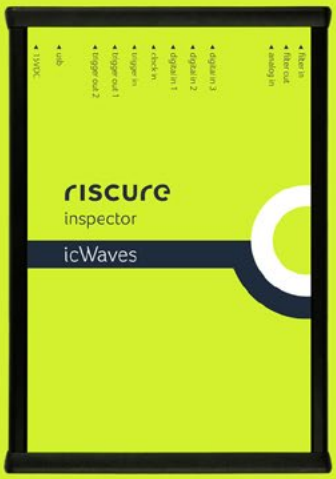
riscure

Challenge your security



icWaves

Advanced pattern-based triggering device for generating time independent pulses to avoid jitter and time-related countermeasures in SCA or FI testing.

Introduction

Generating a trigger pulse at the right point in time is essential in fault injection and side channel analysis testing. Clock jitter and random program interrupts may however make this difficult. This may result in inaccurate timing of the injection of faults. Or, when performing side channel analysis, the measurement window may be unnecessary large resulting in a slow data acquisition process, an excessive amount of data, and strongly misaligned traces. In these situations, it would be much better to detect a pattern in the signal just before the point a fault should be injected or a measurement should start.

icWaves offers a solution for this. This FPGA-based device generates a trigger pulse after real-time detection of a pattern in the power or EM signal of a chip. icWaves has a special narrow band-pass filter built in to enable the detection of a pattern even in noisy signals. The latter is important because side channel signals are typically noisy and detecting a pre-defined pattern is therefore not always feasible without a tuneable filtering mechanism. Besides triggering a fault, icWaves is also used to prevent a smart card from shutting down after detecting a fault injection attack. By detecting the wave pattern that indicates the shutdown of the card, icWaves generates a trigger to stop the shutdown process.

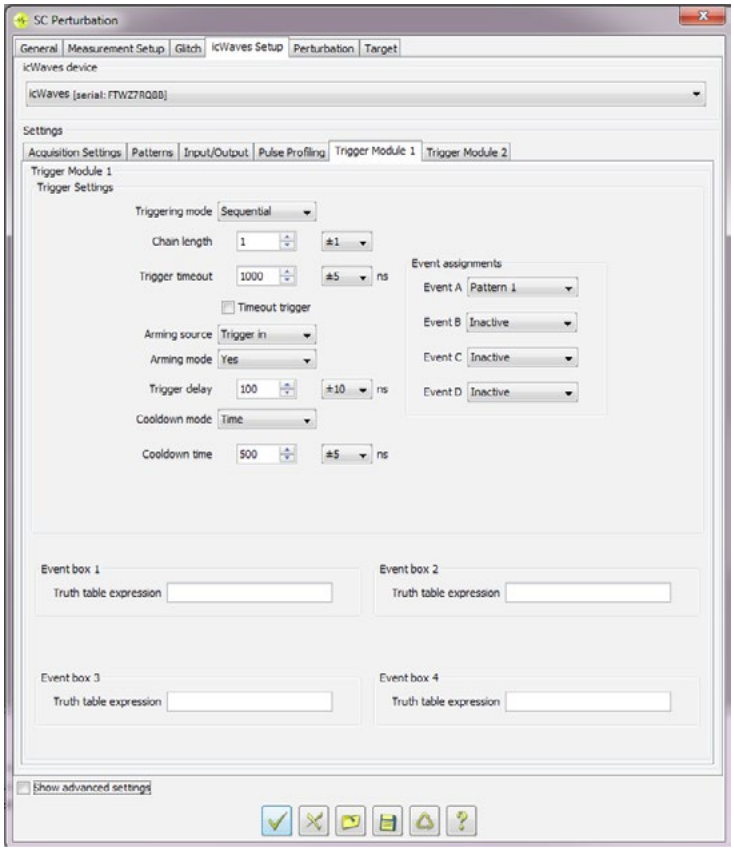


Figure 1 Configuration window of icWaves

Key features

- Offers accurate and real-time detection of any waveform to enable efficient and repeatable fault injection.
- Prevents the smart card to shut down in fault injection testing.
- Reduces the DPA acquisition window and alignment problems on smart cards with significant time variations.
- Enables side channel testing of devices without requiring access to external trigger points such as I/O or other events.
- Uses signal processing features of the Inspector software to create a suitable reference signal
- Provides simulation function for determining the optimal threshold value.
- Acquisition synchronized to internal or external clock. External clock has 360 degrees phase shift coverage.
- Hardware resampler for external clock driven acquisition.
- Digital inputs with user-defined input threshold level and configurable pulse profile tracking
- Triggering via user defined logic function based on, e.g. waveform matching and digital channel pulse profile matching.
- Pre-trigger samples for oscilloscope mode.

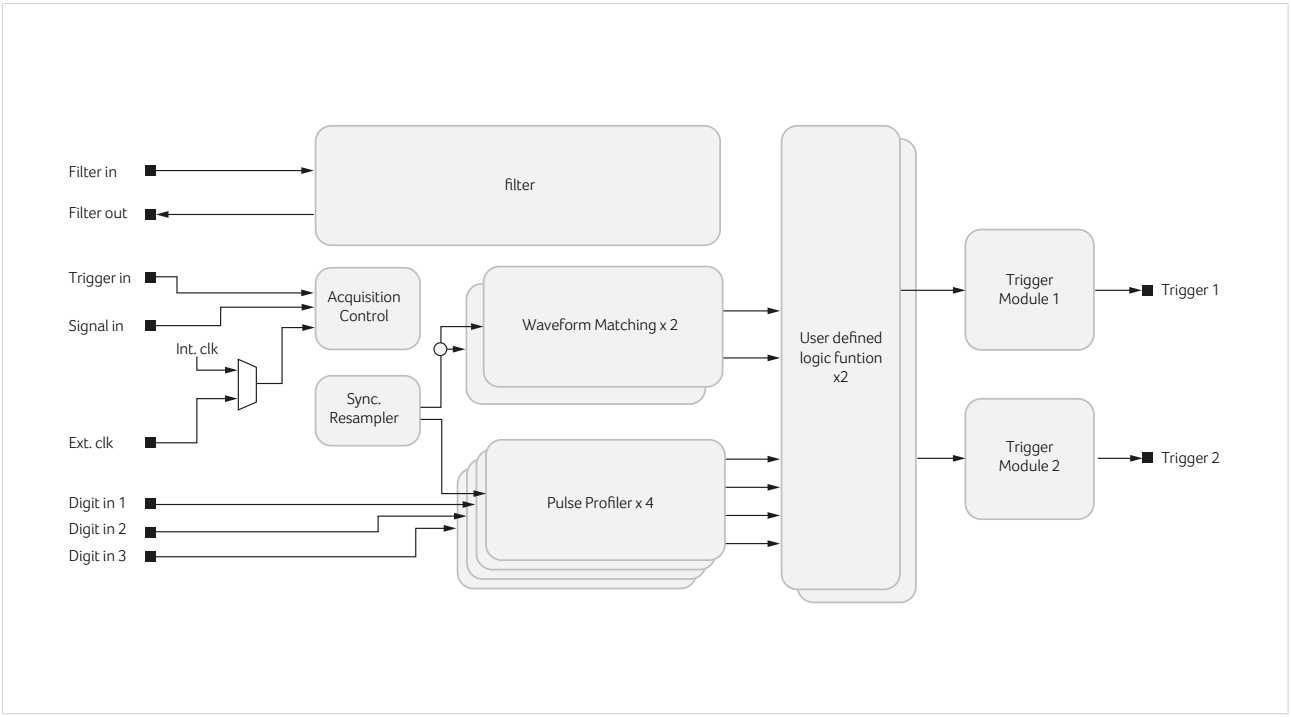


Figure 2 Conceptual overview of icWaves

Conceptual overview

The **Acquisition** block acquires the data from the signal input at 200 MS/s, when internal clock is used or at multiple of external clock frequency.

The **Resampler** block filters/combines the samples when a lower sample speed is required. In the case of external clock sampling, the samples within one clock cycle are averaged.

Each **Pulse Profiler** block monitors a digital signal over relevant features, providing functions of edge detection and precise pulse width timing. Its outputs can be used for trigger generation via logic functions. There are 4 pulse profilers in total.

Each **SAD processor** block matches the waveforms by comparing the input signal with the stored reference signal. It continuously computes the Sum of Absolute Differences (SAD). When the SAD value drops under the specified threshold the Trigger block is notified. A hold-off time can be specified to hold-off the trigger signal in order to find a better correlation. Also, SAD processor can be configured to assert pattern match only after several consecutive occurrences of the reference pattern. There are 2 SAD processors.

Each **logic function** block contains 4 different user-defined logic equations, with its variables being matching events from SAD processors or pulse profiler. The equations can be ordered in sequence or in parallel to form more complex conditions for trigger generation. There are 2 logic function blocks in total.

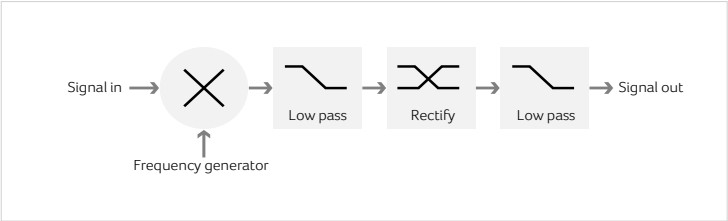


Figure 3 Filter design

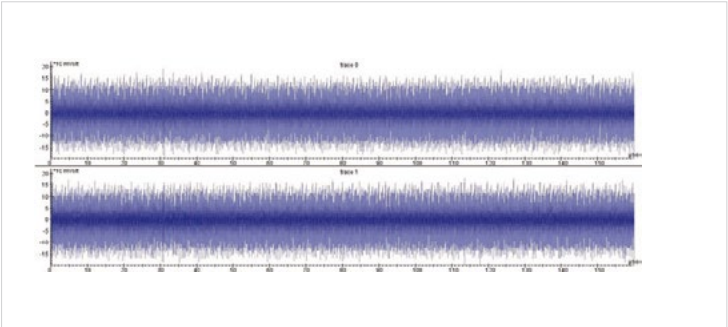


Figure 4 Example of a noisy EM signal with an unrecognisable crypto processor activity at 30 MHz

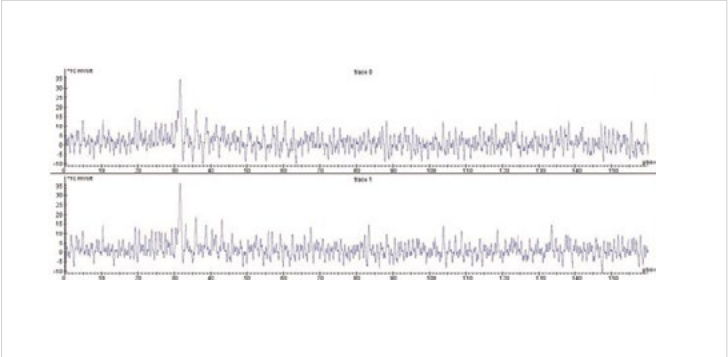


Figure 5 Example of filter out signal with recognisable activity increase at 30 µs

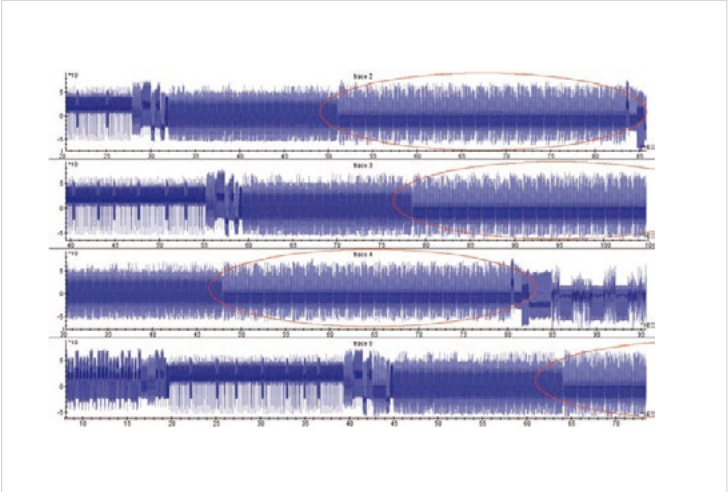


Figure 6 Example signal with large timing variation

The **Trigger** block provides some additional trigger features that can be useful for triggering on complex situation:

- The trigger can be delayed
- Parallel/Sequential triggering
- Interval between two trigger signals can be regulated
- Timeout trigger generation

The **Filter** block filters patterns out of a noisy signal. The filter block is used when:

- The side channel signal is too noisy
- The frequency range of the side channel signal is too high (e.g. because the crypto clock of the test object exceeds the sample frequency of icWaves)

As shown in **Figure 3**, the filter block consists of a mixer that multiplies the side channel signal with a pure sinusoidal signal. The frequency of this sine wave is set by the user through the software interface between 0 and 400 MHz. The mixer shifts down the frequency range of the side channel signal. The mixer is attached to a 1 MHz low pass filter. The mixer with low pass filter operates as a band pass filter with a center frequency equal to the frequency of the sine wave and with a frequency range of 2 MHz. The resulting intermediate signal is demodulated by a rectifier with 1 MHz low pass filter to avoid random phase errors. The demodulated signal is present at the 'filter out' connector and can be fed into the 'signal in' input of the icWaves for pattern detection. **Figure 4** shows an example input signal.
Figure 5 shows the corresponding output of the filter.

The input voltage range of the filter block can be set by the user through the software interface.

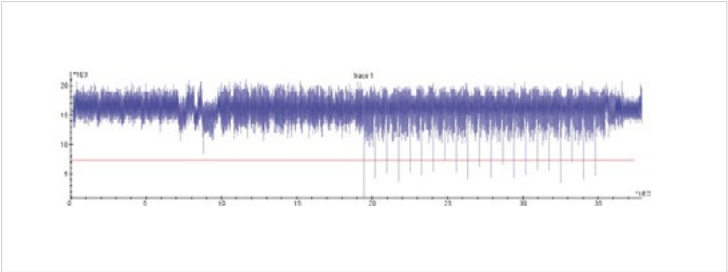


Figure 7 Selecting an appropriate threshold

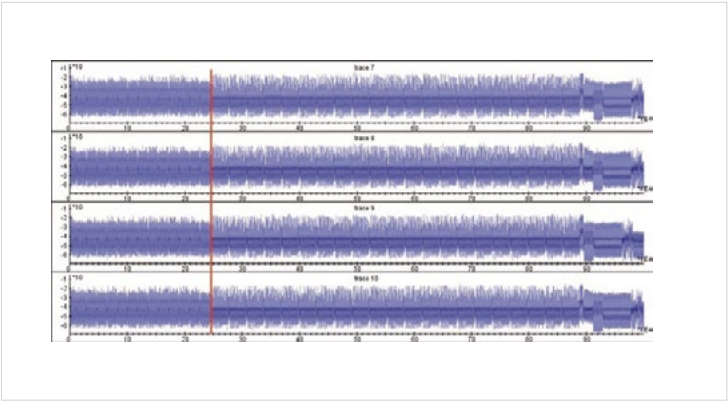


Figure 8 Example of filter out signal with recognisable activity increase at 30 µs

How to use icWaves?

A user configures icWaves for trigger pulse generation in three steps:

1. Operating as an oscilloscope, icWaves stores one or more traces in Inspector. Signal processing, such as additional filtering or averaging, can be performed on the traces using the Inspector software to derive one reference trace.

2. The user selects a distinct pattern from the reference trace. The SAD (Sum of Absolute Differences) simulation function may be used to calculate the SAD-values between the selected pattern and a test trace set. These SAD-values are used to select the most appropriate SAD-threshold for triggering.
   Figure 7 shows the result of the SAD simulation and the selected threshold (the red line).

3. icWaves can now be used as a trigger source. When the reference pattern is detected in the measured signal a trigger pulse is generated in real time. As shown in **Figure 8**, the area of interest is perfectly aligned.

Inspector integration

icWaves is controlled with the Inspector software. It is interoperable with all hardware components. icWaves works on smart cards and embedded chipsets, and supports Inspector's functionality for power and electromagnetic analysis (DPA, DEMA) and perturbation attacks with laser, voltage and clock glitches.

Frequently asked questions

My oscilloscope already provides a pattern trigger feature. Why do I need the icWaves?

Most oscilloscopes provide trigger features such as logic pattern or pulse width triggers. In many cases these features are not sufficient due to noise in the side channel signal. icWaves provides additional features designed for fault injection and side channel analysis. icWaves doesn't only look at edges or pulses in the signal. It compares the signal with the actual analog reference signal in real-time. In addition its narrow band-pass filter can be used to filter a noisy input signal.

icWaves SDK

icWaves can also be operated without using Inspector. A Software Development Kit (SDK) is provided for integrating icWaves in your custom tools. It contains a documented standard C API (Application Programmers Interface) and an example program that shows how to use the API functions. The Inspector software uses this same API, so all the icWaves features available in Inspector can also be used from your custom software.

Are 1024 samples sufficient for trigger generation?

Although the maximum of 1024 samples can seem small at first sight, it actually is more than sufficient for trigger generation. The reason for this is that several parameters are available to tune the signal to a suitable number of samples to trigger on. By varying the number of samples and the sample rate, icWaves handles pattern up to 167.8 milliseconds. In addition, for triggering on high-frequency signals the icWaves internal filter is typically used. The powerful FPGA technology in icWaves has to calculate the correlation of 1 x 1024-sample signal (or 2x 512-sample signals). At the highest supported sample rate, this is done 200,000,000 times per second.

Technical Specifications

Input/Output characteristics

Input/Output	Function	Specification		
15VDC	Power	+15V		
USB	Communication	USB2.0 High-speed		
Trigger Out 1/2	Output	Level	LV 3.3 volt	
		Pulse length	1us	
		Jitter	±120ps	
		Max I_O	128 mA in the low state; 64 mA in the high state.	
Trigger In	Trigger signal input	Threshold	Min	Max
			0	3.3 V
		Input impedance	1MΩ	
		Coupling	DC	
		Protection	+5V	
Clock In	Input		Min	Max
		Input range	0	3.3V
		Input Frequency	10MHz	100MHz
		Threshold	0	3.3V
		Duty Cycle	40%	60%

		Input Impedance	1MΩ	
		Coupling	DC	
		Protection	+5V	
		Input clock period jitter	< 20% of clock input period or 1 ns Max	
Digital In 1/Trigger In 1	Input		Min	Max
		Input Range	0	3.3V
		Input Frequency	0	10MHz
		Threshold	0	3.3V (50mV stepsize)
		Input Impedance	1MΩ	
		Coupling	DC	
		Protection	+5V	
		Other	Can be used as “Arm/Trigger In” Channel;	
Digital In 2 Digital In 3	Input		Min	Max
		Input Range	0	3.3V
		Input Frequency	0	10MHz
		Threshold	0	3.3V (50mV stepsize)
		Input Impedance	1MΩ	
		Coupling	DC	
		Protection	+5V	
Analog In	Input		Min	Max
		Input Frequency	0	100MHz
		Input Range	±62.5mV; ±125mV; ±250mV ; ±500mV; ±1V; ±2V; ±4V	
		Input Impedance	50Ω/1MΩ selectable	

		Coupling	AC/DC selectable
		Protection	5V @ 50Ω input Impedance; 20V@ 1MΩ input Impedance
		Other	Digital threshold for pulse profiling
Filter Characteristics	Output	Output Range	±250mV
		Output Impedance	50Ω
		Max Current	50mA (with 50 Ohm load)
	Input	Input Range	±16mV; ±32mV; ±64mV; ±128mV
		Input Impedance	50Ω
		Coupling	AC

Reference trace

Reference trace length	Single 1024 sample-trace or dual 512 sample-trace
Comparison Method	Real-time Sum of Absolute Differences (SAD)
Sample to trigger delay	250 ns

Acquisition characteristics

Sample Rate	Up to 200MSPS
Digital sample resolution	8 bit
Sample memory capacity	8 MB
Acquire samples before trigger	Up to 8 MB
External clock multiplier	1 - 32
External clock phase shift	0-360° with 1° resolution

Smart-Trigger characteristics

Related Input/Output	Feature	Configurable (via SDK)
Trigger Out 1/2	Cool-down time	0-100ms with 5ns resolution
	Trigger Delay	0-100ms with 5ns resolution
	Trigger counter	Up to 16-bit unsigned integer
	Trigger condition	Edge triggering Level triggering Window triggering
	Trigger mode	Sequential/Parallel triggering;
	Other	Timeout trigger generation

Filter characteristics

Bandwidth	1MHz
Centre Frequency	0-400MHz

riscure

Riscure BV

Frontier Building
Delftechpark 49
2628 XJ Delft
The Netherlands

Phone: +31 (0)15 251 4090
Fax: +31 (0)15 251 4099

E-mail: inforequest@riscure.com
www.riscure.com

ICW 11.09.2011