



# EM-FI Transient Probe Adjustable Pulse Width

## Quick Start Guide



What is in the box .....	3
Safety instructions .....	6
What does it do .....	7
Connecting a Spider.....	8
How to build a setup .....	9
Using the Base unit .....	12
Setting up the power supply .....	22
How to verify your setup .....	24
Help and troubleshooting.....	25



<b>Technical specifications .....</b>	<b>26</b>
<b>In / out puts .....</b>	<b>29</b>











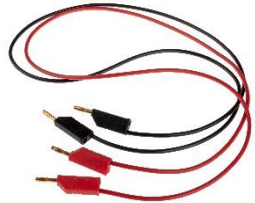
## What is in the box

The box contains the EM-FI Transient Probe Adjustable Pulse Width and all standard accessories and cables to connect it to a glitch generator.



### Box content checklist

Qty [1]	Description	Photo	Identifier [2]
1	EM-FI Transient Probe Adjustable Pulse Width, with bracket		EMFI APW
1	Probe: - High precision HP EM Probe base		Amplifier unit
1	Power Supply Unit, 6 V DC input 100 V to 240 V AC, 50 – 60 Hz,		PSU for base unit
1	Signal differential cable:  Differential BNC coax cable		
4	Probe tips: - flat head tip, red: $\varnothing$ 1.5 and 4 mm 3 windings - flat head tip, red: $\varnothing$ 1.5 and 4 mm 6 windings		
2	Signal cable: SMB – SMB, 50 $\Omega$ , coax, 6 ft		SMB2SMB

Qty [1]	Description	Photo	Identifier [2]
1	Signal cable: SMB – BNC, 50 $\Omega$ , coax, 6 ft		SMB2BNC
1	Signal cable: BNC - BNC, 50 $\Omega$ , coax		BNC2BNC
	Banana plug cables:  - Black - Red		
1	Lab power supply (Optional):  Lab power supply to power EMFI APW		PSU for EMFI APW
-	This “EM-FI Transient Probe Adjustable Pulse Width- Quick Start Guide”		

[1] The amount of registered items (quantity, Qty).

[2] Identifier used in this document to refer to the item.

# Safety instructions

## Electrical safety



**Do not exceed the Pulse Length of 200ns. The EM-FI APW be permanently damaged**



**HIGH VOLTAGE ON THE PROBE TIP**

**DO NOT** touch the probe tip when it is actively firing pulses.



**LIFE-THRETHENING INTERNAL VOLTAGE AND CURRENT**

**DO NOT** open the product casing.



**ONLY USE TIPS LABELED “APW”.** If other tips are used EMFI APW will be permanently damaged

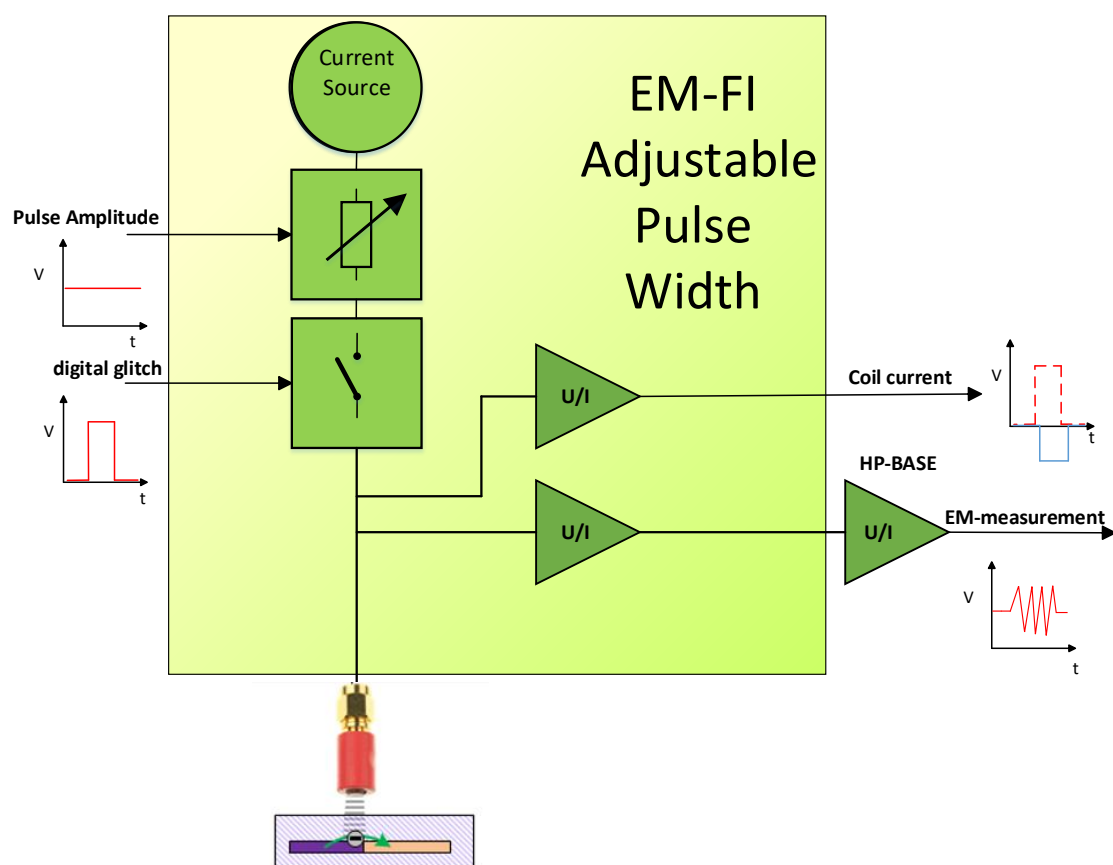


**Do not exceed 12VDC power supply input.** The EM-FI APW be permanently damaged

## What does it do

The EM-FI APW is an electromagnetic (EM) perturbation device used for Fault Injection (FI) attacks and measure the electromagnetic field during the attack.

The probe is capable of delivering fast, precise and powerful electromagnetic pulses, used for inducing currents in metal layers and causing voltage glitches in CMOS logic gates.



*Figure 1 Functional overview of the EM-FI Transient Probe.*

The EM-FI APW uses amplitude and timing signals from an external glitch generator, and is typically used in a XYZ Stage in combination with a Spider.

# Connecting a Spider

## Connecting Spider to EMFI

The following connections need to be made between Spider and EM-FI APW:

1. To trigger generation of an EM pulse, a connection needs to be made between Spider, SMB-SMB cable, 50 ohm feed thru terminator and EM-FI APW in the following order:
  - Connect 50 ohm feed thru terminator to 'glitch out 1' of Spider,
  - Connect SMB-SMB cable to '50 ohm feed thru terminator,
  - Connect SMB-SMB cable to 'digital glitch' input of EM-FI APW
  
2. To set EM pulse strength, a connection needs to be made between Spider, SMB-SMB cable and EM-FI APW in the following order:
  - Connect SMB-SMB cable to 'voltage out 1' of Spider,
  - Connect SMB-SMB cable to 'pulse amplitude' input of EM-FI APW probe.



# How to build a setup

## Setup for EM glitching of a smart card

This setup uses the VC Glitcher as smart card reader and as producer of the glitch triggers. The EM-FI APW is placed above the non-contact side of the smart card.

To measure the EM radiation of the smart card via the EM-FI APW tip “**HP-Base**” is used to amplify the signal. This “**HP-Base**” is connected to a digital scope.

Figure 2 also shows the connection of the **coil current** output with an oscilloscope, to verify if the setup is correctly configured and the probe tip is activated.

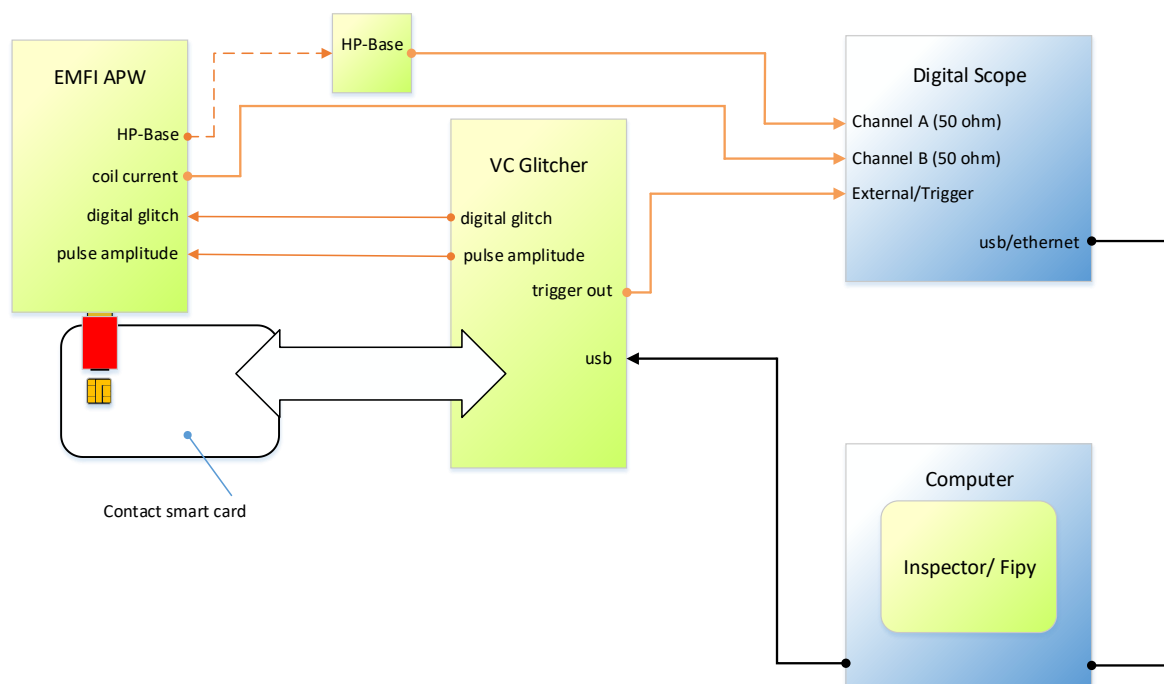


Figure 2 Basic setup for EM fault injection of a smart card.

## Setup for EM glitching of an embedded target

This setup uses the Spider as producer of the glitch triggers.

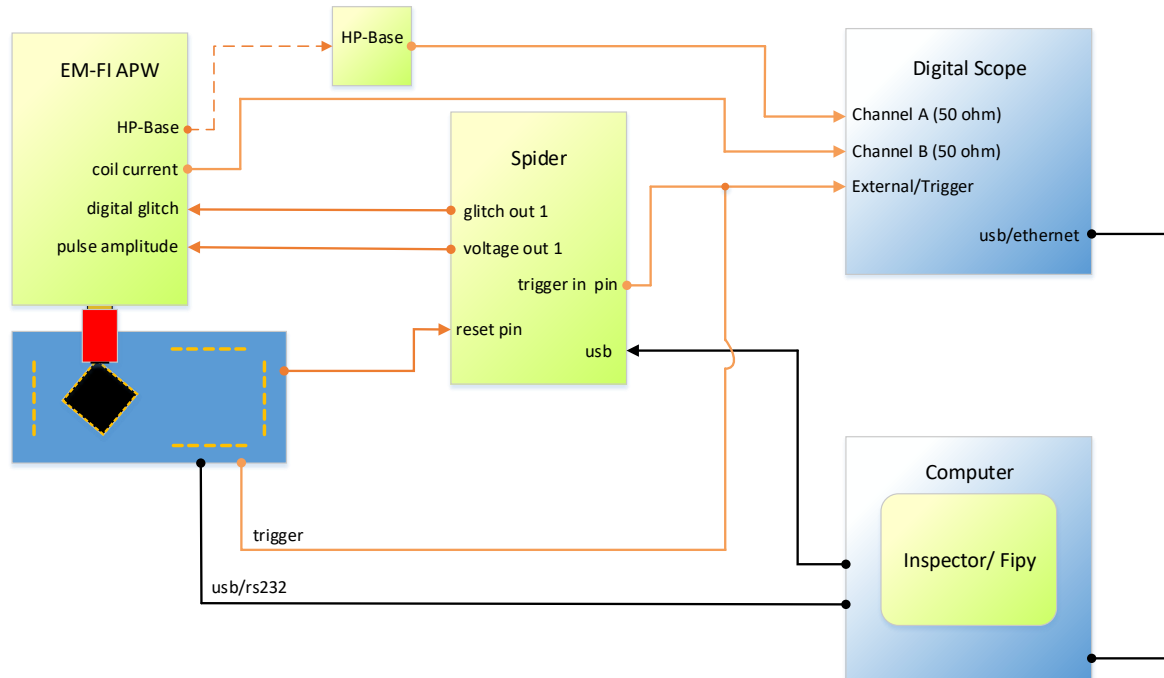


Figure 3 Basic setup for EM fault injection of an embedded target.

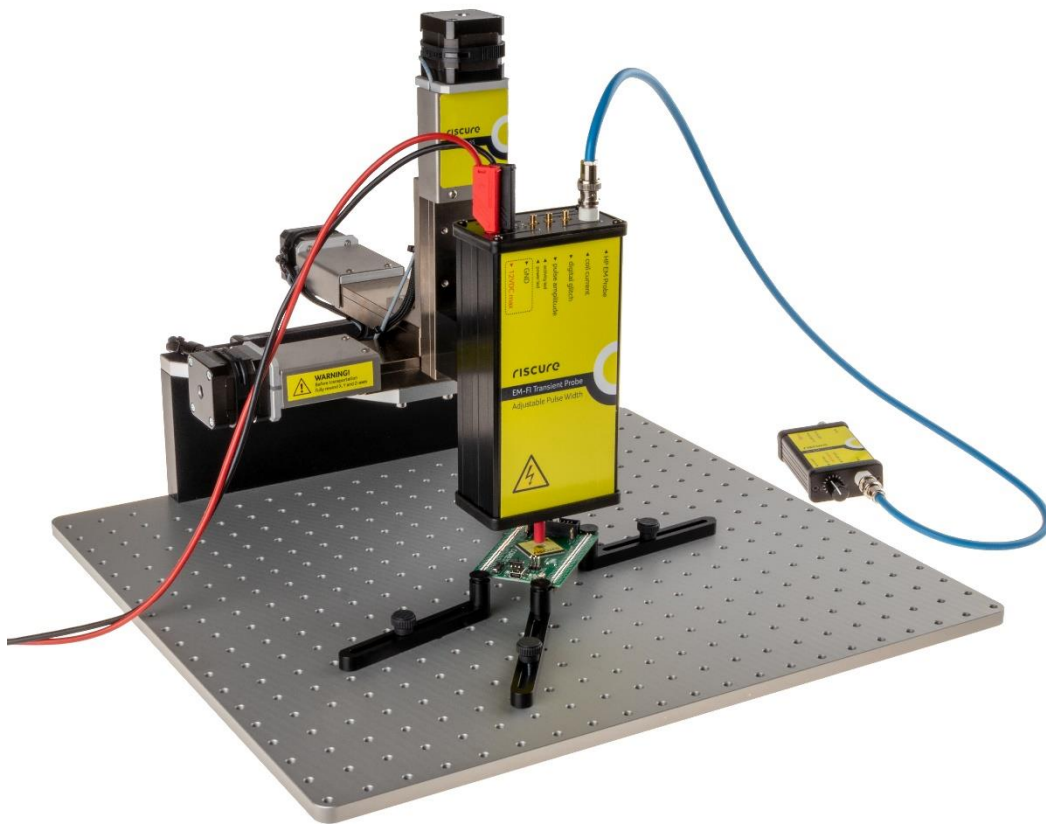


Figure 4 EMFI APW on XYZ Stage with embedded target.

# Using the Base unit

## Connecting the Base Unit

Connect the Base Unit with cable BNC2BNC to a measurement channel with 50  $\Omega$  impedance (or through a 50  $\Omega$  impedance adapter [not supplied]).

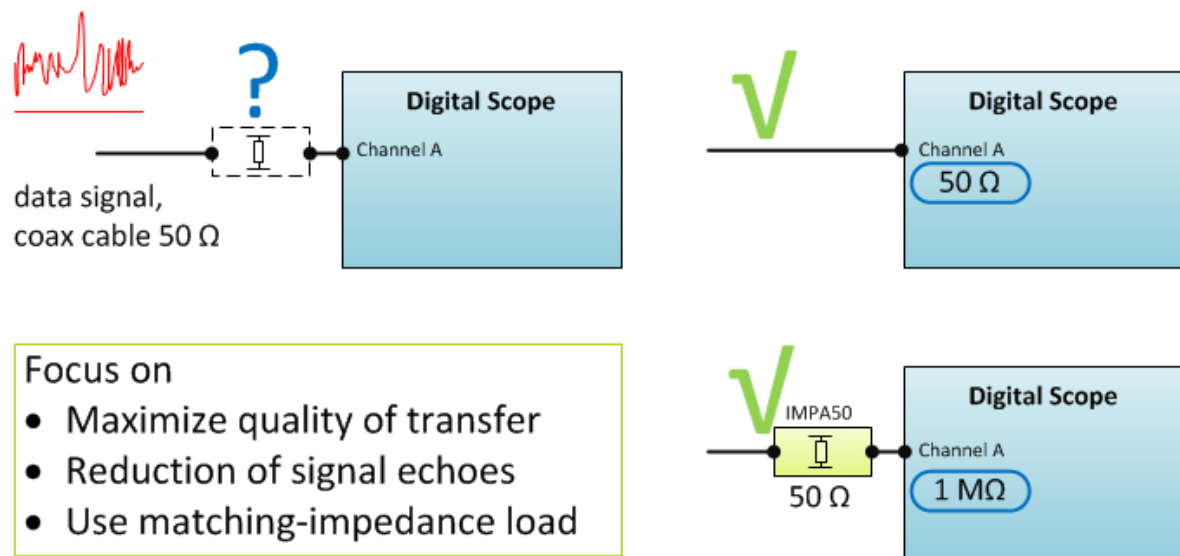


Figure 5 Reading the Base Unit signal with a matching impedance.

## Adjusting the gain

There are two methods of adjusting the probe sensitivity.

The first method is using the manual gain knob.

- Make sure the “man. gain on” LED indicator is lit up. If not, push the gain knob to switch to manual gain.
- Rotate the “man. gain” knob clockwise until the desired gain setting has been met.



*Figure 6 Manual gain.*



Use the engraved markers around the “man. gain” knob for easy reproducibility of the gain setting.

The second method is control gain through an external device that can put an accurate voltage for amplification of the signal by the internal amplifiers of the base unit.

- Make sure to pull the “man. gain” knob. The “ext. gain on” LED indicator will light up.
- Use a device (for example Riscure Spider) to provide an accurate voltage from 0V (low gain) to 3.3V (high gain) to the “ext. gain” SMB input to set the desired gain.



*Figure 7 The “man. gain” knob is pulled out to enable external gain.*



**Do not use a control voltage greater than 3.3V**

This results in damaging the Base Unit.



Smaller probe tips produce weaker signals. To compensate, the oscilloscope sensitivity needs to be increased or adjust the Base Unit gain.

## Connecting the Differential BNC cable

The differential BNC cable connects Core to Base unit.

Mount the differential BNC cable on EM-FI APW unit by placing the notch against the pin of EM-FI APW unit connector.

If connector does not slide in fully, rotate the end of the connector until it does.

Do the same at Base Unit side.



*Figure 8 Differential BNC Connector*



**Do not use force.**

The connector might damage.

## Attaching the bracket

The EM-FI APW comes with a disassembled bracket.

Fit the bracket to the back panel with the 2 screws supplied. There are 3 different fitting positions to meet your need for a height above the baseplate.

With the bracket fitted, the probe fits into the probe clamp of the XYZ Stage as well as the LS2 (Laser Station) (Figure 9).



*Figure 9 the backside bracket enables the EM-FI Transient Probe to be fitted on the LS2 (Laser Station) and the XYZ Stage.*



## Selecting the AWP probe tip



*Figure 10 Different probe tips for EM fault injection.*

The EM-FI APW is supplied with flat head probe tips (Figure 10).



**Only use tips labeled “APW”.** If other tips are used the EMFI APW will be permanently damaged

The flat head probe tip produces a magnetic field which is perpendicular to the surface and is applied to induce currents in a circuit loop between adjacent gates (Figure 11).

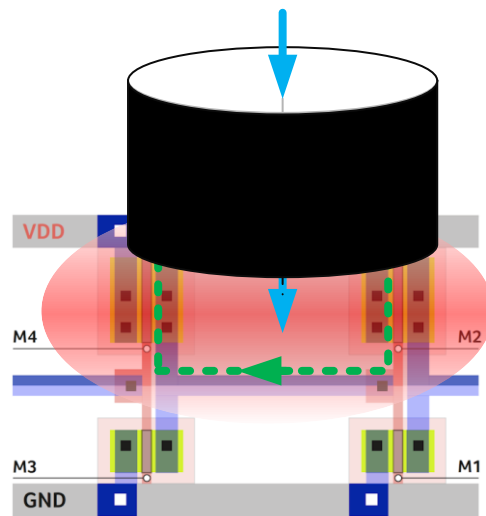


Figure 11 the concepts of glitching with a flat head tip.

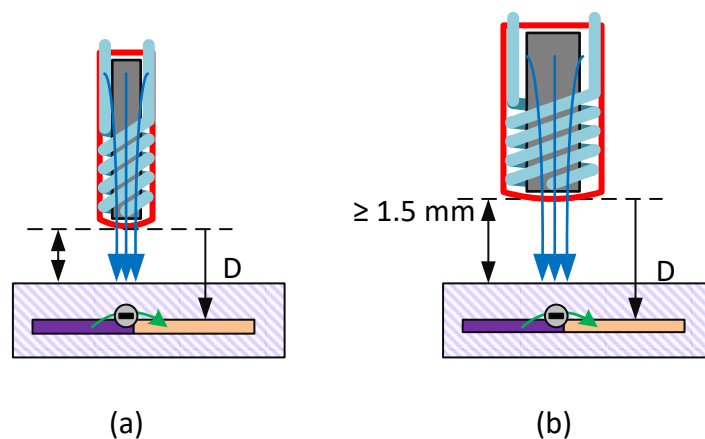


Figure 12 diameter (a, b) for the flat head probe tip

The flat head tips come with different windings and diameter. The tip with six windings is optimized for perturbation.

The tip with three windings is optimized for EM measurements. Both are interchangeable. Select the probe tip best suited for your target.

Choose the appropriate diameter of the flat head tip after considering the thickness (and material density) of the encapsulation and the depth of the metal layer (Figure 12 a, b). Use the **small tip** (Figure 12a) if the penetration depth **D** is less than

1.5 mm, or when acquiring a detailed scan of a surface region. Use the **wide tip** (Figure 12b) if the penetration depth needs to be more than 1.5 mm, or when globally scanning for regions susceptible to faults (hotspots).

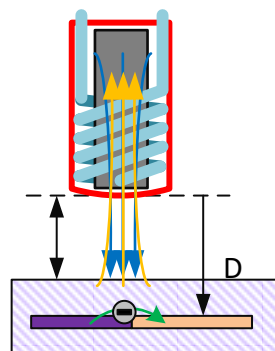
## Perturbation and acquisition

When the **Base Unit** connected to EM-FI APW. It is possible continuously acquire EM measurements from your target via the same tip as to do perturbation.

The measurement circuit is always active.

The Pulse is visible in the EM acquisition. If this behavior is not desired.

Turn off the EM-FI AWP.



*Figure 13 perturbation and acquisition thru the flat head probe tip*

In Figure 14 green is the trigger signal. Yellow is the output of the Base Unit showing EM measurement. The large yellow spike is a EM pulse that is targeting round 9 on AES encryption.

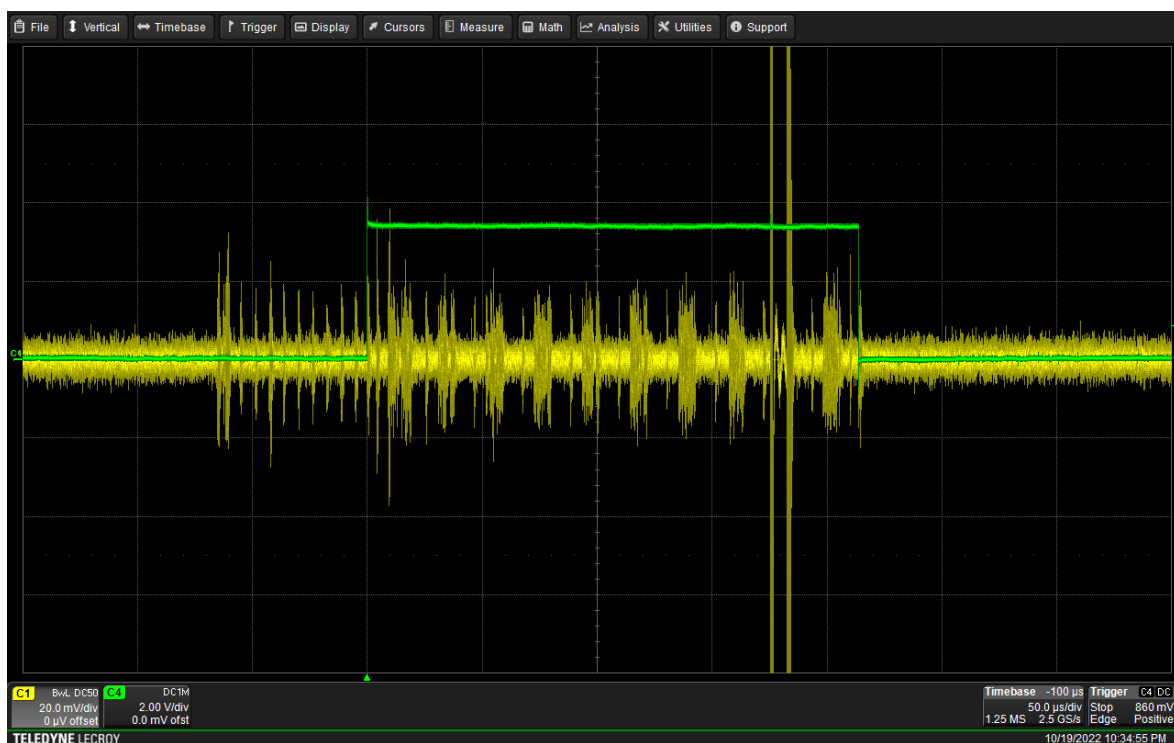


Figure 15 perturbation and measurement of AES on training target Piñata.

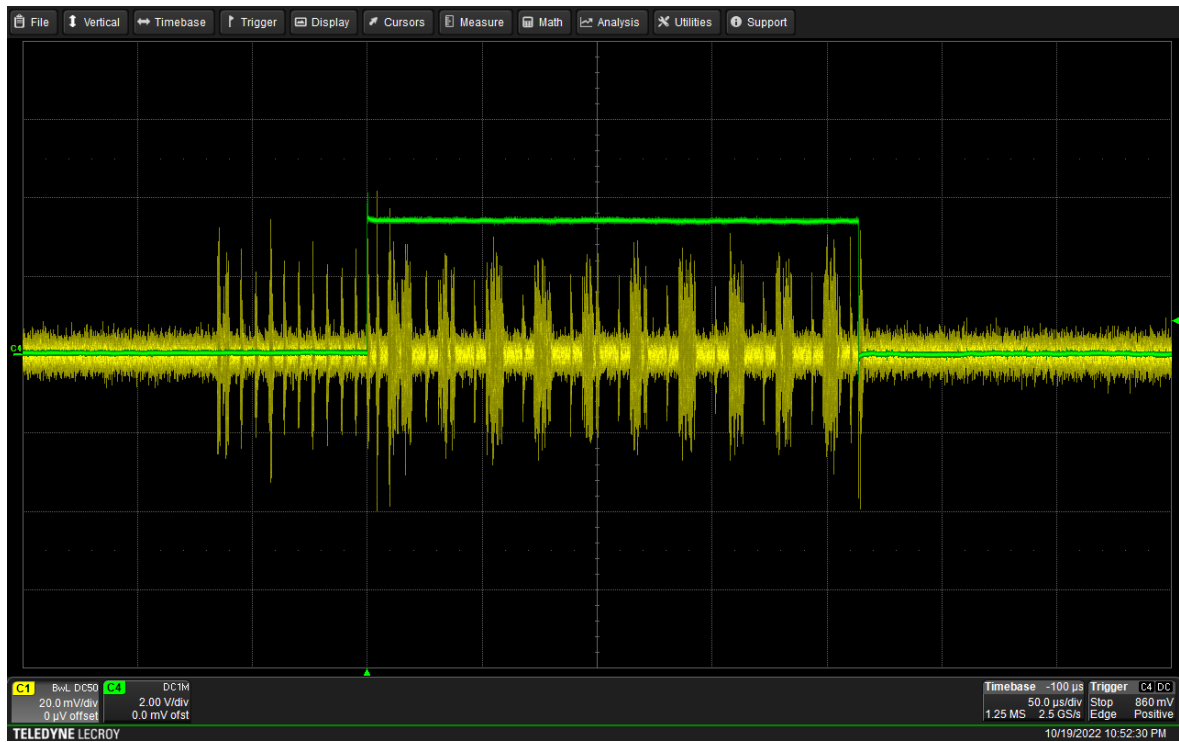


Figure 16 measurement of AES on training target Piñata.

## Setting up the power supply

To Power EMFI APW.

Use a lab power supply that is capable of 12VDC output and 4A initial peak current.

### Connecting the power supply

Make sure the power supply is turned off.

Connect the black and red banana cables from the PSU to the EMFI APW.

Make sure red cable is matching red connectors.

And black cable is matching black connectors.

### Power supply settings

Make sure the output is 12VDC and the maximum current is 4A.

If there are overload protections and/or limits on the power supply enable them.

Overload or limit :

- Voltage: 13VDC
- Current: 4A (only on power up. After power up this can be lowered to 600mA)

Now enable the power supply to power EMFI APW



## How to verify your setup

Follow the next checks to verify a correct setup:

3. Is the EM-FI APW powered?
4. Is the EM-FI APW responding to triggers?

Please ensure that each check is successful, before proceeding to the next one. If not successful, refer to page 25 for solutions.

### Is the probe powered?

There are no visible or audible signs of the EM-FI Transient Probe being powered.

Verify that the EM-FI APW is using a 12 V PSU, and that the PSU is connected to mains supply.

### Is the probe responding to triggers?

Follow the next steps to verify the control behavior of the EM-FI APW:

1. Connect the **coil current** output of the probe to an **input channel** of an oscilloscope.
2. Set input channel range to -2 V .. +2 V.
3. Verify that the **pulse amplitude** and **digital glitch** connections with the VC Glitcher or Spider are not mixed up.
4. Execute a perturbation program in Inspector or FiPy.  
Configure the pulse amplitude to 3.3 V.
5. For each active-high trigger pulse received on port **digital glitch** of the EM-FI Transient Probe, the oscilloscope must display a negative pulse. This is evidence that the probe tip coil emits EM pulses.



# Help and troubleshooting

## Common problems

---

Probe does not work.

**CAUSE:** Probe not powered.

**SOLUTION:** Verify the connection of the power cable to the EM-FI APW and to the PSU.

---

**CAUSE:** The probe's **digital glitch** port has a static value because it is connected to **pulse amplitude** of the VC Glitcher or Spider.

**SOLUTION:** Reconnect the mixed up cables to the correct ports of the VC Glitcher or Spider.

---

**CAUSE:** At least one of the cables is not connected.

**SOLUTION:** Guide all cables from input to output, and reseal its connectors.

---

**CAUSE:** Probe tip is not properly fitted.

**SOLUTION:** Fastened the probe tip.

---

## Still have questions?

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

# Technical specifications

## Operational conditions

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



Do not Exceed the Pulse Length of 200ns. The EM-FI APW will break down.



Do not block the ventilation holes of the EM-FI APW. A blocked air flow may cause malfunction or break down.



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



Turning OFF the EM-FI Transient Probe is not required but recommended when not used for an extended period.

## Power supply input

- EMFI APW 12V DC. 500mA max (4 A initial peak current)
- Banana plug : Red = 12V DC.
- Banana plug : Black = Ground.
  
- Base amplifier 6V DC, nominal load 2 A  
Center-positive plug, inner-Ø 2.5 mm, outer-Ø 5.5 mm

## Probe characteristics

- Max. voltage over coil: 100 V  $\pm$  10%
- Max. internal current: 92 A  $\pm$  10%

- EM pulse power control: 5 .. 100%
- Digital glitch pulse width for full power: Adjustable, 4–200ns  $\pm$  10%
- Max. switching frequency for constant power: 1 MHz

Characteristic	Tip ø 1.5 mm 6windings	Tip ø 4 mm 5 3windings
<b>Electromagnetic propagation delay</b> (10% edge of digital glitch to 10% edge of magnetic/EM field change)	20 ns $\pm$ 10%	20 ns $\pm$ 10%
<b>Electric propagation delay</b> (10% edge of digital glitch to 10% edge of coil current signal)	18 ns $\pm$ 10%	18 ns $\pm$ 10%
<b>Max. current</b> through coil	56 A $\pm$ 10%	69 A $\pm$ 10%
<b>Max. voltage</b> at coil current port	-1.4 V $\pm$ 10%	-2 V $\pm$ 10%
<b>Pulse width</b> of waveform at coil current port	4 / 200 ns $\pm$ 10%	4 / 200 ns $\pm$ 10%
<b>Operating distance</b> tip to target layer	$\leq$ 1.5 mm	$\leq$ 4 mm

## Probe attachment

- Outer diameter of bracket: ø 25 mm
- Weight: 650 g

## In / out puts



## Product case

- Dimensions: 181 x 92 x 50 [mm], 7.23 x 3,62 x 1,97 [inch] (L x W x H)

Element	Label	Description
1	-	Probe tip.
2	<b>HP EMPProbe</b>	Connector for the Base Unit. To perform EM measurements
3	<b>coil current</b>	SMB, 50 $\Omega$ Analog output. -2.0 V .. 0V. A voltage proportional to the current through the coil for monitoring purposes. Usually connected to an oscilloscope.
4	<b>digital glitch</b>	SMB, 50 $\Omega$ Binary active high input. A probe fires a single EM pulse if the voltage gets over 2.4 V.
5	<b>pulse amplitude</b>	SMB, 50 $\Omega$ . Analog input, 0 .. 3.3 V. Defines proportional EM power level 0 V= 5%, 3.3 V = 100%.
6	<b>Activity led</b>	LED , Blink when probe fires. Illuminates proportional to digital glitch plus pulse amplitude
7	<b>Power led</b>	LED, Status LED. Illuminates when EMFI APW is powered
8+9	<b>GND + 12VDC</b>	12 VDC Power supply input. Banana Plugs connectors



Element	Label	Description
1	<b>out</b>	BNC, Analog output -2.5 V ~ +2.5V (50 ohm)
2	<b>ext. gain</b>	Control voltage input 0V ~ +3.3V (2.3k ohm)
3	<b>ext gain LED</b>	When ON amplification is controlled with external voltage (2)
4	<b>Power in</b>	Connector for the 6 V DC 2 A PSU
5	<b>Power on</b>	When lit power is OK
6	<b>man gain</b>	Knob to control the gain
7	<b>Man. gain LED</b>	When ON amplification is controlled with potentiometer.
8	<b>in</b>	Connection to the HP EMProbe connector on EMFI APW

## 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)

EM-FI Transient Probe Adjustable Pulse Width

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-EM-FI APW.

### 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

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

Name

Dr.ir. F.G. de Beer /  
Technical Director

Issued Date

01 / 11 / 2022



Signature of representative