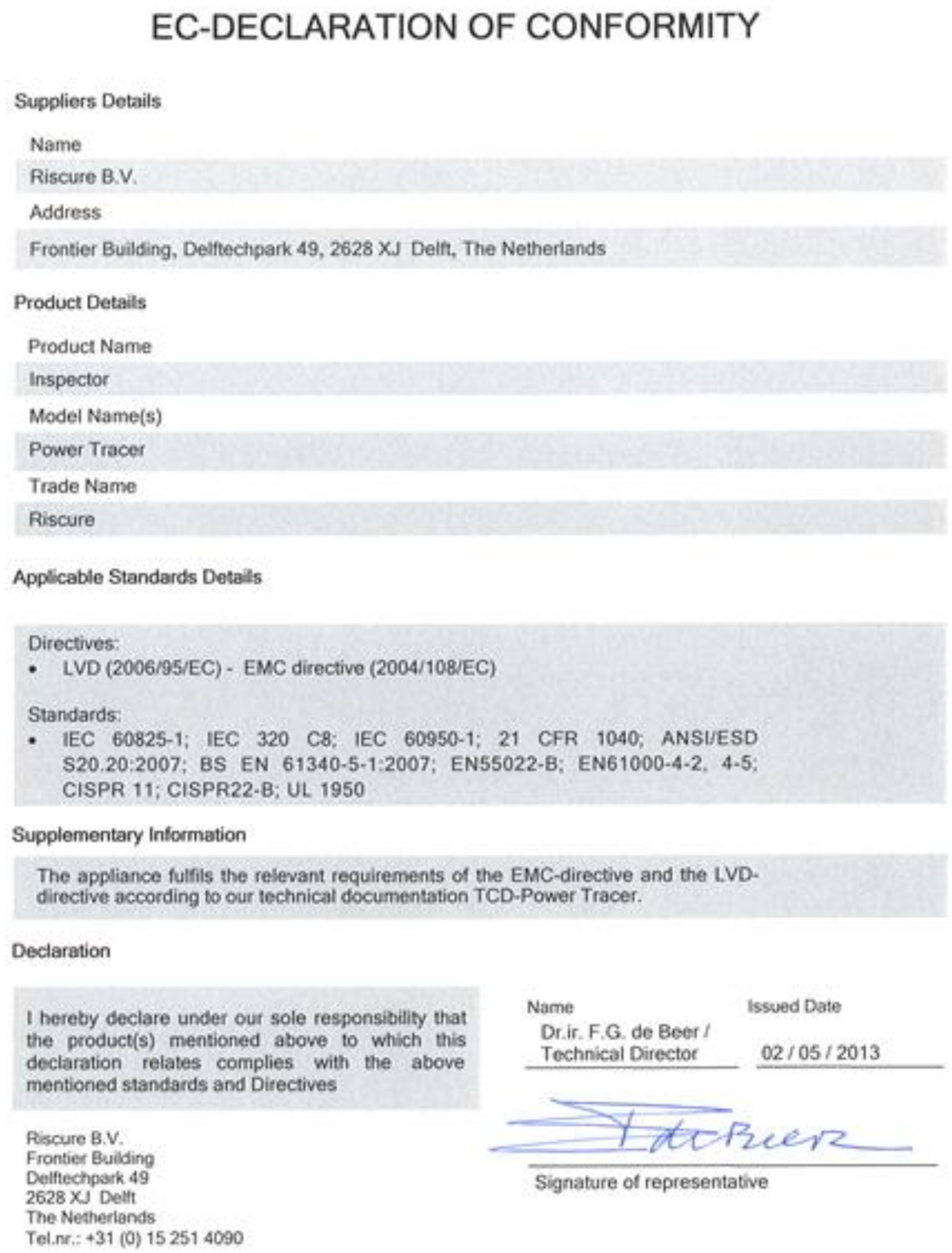


Figure 13 Probing an embedded target while communicating via the RS232 interface.

Declarations 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)

Power Tracer

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-Power Tracer.

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

Notes: