

DS1160A Smartcard Voltage and Clock Glitcher

Generate accurate and repeatable two nanosecond voltage or clock glitches with fully programmable pattern and control logic

Introduction

The Keysight DS1160A Smartcard Voltage and Clock Glitcher forms the heart of Inspector's fault injection architecture. Using ultra-fast FPGA technology, this device can generate faults that are two nanoseconds short while its hardware can still be programmed by the user in an easy manner. The DS1160A Smartcard Voltage and Clock Glitcher has integrated circuitry for performing voltage and clock glitching and it has an output channel for controlling optical pulses on the Keysight Fault Injection Laser.



Context

The DS1160A Smartcard Voltage and Clock Glitcher is designed to inject block glitches with programmable amplitude and duration. This enables the automated search for fault injection vulnerabilities by controlled or random variation of the glitch pattern with two nanoseconds resolution of glitch and pause duration. Using DS1160A Smartcard Voltage and Clock Glitcher, it is easy to create the ultimate fault injection test case for any smart card application.

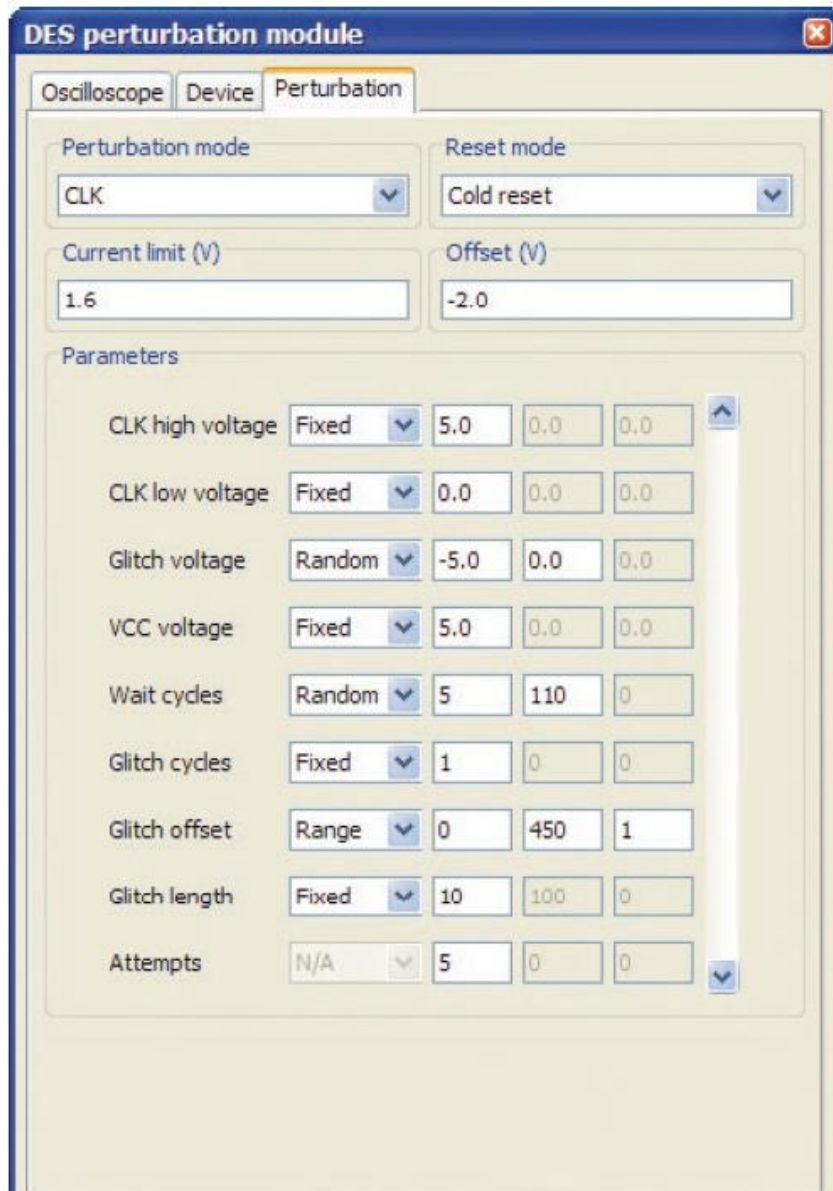


Figure 1. Setting the parameters for DES perturbation testing with Inspector

Key Features

- Very powerful tests due to integrated digital pattern generator that generates very short glitches using FPGA technology.
- Easy to create any test scenario with the perturbation instruction set.
- Reduction in testing time due to automated testing of a large set of perturbation parameters.
- Good reproducibility of tests by accurate logging of smart card behavior.
- Consistent and complete perturbation testing to reach a high level of assurance.
- Seamless integration with the Fault Injection Laser and DS1002A Pattern Based Trigger Generator.
- Card damage can be prevented using adjustable current limiter.

Before a test run, the DS1160A Smartcard Voltage and Clock Glitcher loads a fault injection program on its FPGA. This program is transparently created by the user by configuring a set of parameters as displayed in Figure 1. Although Inspector offers several examples, new fault injection programs can also be created by the user using a wizard and a dedicated fault injection instruction set. This way the user can develop any new glitch program while the tool converts and loads the program onto the DS1160A Smartcard Voltage and Clock Glitcher hardware to perform high-performance fault injection test runs.

Inspector Integration

DS1160A Smartcard Voltage and Clock Glitcher is part of the Inspector FI version. The Fault Injection Laser is the laser output extension of the Smartcard Voltage and Clock Glitcher. The triggering functionality of the Smartcard Voltage and Clock Glitcher can be extended by adding DS1002A Pattern Based Trigger Generator to inject faults based on a matching waveform.



Figure 2. DS1160A Smartcard Voltage and Clock Glitcher with a smart card inserted for testing

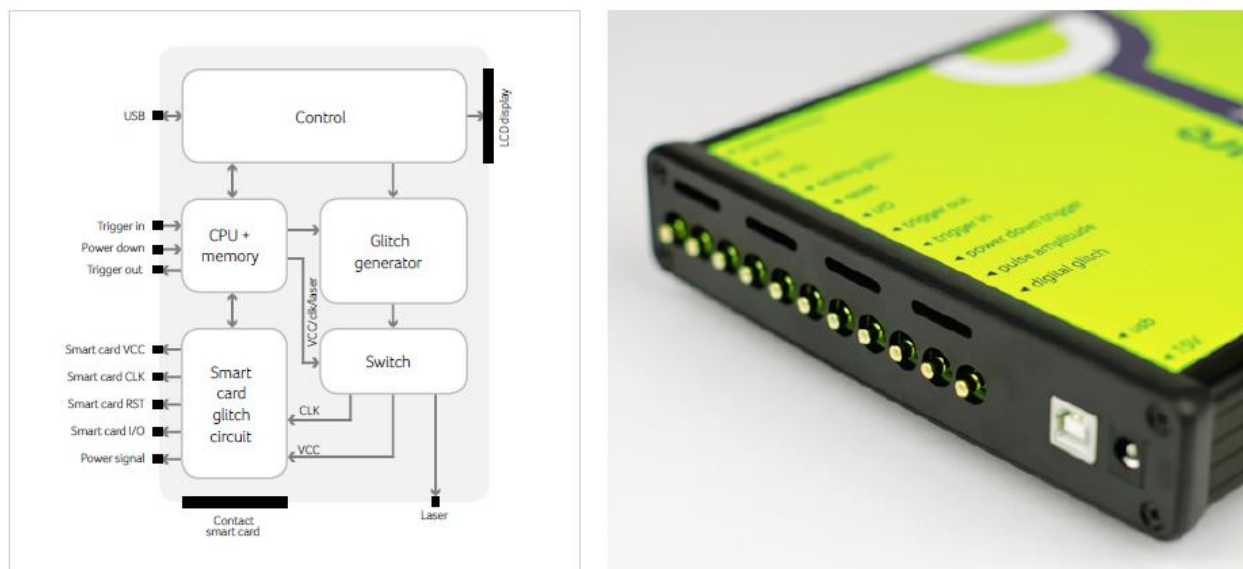


Figure 3. Conceptual overview of DS1160A Smartcard Voltage and Clock Glitch

VC Glitcher report - DES perturbation module (started 2009-08-04 15:32:21)

Wait cycles	Glitch cycles	Glitch offset	Glitch length	Timed out	Data
7	1	107	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	50	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3
7	1	30	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	105	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	9	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	78	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	56	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	34	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	94	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	99	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	14	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3
7	1	21	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	36	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	91	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3
7	1	48	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	87	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	107	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	10	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	9	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	43	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	34	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	86	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	71	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	32	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	80	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	67	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00
7	1	80	5	0	3B 07 13FF C0 80 31 80 75 52 59 73 63 75 72 65 F5 A0 04 00 00 08 04 C7 39 D7 EA FAE4 ED A3 61 08 A0 C0 00 00 08 C0 FF 2C 77 ED 02 6E B6 5D 90 00

Figure 4. Intermediate results of a DFA test run on a DES implementation; red lines show corrupted data, yellow lines a card reset

Technical Specifications

- Adjustable fault injection parameters including voltage, glitch pattern, skip cycles, glitch cycles, power level, and pulse duration.
- FPGA fault injection instruction set with over 40 instructions.
- Digital pattern generator (i.e. glitch generator), patterns of 500 samples @ 500M samples/sec.
- Adjustable current limiter.
- Dedicated CPU (FPGA technology):
 - 2kB data memory (512 × 32 bits) for storing communication with smart card and glitch parameters.
 - 4kB instruction memory (2k × 16 bits) to store the low-level glitch program.
 - Runs at 50 MHz
- Input/output:
 - Glitch outputs (digital pulse, analogue pulse and power level for laser beam).
 - Monitor outputs for power consumption, VCC, RST, CLK, and I/O signals.
 - Trigger in, trigger out.
 - Power down input (e.g. from DS1002A Pattern Based Trigger Generator)
- Voltage specifications:
 - Min / max voltage VCC, CLK (excluding glitch): 0.0V / +6.6V
 - Absolute min / max voltage VCC, CLK (including glitch): -0.8V / +7.5V
 - Min / max glitch voltage: -9.8V / +4.2V
- Smart card connector.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.



This information is subject to change without notice. © Keysight Technologies, 2024,
Published in USA, November 8, 2024, 3124-1820.EN