DATA SHEET

DS1120A Unidirectional Fault Injection Probe

High speed pulsed EM fault injection probe for localized glitches

Introduction

With increasingly challenging chip packages and sophisticated light-sensitive sensors to prevent optical laser faults, Keysight presents a new testing vector for fault injection scenarios. The DS1120A Unidirectional Fault Injection Probe induces fast, high power, EM pulses on a user-defined location of the chip. EM-FI (electromagnetic fault injection) testing allows bypassing traditional countermeasures and provides the next step in high-end security tests.

KEYSIGHT

Description

The Unidirectional Fault Injection Probe offers a powerful addition to the fault injection setup. The easy setup and testing make it a relatively easy and time-saving way of performing localized faults on modern chips. The Unidirectional Fault Injection Probe offers a fast and predictable pulse that meets the demands of international testing laboratories and manufacturers. The set of probes, XY table, and camera offer a complete and powerful setup that can be controlled and parameterized flexibly through the Inspector FI software. The software allows automation of testing scenarios and easy reporting for further analysis and refinements of the scenario. Like all other hardware components, Keysight offers the Unidirectional Fault Injection Probe to be used in stand-alone or custom environments as well integrated with your own hardware and software.

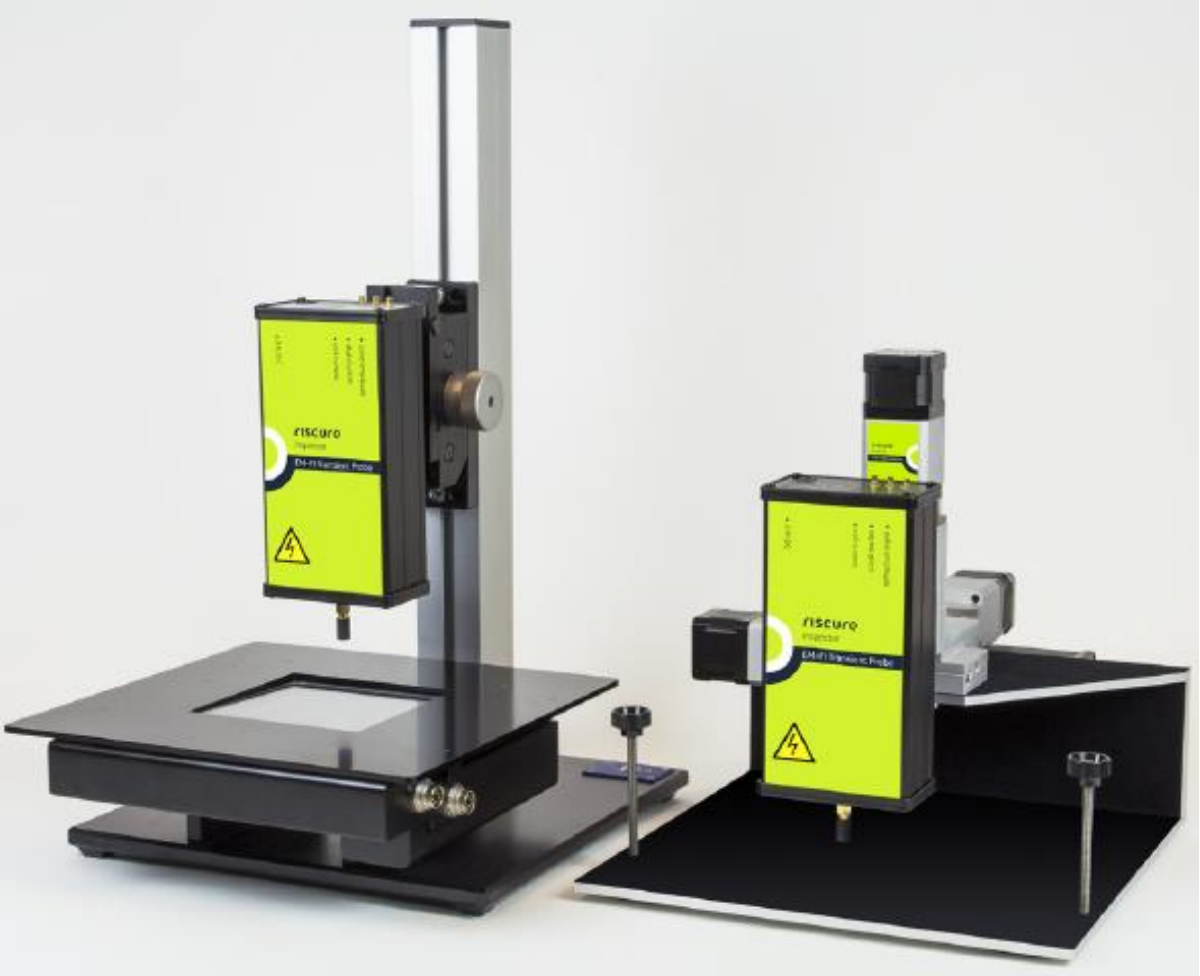

Figure 1. Unidirectional Fault Injection Probe

Key Features

- Does not require de-packaging the chip.
- EM glitches are not detected by light sensors meshes.
- Flips value of logic cells on target device.
- Lower chance of permanent chip damage compared to laser glitching.
- Adjustable high-power pulses.
- Different coils included to generate different EM fields over a chip.
- Optional camera for precise and careful probe positioning.
- Fast and short pulses configurable from software.
- Fast and predictable response to trigger.
- Fits Keysight EM Probe Station and Fault Injection Laser System for automated scanning.

XYZ Positioning

The probe is supplied with a holder which fits to the EM Probe Station or Fault Injection Laser System stand. Optionally the Unidirectional Fault Injection Probe can be supplied with either Keysight DS1010A Precision XYZ stage to position the probe through the Inspector software and perform automatic scanning. Existing customers can use the holder to upgrade their set-up without purchasing additional XY hardware.

Integrated with Inspector or Standalone

Inspector integration: The Keysight DS1160A Smartcard Voltage and Clock Glitcher controls the timing and power settings of the probe EM pulse, and performs triggering, synchronous power measurements for card communication. For embedded devices, Inspector supports a multitude of devices and protocols to generate an environment suitable for your testing setup. A current probe or power probe is recommended for power monitoring of the embedded device. The stage and camera connect to the Inspector FI software for navigation and automated surface scanning. The solution can further be extended with DS1002A Pattern Based Trigger Generator to trigger faults and to prevent a device from breaking down after an EM attack.

Standalone: The Unidirectional Fault Injection Probe can be integrated with any fault injection test software and hardware. The stage and camera are optional in this case; they too come with an SDK.

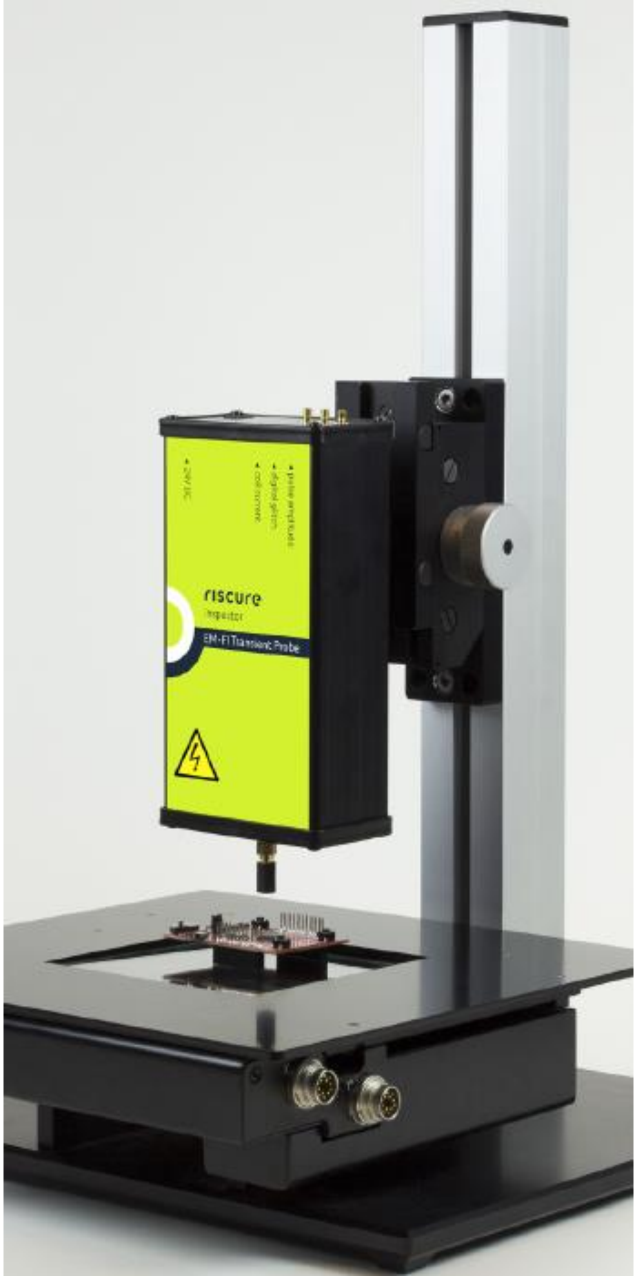

Figure 2. Unidirectional Fault Injection Probe

Application

The Unidirectional Fault Injection Probe is designed to test devices of the latest generations. Used on a daily basis in the Keysight Security Evaluation Lab, we make sure it meets the highest demands of both the industry and security analysts. This way, we ensure the device to be effective in testing both smart card and embedded based products. We have proven that the effects of hardware and software countermeasures available in up-market devices can be challenged successfully. Fine control over all parameters used to execute a Fault Injection scenario in our software and programmability means ensuring a high degree of security in the product under test.

User Control

The user controls the following parameters from the Inspector FI software:

- Flexible multi-glitch testing.
- Automated testing with randomized or fixed parameters: offset, repetition count, timing.
- Digital scaling of probe power.
- Automatic scanning range.

Unidirectional Fault Injection Probe versus Fault Injection Laser System

For the Unidirectional Fault Injection Probe, removing the packaging is not required to induce a fault. The EM pulse will be traveling through the non-metal material that is used to encapsulate the chip. This saves time and energy for the security analyst, but it will also introduce some uncertainty of how the actual glitch is carried through. With the Fault Injection Laser System, it is necessary to remove the packaging, but it provides more reliability and ease of navigation on the chip’s surface. Removing the packaging for Unidirectional Fault Injection Probe is a good option for organizations that do white box testing or where repeatability is key.

Laser Effects

The laser photons generate free electrons in the P- and N-channel of transistors. As a result, the conductivity of any transistor inside the laser spot increases and transistors switch to ‘ON’ state. Conductance of both transistors of a P- and N-channel pair causes short circuiting between VDD and GND which may damage the chip. The laser located above M2 and M1 changes the status of M1 or M2 or both, which depends on laser’s wavelength and pulse strength.

On a lower level, rather than short circuiting FETs as lasers, the faults induced with Unidirectional Fault Injection Probe cause the flux to change in a particular part of a circuit changing the state of the FETs. This behavior has also proven to be less destructive for devices saving precious samples and work while performing a testing scenario.

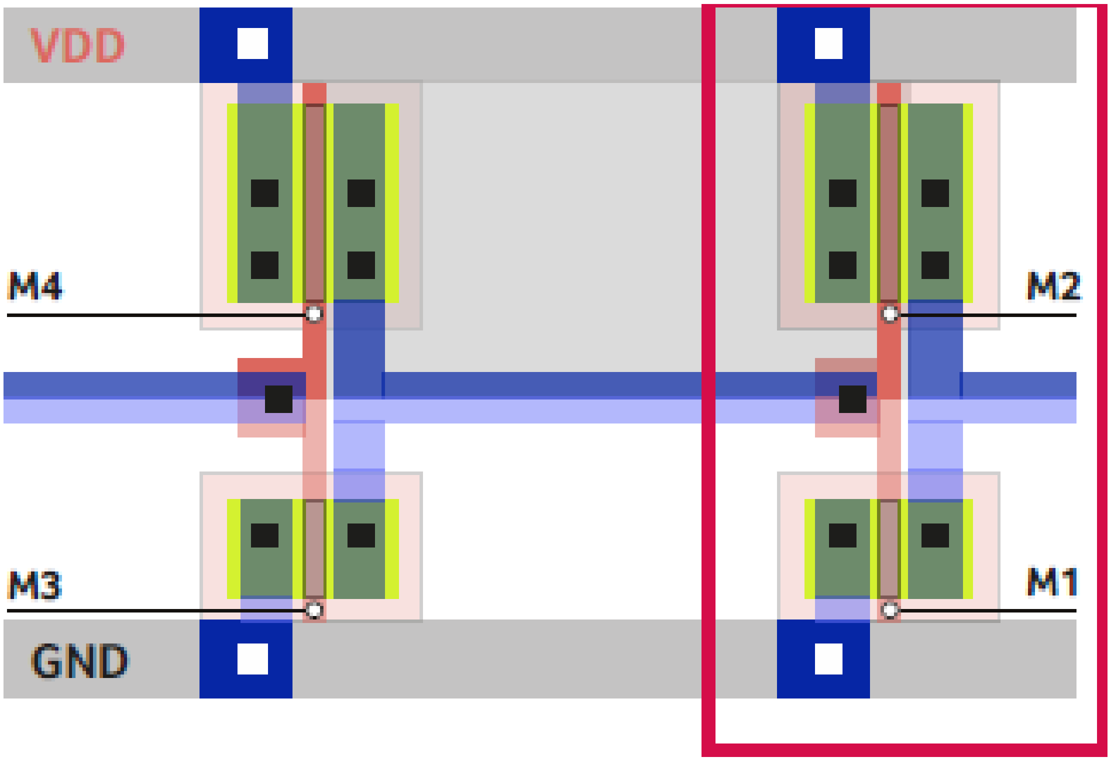

Figure 3. VDD and GND

Unidirectional Fault Injection Probe Effects

Unidirectional Fault Injection Probe may follow various principles: magnetic transient pulses or harmonic power injection. The Unidirectional Fault Injection Probe generates magnetic pulses. The magnetic pulse induces a voltage glitch in any circuit loop under the coil. The voltage glitch may change a transistor status from ‘OFF’ to ‘ON’ or vice versa depending on the polarity of the voltage glitch and type of transistor. The voltage glitch will only switch one transistors of a P- and N-channel transistor pair to ‘ON’ and therefore does not cause short circuit between VDD and GND. The effectiveness depends on loop area A and time derivative of magnetic field B. The relation is shown below:

$$U = A \times \frac{\partial B}{\partial t}$$

Figure 4 gives an example of a circuit layout. The coil located above M2 (coil not shown in the figure) induces voltage glitches separately in two loops: the loop outlined in red and the loop outlined in orange. Since the loop area in red is much bigger than that in orange, the one loop in red will get most effective glitch.

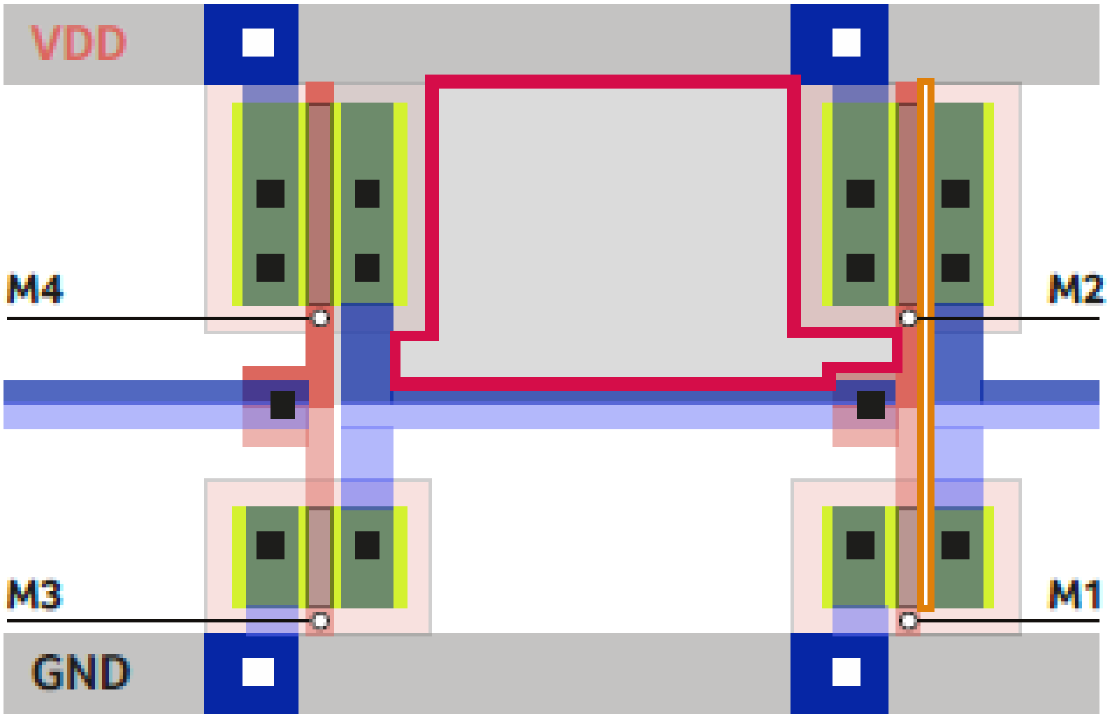

Figure 4. Example of a circuit layout

Characteristics

Figure 5 shows Unidirectional Fault Injection Probe behavior under different conditions with a 1.5 mm positive polarity tip. In each picture, the first line is digital glitch on the “digital glitch” input; the second line is the voltage measured over “current monitor” from Unidirectional Fault Injection Probe with 90MHz low pass filter with the “pulse amplitude” set at 0.33 V corresponding to 10% power. The third line is the voltage over the measurement coil (model name EM 6995 1 cm loop H-field sensor by Electro-Metrics) with the ‘pulse amplitude’ set at 0.03 V corresponding to minimal power.

The fixed delay between trigger signal and the EM glitch (see Note 5 and 6) is introduced by the electronic circuit. The trigger timing (T1) and trigger width can be set by users while pulse start T2 and T4 and pulse end T3 are fixed relative to trigger start T1. The strength of EM Glitch can be set by users by setting the voltage on “Pulse amplitude-1” input. The technical specifications are shown in Figure 5. Figure 6 shows pulse pattern at maximum repetition frequency of 1 MHz.

Without a Low Pass filter an oscillation on the waveform at approximately 300 MHz is observed. The oscillation is due to the oscillation between the ground of the EM-FI probe, see Figure 7. This is the measurement artifact. The oscillation is not present in the EM pulse.

The current pulse of the 4 mm tip is weaker and longer due to higher inductance of the larger tip coil (please refer to the Technical Specifications below). However, since the loop area of 4mm tip is six times bigger than 1.5 mm tip, the EM pulse will be stronger. For this reason, a 4mm tip is suggested when the target’s thickness exceeds 1.5 mm. Otherwise a 1.5 mm tip is suggested. The polarity of tips determines the polarity of glitch voltage induces in the TOE.

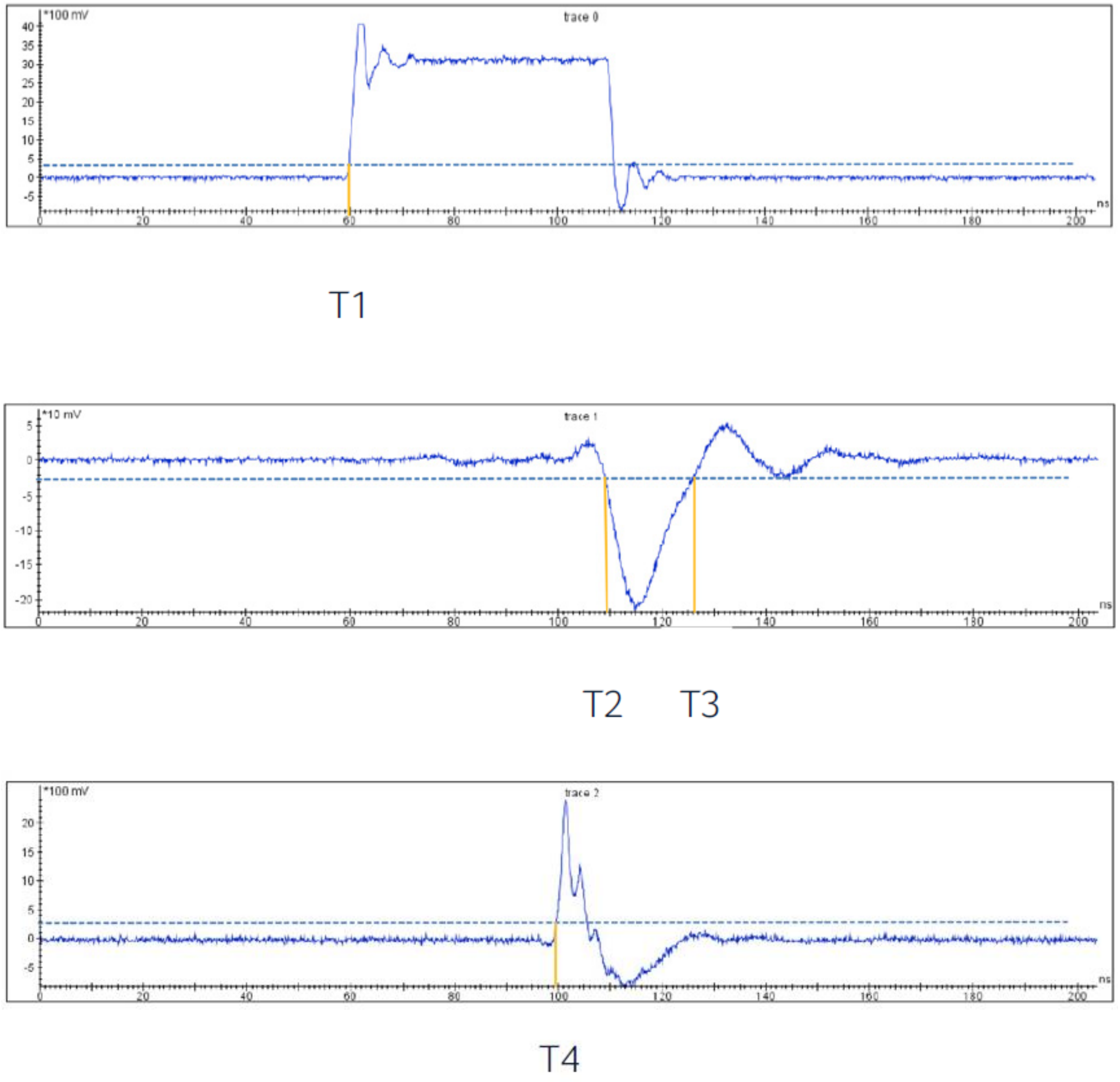

Figure 5. Unidirectional Fault Injection Probe behavior when glitch pulse width is 50 ns

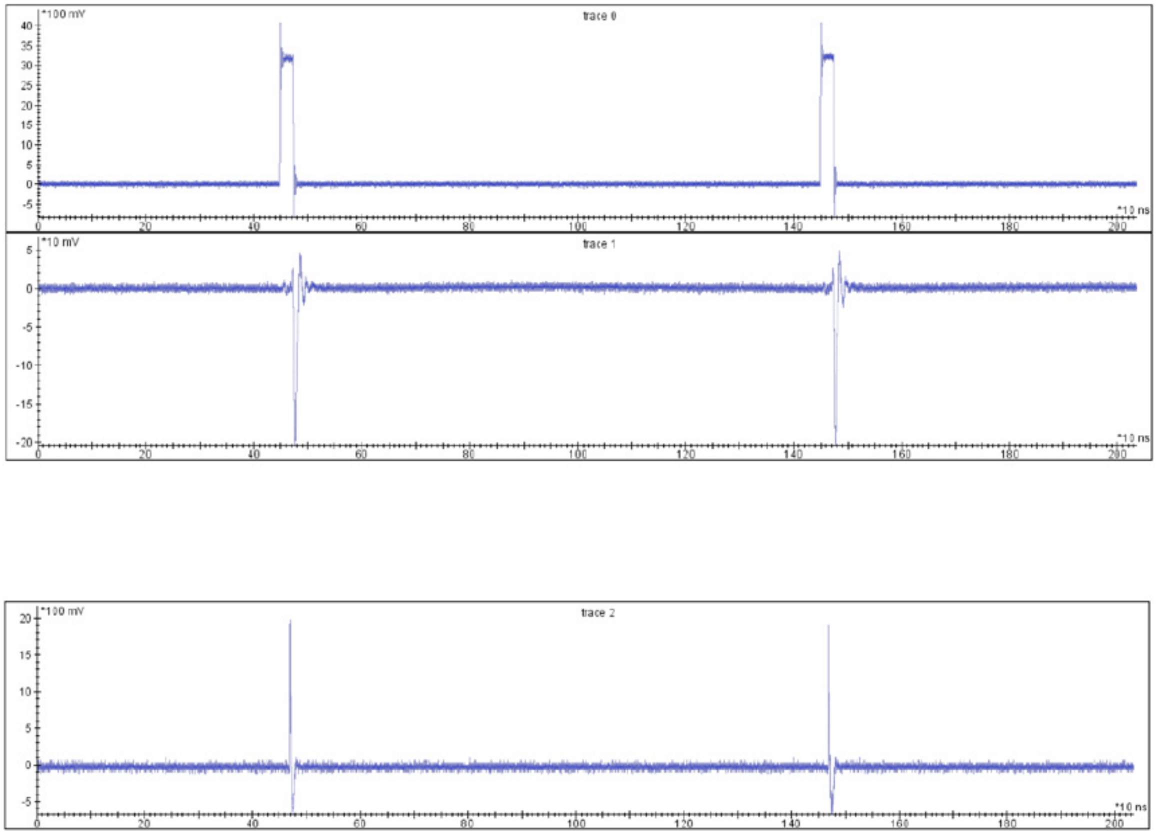

Figure 6. Unidirectional Fault Injection Probe behavior with maximal switching frequency, 2 pulses with width of 50 ns, the interval time between pulses is 1us

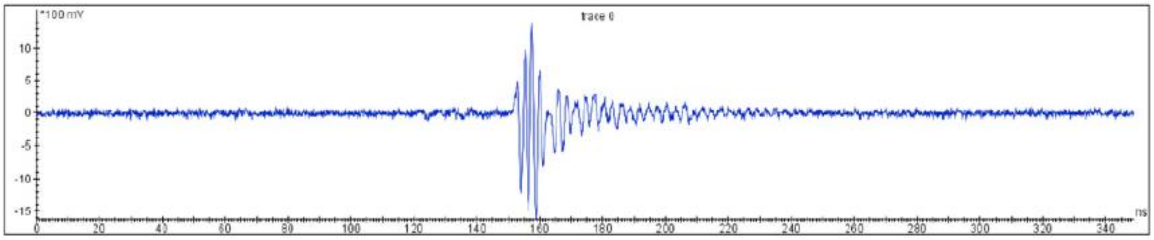

Figure 7. The output waveform of current monitor without low pass filter

Technical Specifications

Input/Output characteristics

Input/Output	Function	Min	Max	Unit
24V	Power	+24		V
Pulse amplitude[1]	Input	0	3.3	V
Digital glitch[1]	Input	0	3.3	V
Output Current monitor[2]	Output			-40 A/V

[1] CMOS to 1K Ohm
[2] Measured with 50 Ohm oscilloscope input impedance

Probe tips

Quantity	Diameter	Polarity
1	1.5 mm	Positive
2	1.5 mm	Negative
3	4 mm	Positive
4	4 mm	Negative

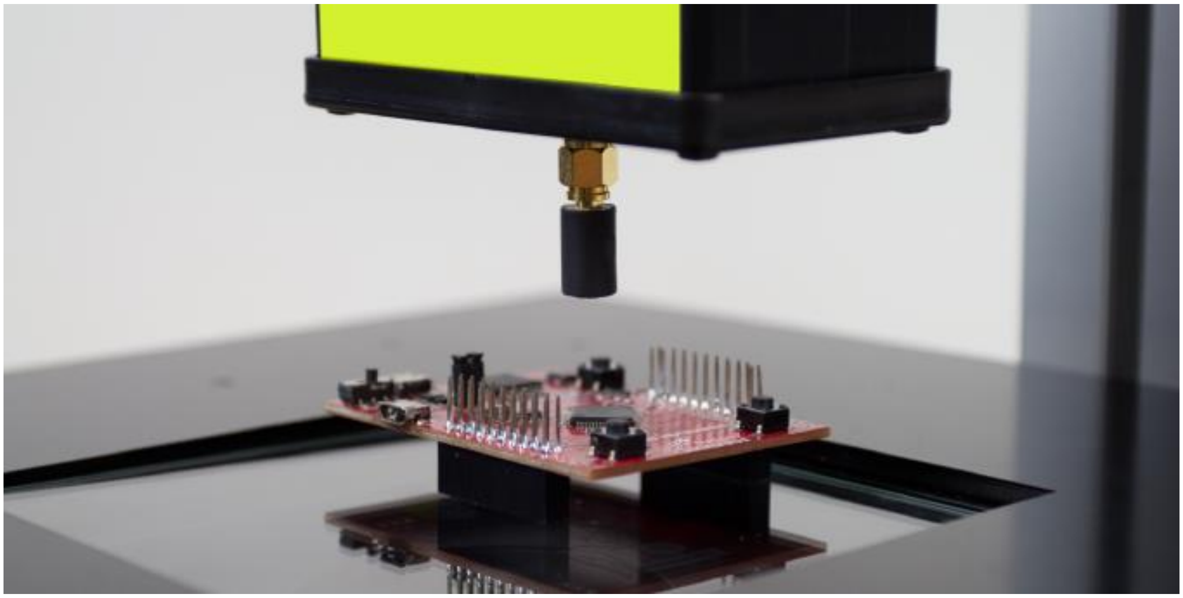

Figure 8. Unidirectional Fault Injection Probe

Characteristics

Type	Magnetic transient
Maximum voltage over coil	450 V (+/-10%)
Maximum internal current1	64A
EM pulse power control	5 – 100%
Pulse width at digital glitch input for full power	50 ns
Max switching frequency with constant power2	1 MHz
Operating temperature	0-70°C

	1.5mm tip	4mm tip
Propagation delay 13	50ns (+/-10%)	51ns (+/-10%)
Propagation delay 24	40ns (+/-10%)	42ns (+/-10%)
Max current through coil of probe tip	56 A (+/-10%)	48 A (+/-10%)
Max voltage at current monitor5	–1.4 V (+/-10%)	-1.2 V (+/-10%)
Pulse width of the waveform at Current Monitor6	17ns (+/-10%)	20ns (+/-10%)

1. Measured when probe tip is replaced by short circuit
2. Strength of 2nd pulse at least 90%
3. Propagation delay1 is defined as time difference from 10% of digital glitch to 10% of current monitor T2-T1 (see Figure 3)
4. Propagation delay2 is defined as time difference from 10% of digital glitch r to 10% of EM pulse T4-T1 (see Figure 3)
5. Measured with 50 Ohm oscilloscope input impedance
6. Pulse width is defined as time difference from 10% of current monitor amplitude’s change at rising edge to 90% at falling edge T3-T2 (see Figure 3)

The idea of EM-fault injection is to flip data bits so that it can influence a process at a certain phase. To reach such an effect, the strength of EM pulse(s) should exceed a threshold value, and the timing of the EM pulse(s) should be selected by setting trigger signal at the appropriate process phase.

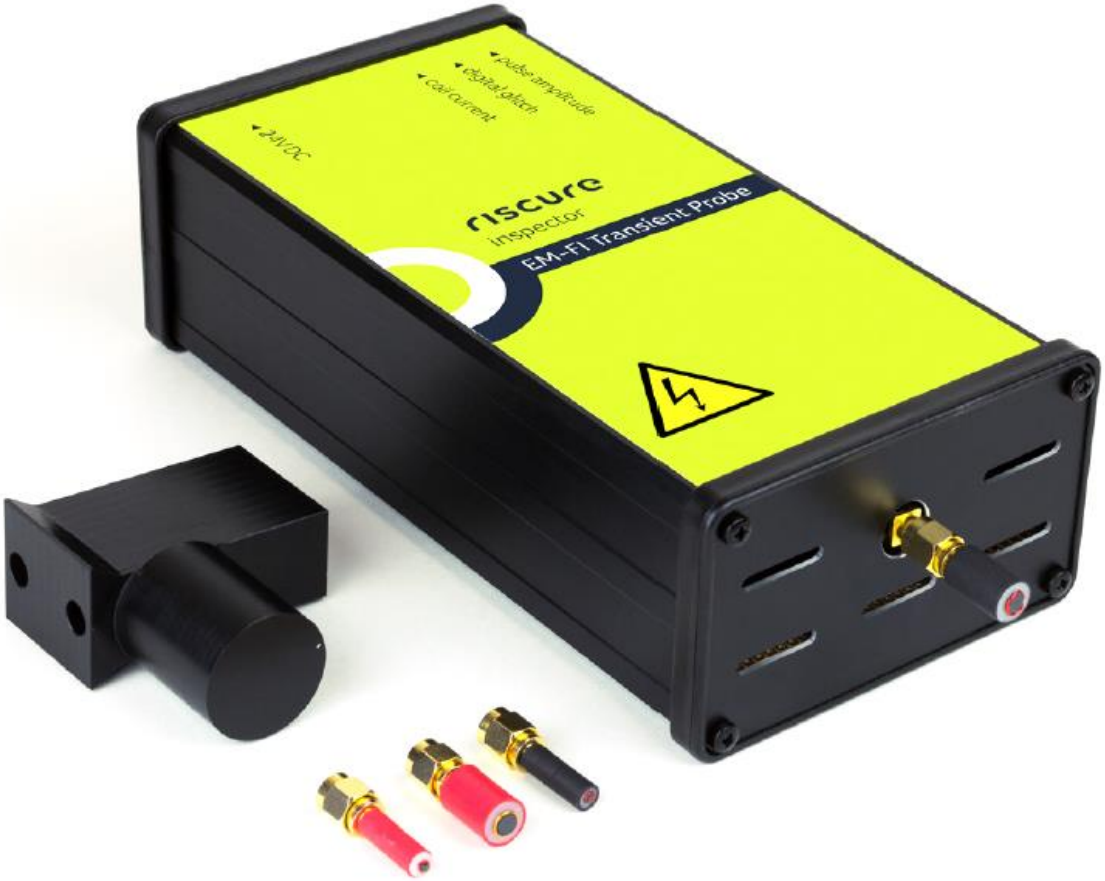

Figure 9. Unidirectional Fault Injection Probe

Published in USA, November 8, 2024, 3124-1803.EN