Keysight Bidirectional Fault Injection Probe

DS1121A Bidirectional Fault Injection Probe

KEYSIGHT

USER MANUAL

Notices

Trademark Acknowledgments

Manual Part Number

DS1221-90002

Edition

Edition 1, October 2024

Published by:
Keysight Technologies
1400 Fountain Grove Parkway
Santa Rosa, CA 95403

Warranty

THE MATERIAL CONTAINED IN THIS DOCUMENT IS PROVIDED "AS IS," AND IS SUBJECT TO BEING CHANGED, WITHOUT NOTICE, IN FUTURE EDITIONS. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, KEYSIGHT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED WITH REGARD TO THIS MANUAL AND ANY INFORMATION CONTAINED HEREIN, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. KEYSIGHT SHALL NOT BE LIABLE FOR ERRORS OR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, USE, OR PERFORMANCE OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. SHOULD KEYSIGHT AND THE USER HAVE A SEPARATE WRITTEN AGREEMENT WITH WARRANTY TERMS COVERING THE MATERIAL IN THIS DOCUMENT THAT CONFLICT WITH THESE TERMS, THE WARRANTY TERMS IN THE SEPARATE AGREEMENT WILL CONTROL.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation

("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at

https://www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, browse to one of the following URLs, according to the name of your product:

https://www.keysight.com/us/en/product/DS1121A/bidirectional-fault-injection-probe.html

To receive the latest updates by email, subscribe to Keysight Email Updates at the following URL:

https://support.keysight.com

Information on preventing instrument damage can be found at:

https://www.keysight.com/find/PreventingInstrumentDamage

Is your product software up-to-date?

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates for your product, go to the Keysight Technical Support website at:

https://www.keysight.com/us/en/about/quality-and-security/security/product-and-solution-cyber-security.html

Product and Solution Cybersecurity

Keysight complies with multinational regulations for the cybersecurity of its own products and is committed to providing information to assist you in protecting your products and solutions from external cyber threats. For more information, see:

https://www.keysight.com/us/en/about/quality-and-security/security/product-and-solution-cyber-security.html

Keysight also recommends that you secure your IT environments using appropriate third-party tools. For instruments that run the Microsoft Windows operating system, Keysight concurs with Microsoft's recommendations for ensuring that the instrument is protected:

- Get the latest critical Windows updates
- For network-connected instruments, use an Internet firewall (in Keysight instruments, Windows Firewalls enabled by default)
- For network-connected instruments, use up-to-date antivirus and anti-spyware software

Responsible Disclosure Program

Keysight recommends that security researchers share the details of any suspected vulnerabilities across any asset owned, controlled, or operated by Keysight (or that would reasonably impact the security of Keysight and our users) using this form:

https://www.keysight.com/us/en/contact/responsible-disclosure-program.html

Report a Product Cybersecurity Issue

If you discover a cybersecurity issue that you suspect may involve Keysight's proprietary software, or third-party software supplied by Keysight as part of a product, or that may affect the operation of Keysight products, we encourage you to report it to us using this form:

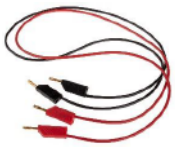
https://www.keysight.com/us/en/about/quality-and-security/security/product-and-solution-cyber-security.html

Contents

What's in the Box?

The box contains the Bidirectional Fault Injection Probe and all standard accessories and cables to connect it to a glitch generator.

Quantity[1]	Description	Photo	Identifier[2]
1	Bidirectional Fault Injection Probe, with bracket		EMFI APW
— 1	Probe: — High Precision Electromagnetic 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: ø 1.5 and 4 mm 3 windings — flat head tip, red: ø 1.5 and 4 mm 6 windings		
2	Signal cable: SMB – SMB, 50 Ω, coax, 6 ft		SMB2SMB
1	Signal cable: SMB – BNC, 50 Ω, coax, 6 ft		SMB2BNC

	Banana plug cables: — Black — Red 	
1	Lab power supply (Optional): Lab power supply to power Bidirectional Fault Injection Probe	PSU for Bidirectional Fault Injection Probe
-	This "DS1121A Bidirectional Fault Injection Probe User Manual"	

1. The number of registered items (quantity, Qty).
2. Identifier used in this document to refer to the item.

Safety Instructions

Electrical safety

WARNING Do not exceed the Pulse Length of 200ns. The Bidirectional Fault Injection Probe will be permanently damaged.

WARNING High voltage on the probe tip.
Do not touch the probe tip when it is actively firing pulses.

WARNING Life-threatening internal voltage and current.
Do not open the product casing.

WARNING Only use tips labeled "APW". If other tips are used Bidirectional Fault Injection Probe will be permanently damaged.

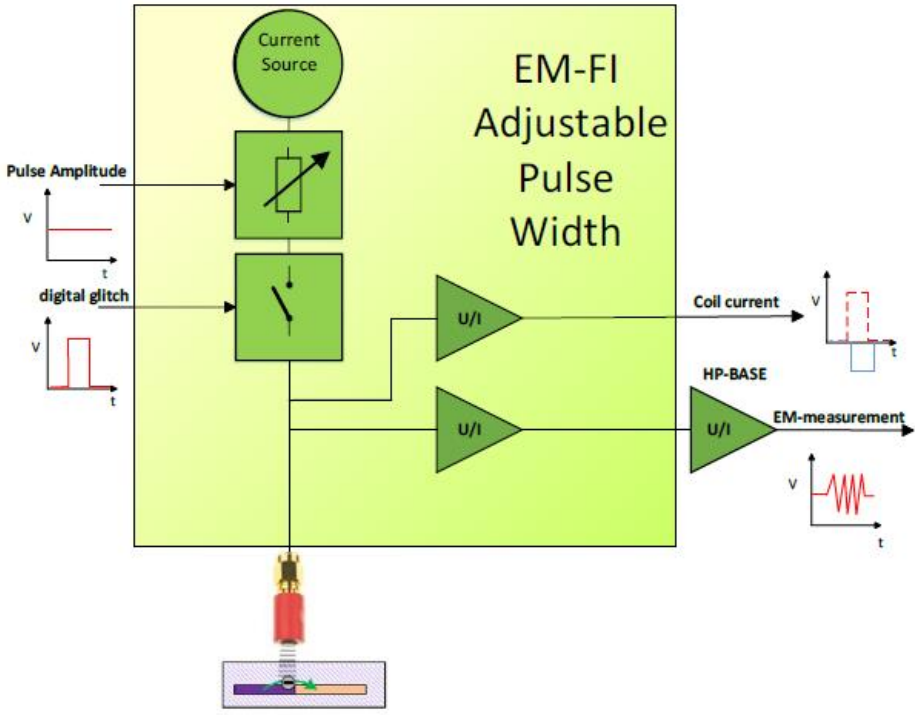
WARNING Do not exceed 12VDC power supply input. The Bidirectional Fault Injection Probe will be permanently damaged.

What It Does

The Bidirectional Fault Injection Probe is an electromagnetic (EM) perturbation device used for fault injection (FI) attacks and measures 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 Bidirectional Fault Injection Probe



The Bidirectional Fault Injection Probe uses amplitude and timing signals from an external glitch generator and is typically used in a XYZ Stage in combination with a Glitch Pattern Generator.

Connecting a Glitch Pattern Generator

Connecting Glitch Pattern Generator to Bidirectional Fault Injection Probe

The following connections need to be made between Glitch Pattern Generator and Bidirectional Fault Injection Probe:

1. **To trigger generation of an EM pulse, a connection needs to be made between Glitch Pattern Generator, SMB-SMB cable, 50 ohm feed thru terminator and Bidirectional Fault Injection probe in the following order:**
   - Connect 50 ohm feed thru terminator to 'glitch out 1' of Glitch Pattern Generator.
   - Connect SMB-SMB cable to 50 ohm feed thru terminator.
   - Connect SMB-SMB cable to 'digital glitch' input of Bidirectional Fault Injection probe.
2. **To set EM pulse strength, a connection needs to be made between Glitch Pattern Generator, SMB-SMB cable, and Bidirectional Fault Injection Probe in the following order:**
   - Connect SMB-SMB cable to 'voltage out 1' of Glitch Pattern Generator.
   - Connect SMB-SMB cable to 'pulse amplitude' input of Bidirectional Fault Injection Probe.

How to Build a Setup

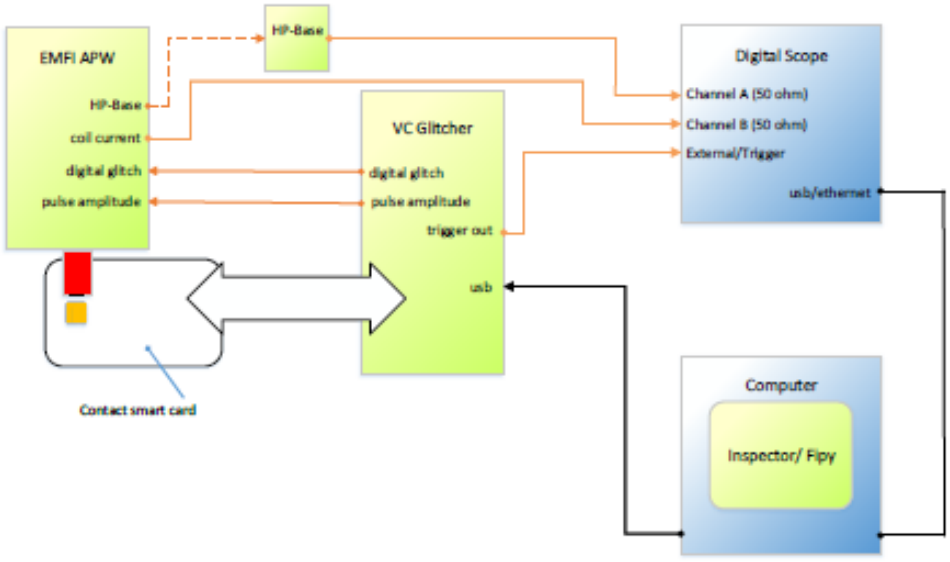
Setup for EM glitching of a smart card

This setup uses the Smartcard Voltage and Clock Glitcher as smart card reader and as producer of the glitch triggers. The Bidirectional Fault Injection Probe is placed above the non-contact side of the smart card.

To measure the EM radiation of the smart card via the Bidirectional Fault Injection Probe 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 Glitch Pattern Generator as producer of the glitch triggers.

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

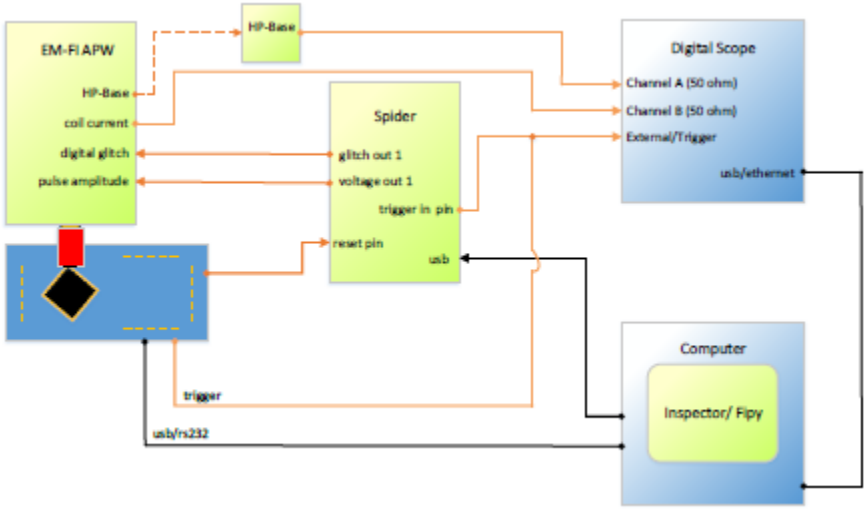
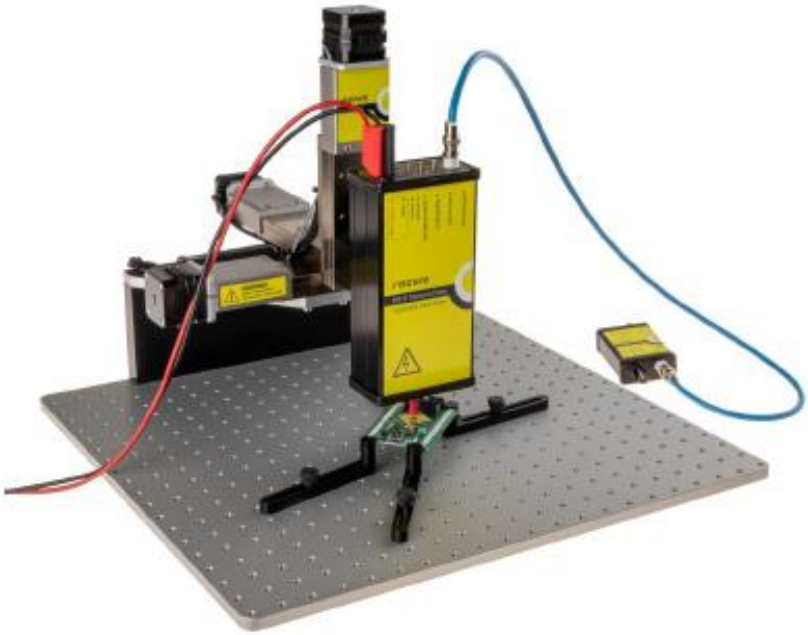


Figure 4 Bidirectional Fault Injection Probe on XYZ Stage with embedded target

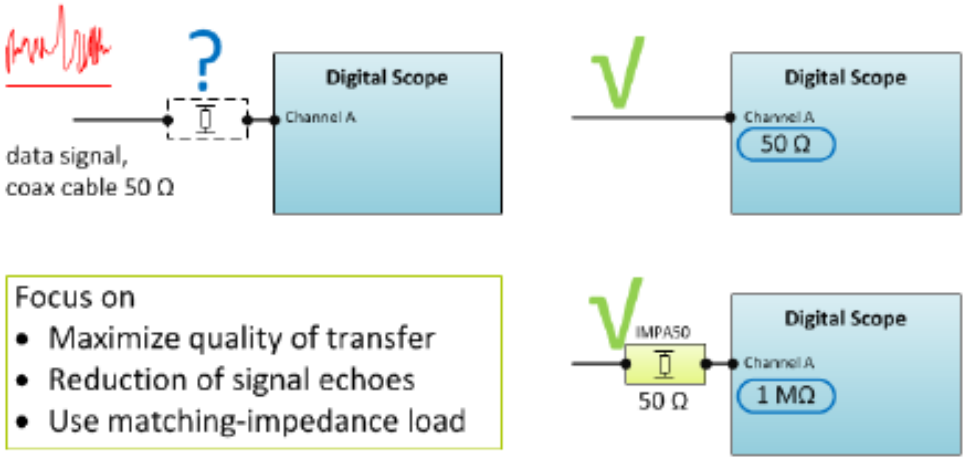


Using the Base Unit

Connecting the Base Unit

Connect the Base Unit with cable BNC2BNC to a measurement channel with 50 Ω impedance (or through a 50 Ω 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

NOTE

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 Keysight Glitch Pattern Generator) 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

WARNING Do not use a control voltage greater than 3.3V
This results in damaging the Base Unit.

NOTE 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 Bidirectional Fault Injection Probe unit by placing the notch against the pin of Bidirectional Fault Injection Probe 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

WARNING

Do not use force.
The connector might damage.

Attaching the bracket

The Bidirectional Fault Injection Probe comes with a disassembled bracket.

Fit the bracket to the back panel with the two screws supplied. There are three 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 Bidirectional Fault Injection Probe to be fitted on the LS2 (Laser Station) and the XYZ Stage.

Selecting the AWP probe tip

Figure 10. Different probe tips for Bidirectional Fault Injection Probe

The Bidirectional Fault Injection Probe is supplied with flat head probe tips (Figure 10).

WARNING **Only use tips labeled “APW”. If other tips are used the Bidirectional Fault Injection Probe 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

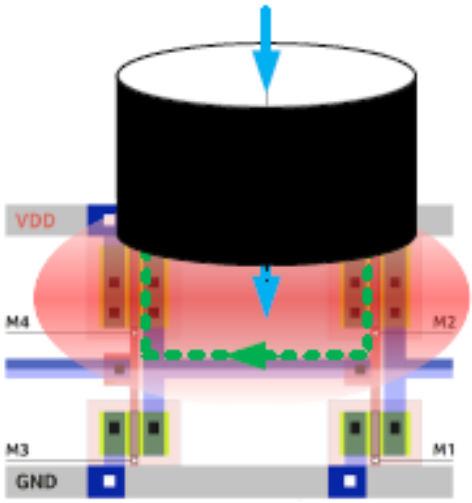
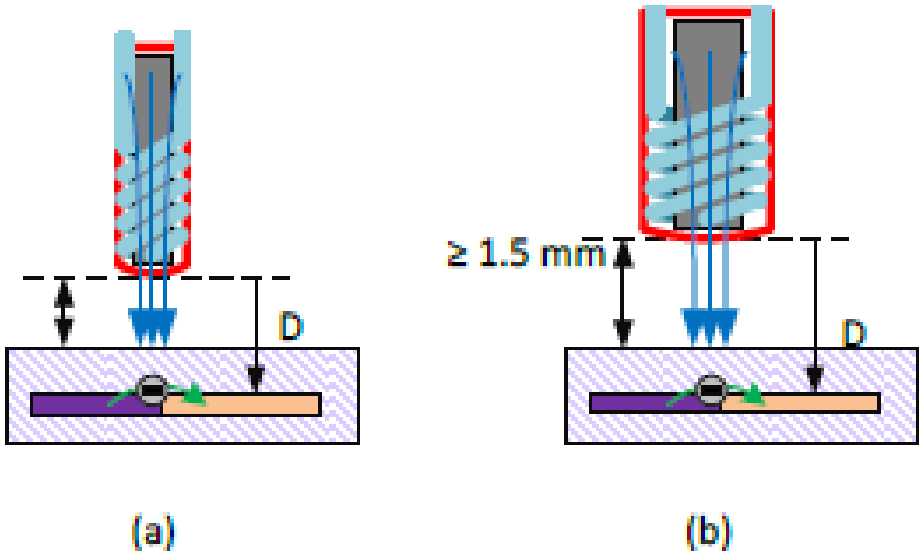


Figure 12 Diameter (a, b) for the flat head probe tip



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

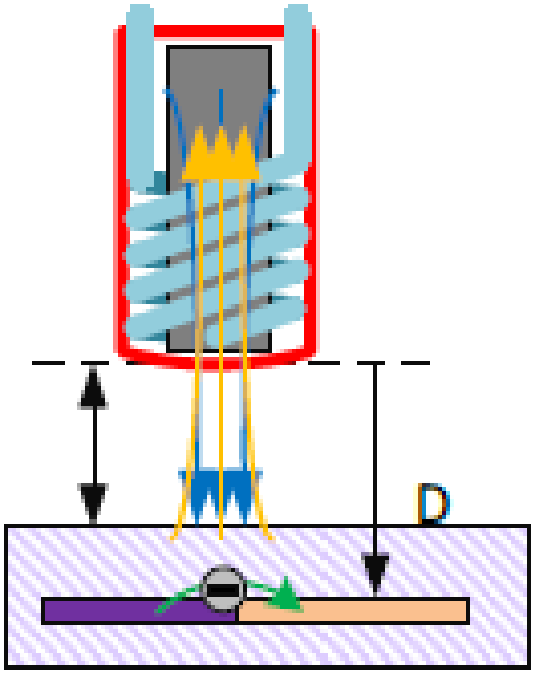
When the Base Unit is connected to Bidirectional Fault Injection Probe, it is possible to continuously acquire EM measurements from your target via the same tip as to do perturbation.

The measurement circuit is always active.

The Pulse is visible in the EM acquisition.

If this behavior is not desired, turn off the Bidirectional Fault Injection Probe.

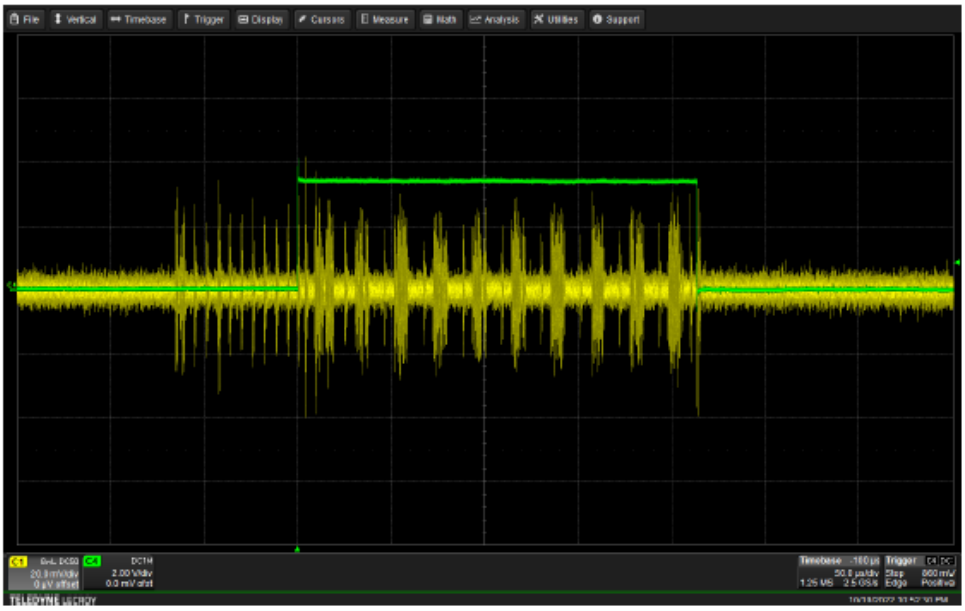
Figure 13 Perturbation and acquisition thru the flat head probe tip



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

Figure 15 Perturbation and measurement of AES on training target Software and Hardware Crypto Training Target

Figure 16 Measurement of AES on training target Software and Hardware Crypto Training Target



Setting Up the Power Supply

To power the Bidirectional Fault Injection Probe 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 Bidirectional Fault Injection Probe.

Make sure the red cable matches the red connectors, and the black cable matches the 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 Bidirectional Fault Injection Probe.

How to Verify Your Setup

Follow the next checks to verify a correct setup:

1. Is the Bidirectional Fault Injection Probe powered?
2. Is the Bidirectional Fault Injection Probe 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 Bidirectional Fault Injection Probe being powered.

Verify that the Bidirectional Fault Injection Probe 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 Bidirectional Fault Injection Probe:

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 Glitch Pattern Generator 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 Bidirectional Fault Injection Probe, the oscilloscope must display a negative pulse. This is evidence that the probe tip coil emits EM pulses.

Help and Troubleshooting

Common problems

Problem	Cause	Solution
Probe does not work	Probe not powered.	Verify the connection of the power cable to the Bidirectional Fault Injection Probe and to the PSU.
	The probe's digital glitch port has a static value because it is connected to pulse amplitude of the VC Glitcher or Glitch Pattern Generator.	Reconnect the mixed cables to the correct ports of the VC Glitcher or Glitch Pattern Generator.
	At least one of the cables is not connected.	Guide all cables from input to output and reseat its connectors.
	Probe tip is not properly fitted.	Fastened the probe tip

Still have questions?

Visit the Keysight Support Portal: https://support.keysight.com/

Technical Specifications

Operational conditions

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

WARNING Do not Exceed the Pulse Length of 200ns. The Bidirectional Fault Injection Probe will break down.

WARNING Do not block the ventilation holes of the Bidirectional Fault Injection Probe . A blocked air flow may cause malfunction or break down.

NOTE Maintain a stable and identical environment to reliably repeat tests.

NOTE Turning OFF the Bidirectional Fault Injection 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 ± 10%.
- Max. internal current: 92 A ± 10%.

– EM pulse power control: 5 .. 100%.

– Digital glitch pulse width for full power: Adjustable, 4–200ns ± 10%.

– Max. switching frequency for constant power: 1 MHz.

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

Probe attachment

– Outer diameter of bracket: ø 25 mm

– Weight: 650 g

In / Out Puts

Figure 17 Keysight DS1121A Bidirectional Fault Injection Probe Inputs and Outputs (Top Side)

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	High Precision Electromagnetic Probe	Connector for the Base Unit. To perform EM measurements.
3	Coil current	SMB, 50 Ω Analog output. -2.0 V .. 0V. A voltage proportional to the current through the coil for monitoring purposes. Usually connected to an oscilloscope.
4	Digital glitch	SMB, 50 Ω Binary active high input. A probe fires a single EM pulse if the voltage gets over 2.4 V.
5	Pulse amplitude	SMB, 50 Ω. Analog input, 0 .. 3.3 V. Defines proportional EM power level 0 V= 5%, 3.3 V = 100%.
6	Activity led	LED, Blink when probe fires. Illuminates proportional to digital glitch plus pulse amplitude.
7	Power led	LED, Status LED. Illuminates when Bidirectional Fault Injection Probe is powered.
8+9	GND + 12VDC	12 VDC Power supply input. Banana Plugs connectors.

Figure 18 Keysight DS1121A Bidirectional Fault Injection Probe Inputs and Outputs (Bottom Side)

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

Edition 1, October 2024

DS1121-90002

www.keysight.com