

icWaves

Quick Start Guide



What is in the box.....	2
What does it do.....	4
How to build a setup	6
How to verify your setup.....	8
How to control in custom applications.....	10
Help and troubleshooting	11
Technical specifications	12









What is in the box

In the box you will find the icWaves and all accessories to connect it to a computer and an oscilloscope.



Box content checklist

Qty	Description	Photo	Identifier (*)
1	icWaves 3		ICW
1	Power supply unit, 15 V DC, 2.4 A input 100 .. 240 V AC, 50 .. 60 Hz		PSU
	Power cable	Country specific	
1	Communication cable: USB-A – USB-B		USB
4	Signal cables: BNC - SMB, coax, 50 Ω , 90 cm (3 ft)		BNC2SMB
2	Signal cables: BNC – BNC, coax, 50 Ω		BNC2BNC

Qty	Description	Photo	Identifier (*)
3	Signal cables: SMB - SMB, 50 Ω , coax, 90 cm (3 ft)		SMB2SMB
2	Signal splitter: BNC-Tee Connector, 50 Ω , coax		BNC2TEE
1	Signal attenuator: 20 dB Attenuator, 50 Ω , BNC-BNC		ATT20
1	Signal filter: Low-pass filter 1.9 MHz, 50 Ω , BNC - BNC		LPF1M9
1	Connector adapter: BNC - SMB adapter		SMBA
	This "icWaves- Quick Start Guide"		

(*) The identifier is used by references in this document only.

Manufactured by

Riscure BV

Delftechpark 49, 2628 XJ Delft, The Netherlands

Phone: +31 15 251 40 90, Fax: +31 15 251 40 99

Email: inforequest@riscure.com

Web: www.riscure.com

What does it do

The icWaves is a device for real-time wave pattern detection used in Side Channel Analysis (SCA). It is capable of performing signal convolution with multiple signal patterns concurrently, and combining pattern events into triggers.

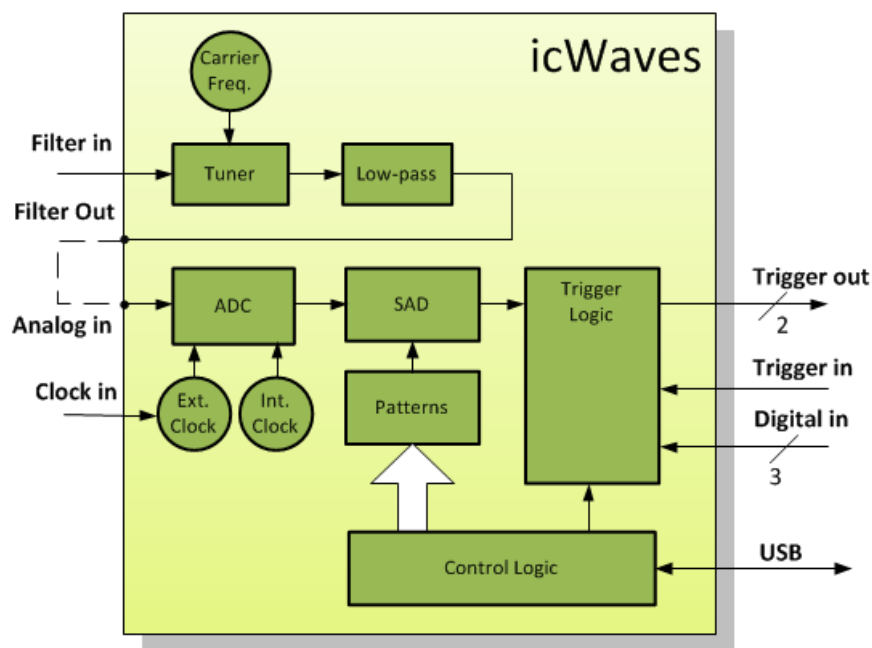


Figure 1 Functional overview of the icWaves.

The icWaves is typically applied on targets having countermeasures preventing static alignment of traces in time. Examples of such countermeasures are random processing delays and non-static processor clocks.

The icWaves comes with a optional filter stage, an analog to digital converter (ADC), a convolution processor (SAD) and programmable logic for generating triggers.

The filter stage has a tuner (or frequency shifter) to extract signals around a frequency of interest.

The icWaves is normally used with the Inspector suite of software.

Example of a pattern based use case

When an acquired signal almost resembles the reference pattern, the output value of the SAD-processor shows a dip.

A recognition event is signalled if this output value gets below a threshold value. A next acquired sample may improve the recognition, so a preemptive hold-off is implemented to wait for a better, lower SAD value.

When no further recognition events takes place, the hold-off state times-out and a counter is incremented. After a predefined number of counts (or a counting time-out), an external trigger can be generated.

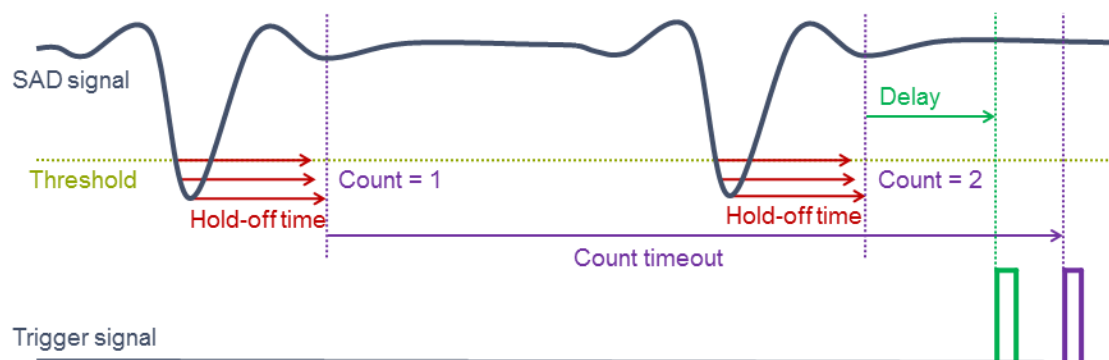


Figure 2 Simplified overview of timing condition parameters for a trigger signal.

In Figure 2 the external trigger (green) is generated by intention after detecting the second occurrence of the reference pattern. If there is no second detection, the trigger (purple) is generated.

How to build a setup

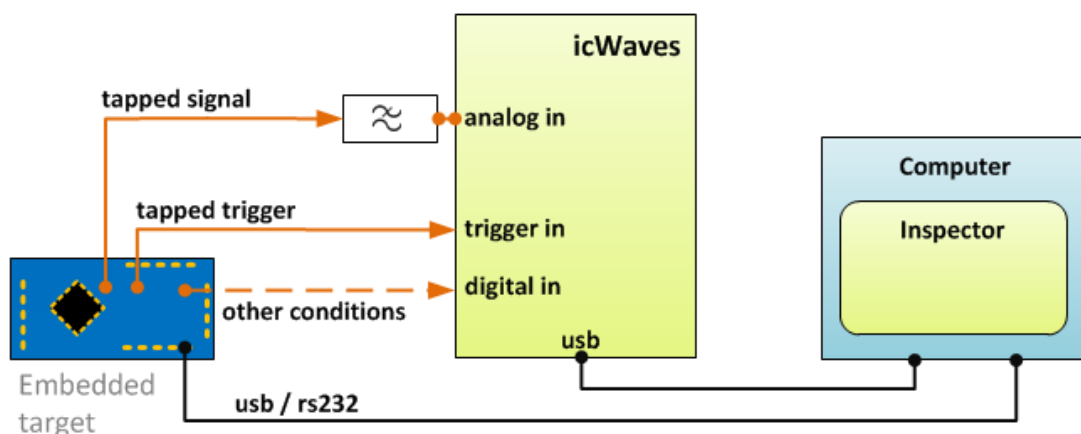
Purpose

Applying the icWaves requires two stages of setup:

1. A setup to record a reference trace and select a **marker** pattern.
2. A setup to record data traces triggered by a **certain occurrence of the marker**.

Basic setup for marker acquisition

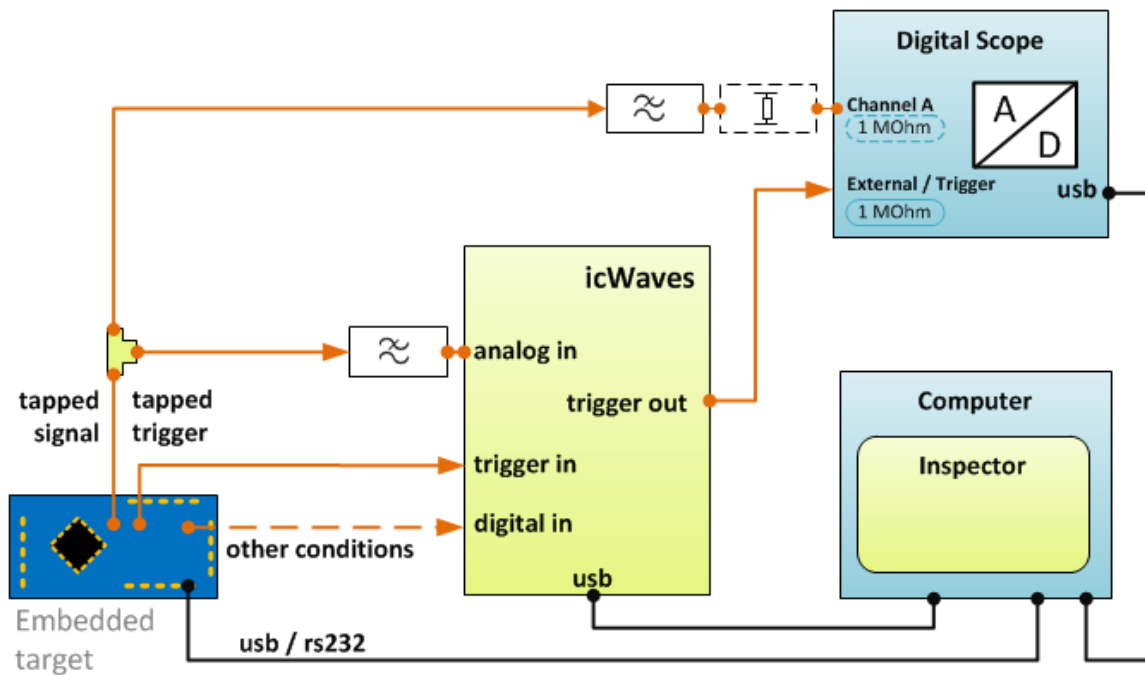
In this setup, Inspector uses the icWaves as an oscilloscope device which performs the acquisition and produces signal traces.



The operator selects a time fragment of interest (marker) in a reference signal trace and programs that fragment as a pattern in the icWaves.

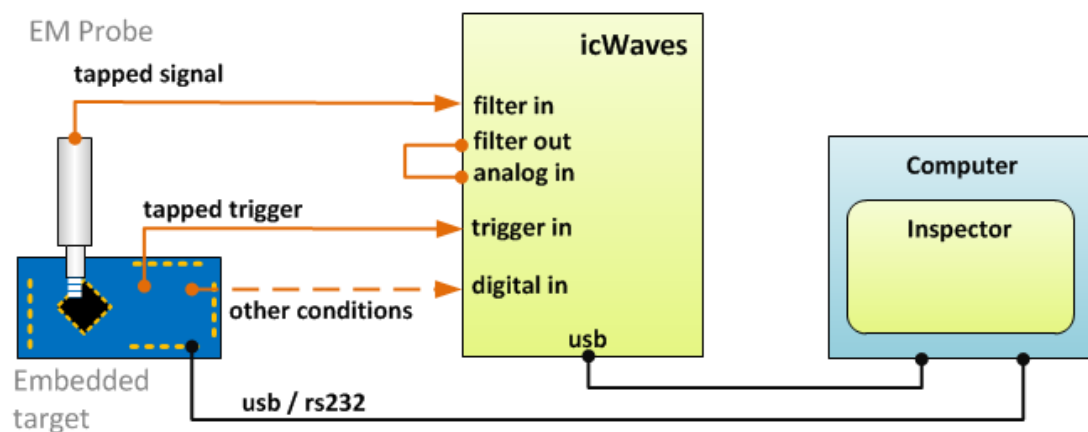
Basic setup for smart triggering

In this setup the digital oscilloscope is performing the acquisition, and the icWaves is generating the trigger signal to record a signal trace.



Alternative setup for marker acquisition in noisy signals

In this setup the tapped signal is routed first through a narrow bandpass filter to isolate the signal from noise.



How to verify your setup

Is the icWaves powered?

If the icWaves is powered, the display will show the product version and copyright message.



Figure 3 Example of the power-on message of the icWaves.

Is the icWaves recognized by Windows?

If a powered icWaves is connected to the computer for the first time, its USB drivers will be installed, if not done before, and registered.

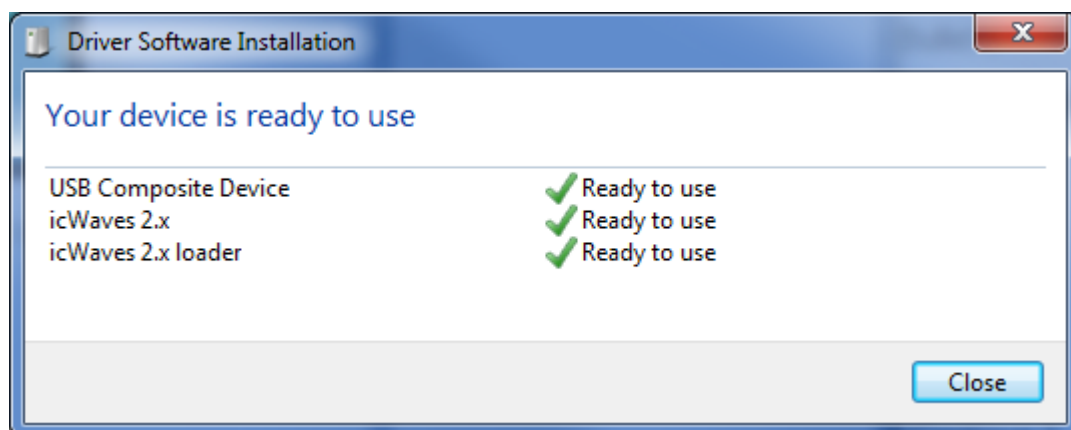


Figure 4 Example of first time icWaves driver installation dialog.



The icWaves 3 will also register itself as icWaves 2 for backward compatibility.

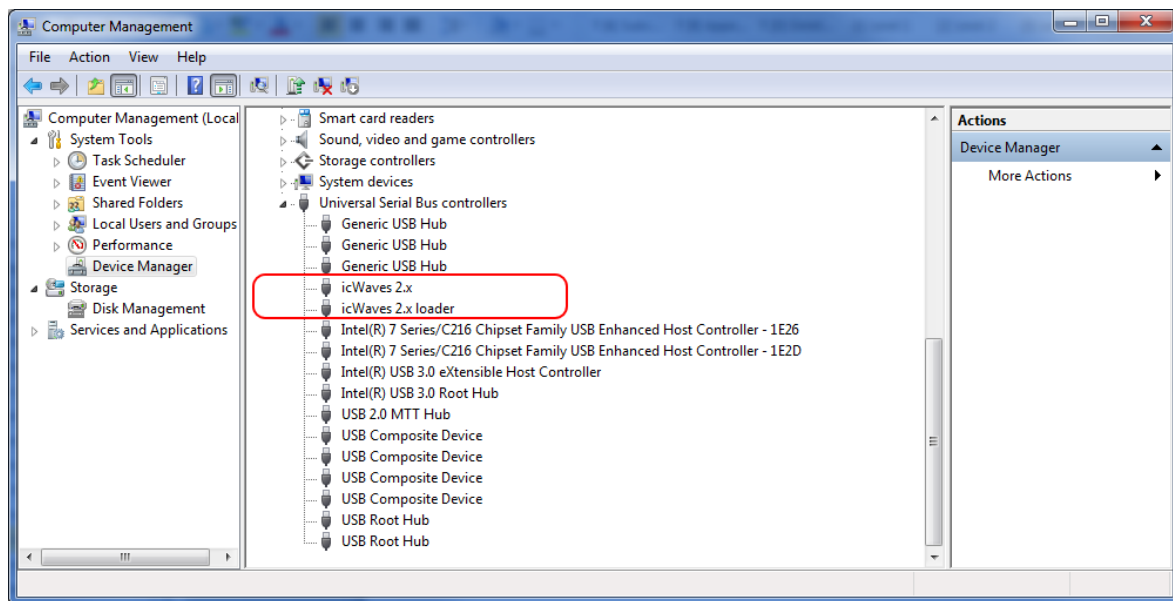


Figure 5 Highlighted drivers registered for icWaves in the Windows' Device Manager.

How to control in custom applications

Setup for application development



Figure 6 Using the SDK to communicate with the icWaves.

icWaves SDK

Use the icWaves Software Development Kit (SDK) if you want to communicate with icWaves in your own application.

The SDK is a software package containing code libraries that implement the icWaves Application Programming Interface (API).

The API provides building blocks that enable your application to exchange data with the icWaves and the smart card.

The SDK contains:

- Full documentation of the API;
- Header files and library files to be linked with your C/C++ source code;
- Python script files with examples of API usage;
- icWaves USB device drivers.

The current Windows version supported by the SDK is Windows 7.

For more information, visit the Riscure Support Portal, <https://support.riscure.com>.

Help and troubleshooting

Common problems



Connecting USB
cables

First connect the USB cable with the computer, **then** power the icWaves.

The icWaves is not working.
The LCD display shows full
progress bar:



CAUSE: The icWaves has not been initialized correctly. This may happen when power or communication to the device is lost during the initialization.

SOLUTION: The icWaves needs to be re-initialized with factory settings.

Please contact support.riscure.com.

icWaves initialization

Inspector tools and software are continuously improved. Newer Inspector versions expect certain parameters to be reported by old hardware too. This problem of backward compatibility is solved by a process called hardware initialization.

Still have questions?

1. Go to the Inspector Help menu, and read detailed information on the icWaves device.
2. Visit the Riscure internet support portal: <http://support.riscure.com>.

Technical specifications

Operational conditions

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



Do not block the ventilation holes of the icWaves. A blocked air flow may cause malfunction or break down.



Maintain stable environmental conditions (temperature, humidity, airflow, EMC shielding etc.) in order to reliably repeat tests and compare test results.



Turning OFF the icWaves is not required, but recommended when not used for an extended time.

Power supply

- 15 V DC, nominal load 400 mA.
- Center-positive plug, inner-Ø 2.5 mm, outer-Ø 5.5 mm.



Use of a PSU other than supplied by Riscure is not supported. Power spikes may cause internal damage and loss of accuracy.

Filter unit

- Extraction of signals within ± 1 MHz of carrier frequency.
- Internal carrier sine wave, configurable 1 MHz - 400 MHz.
- Analog input, 4 selectable ranges (± 8 mV, ± 16 mV, ± 32 mV, ± 64 mV).
- Input impedance 50 Ω .
- Low pass filter 2nd order, 1 MHz.

Acquisition unit

- Digitization of analog signal, 8 bit resolution.
- Analog input, 7 selectable ranges (± 62.5 mV, ± 125 mV, ± 250 mV, ± 500 mV, ± 1 V, ± 2 V, ± 4 V), switchable AC/DC coupling.
- Input impedance switchable 50 Ω (default)/1 M Ω .
- Input overvoltage protection, 5 V @ 50 Ω , 20 V @ 1 M Ω .
- Selectable use of internal or external sampling clock.
- Internal sampling clock 200 MHz.
- External clock input 10 MHz .. 100 MHz internally multiplied 1 .. 20 x.
- Configurable realtime sample value averaging.
- Single acquisition trace max. 8,000,000 samples.

Waveform detection unit

- Detection based on Sum of Averaged Differences (SAD) calculation followed by a progressive local minimum detector.
- Detector is capable of running in single or dual concurrent pattern mode.
- Pattern maximum size, 512 samples (single mode), 256 samples (dual mode).
- Detection of pattern 1 can fire trigger out 1, detection of pattern 2 can fire trigger out 2 etc.

Trigger unit

- Three Digital Inputs (DI1 - DI3) and one Trigger Input (TI) can be used to combinatorially define events. Trigger logic can be programmed to fire Trigger Out on parallel or sequential occurrence of events.
- Inputs, 0 .. +3.3 V, DC coupled, 1 M Ω impedance, overvoltage protection 5 V.
- Configurable threshold level for logic HIGH 0 .. +3.3 V with resolution 50 mV.
- Positive/negative minimum pulse width 25 ns.
- Capable of pre-trigger (recording samples following the trigger event) and post-trigger (use recorded samples preceding the trigger event) handling.
- Trigger logic can time-out after being armed and no trigger events occurred.
- Trigger logic can apply an inhibit period after a trigger event occurs.

- Trigger logic can be armed by software, with a configurable edge of Trigger In, or as long as Trigger In is HIGH.

Product case

- Dimensions L x W x H: 220.00 x 169.50 x 34.63 [mm], 8.661 x 6.673 x 1.363 [inch].



Port	Label	Description
A1	-	LCD Text display. 2 lines of text for messages.
B1	filter in	SMB. 50 Ω. Analog input (128 mVp-p). Signal to be filtered.
B2	filter out	SMB. 1 MΩ. Analog output. Filtered signal. This port is usually connected to B3.
B3	analog in	SMB. 50 Ω (default)/ 1 MΩ. Analog input. (0 .. 3.3 V). Signal source for recognition of wave patterns.
B4	digital in 3	SMB. 1 MΩ. Binary input. Configurable condition used in arming the trigger logic.
B5	digital in 2	SMB. 1 MΩ. Binary input. Configurable condition used in arming the trigger logic.

Port	Label	Description
B6	digital in 1	SMB. 1 MΩ. Binary input. Configurable condition used in arming the trigger logic.
B7	clock in	SMB. 1 MΩ. Binary input. Clock defining for sampling frequency of the analog in (B3) signal.
B8	trigger in	SMB. 1 MΩ. Binary input. Configurable condition on edge or level used in arming the trigger logic
B9	trigger out 1	SMB. Binary TTL output (0.. 3.3 V). A pulse is raised when meeting a preset event pattern condition.
B10	trigger out 2	SMB. Binary TTL output (0.. 3.3 V). A pulse is raised when meeting a preset event pattern condition.
C1	usb	USB-B type port, USB 2.0. Communication link with a computer.
C2	15VDC	15 V DC Power supply input.

Notes