

# CleanWave

## Quick Start Guide








What is in the box.....	2
What does it do.....	3
How to build a setup .....	4
Help and troubleshooting .....	6
Technical specifications .....	7

## What is in the box

In the box you will find the CleanWave and all accessories to connect it to an oscilloscope.



### Box content checklist

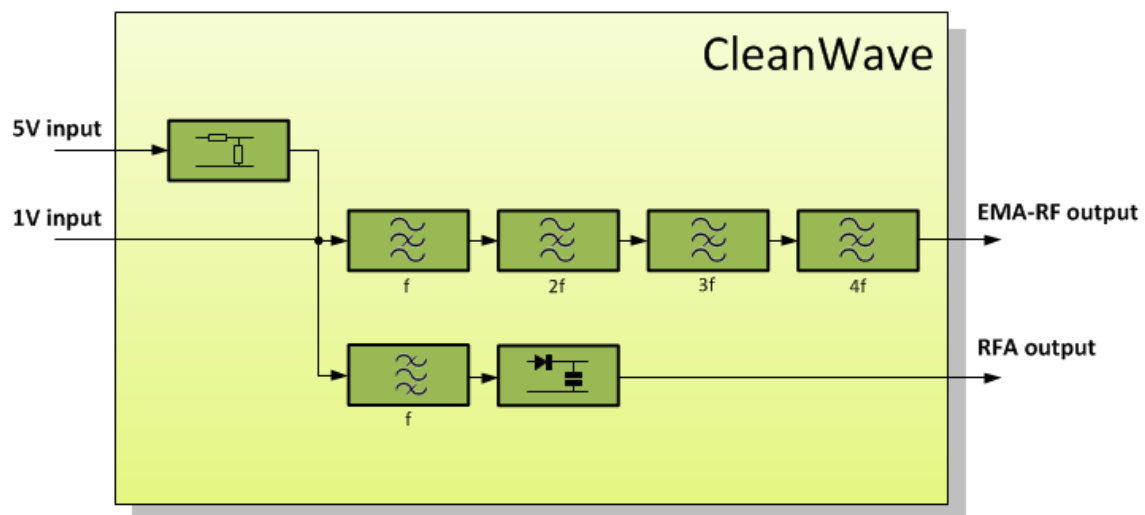
Quantity	Description		Identifier (*)
1	CleanWave		
1	15V DC Power Supply Unit, input 100 V – 240 V AC, 50 – 60 Hz		PSU
-	Power cord (included with PSU)	 Country specific	
2	Signal cable: BNC - BNC, 50 $\Omega$ , coaxial		BNC2BNC
3	Signal cable: BNC – SMB, 50 $\Omega$ , coaxial , 1 m (3 ft)		BNC2SMB
-	This “CleanWave - Quick Start Guide”		

(\*) Identifier is used for reference in this document only.

## What does it do

The CleanWave is a tool for Side Channel Analysis (SCA) of radiofrequency communication (RF) with contactless smart cards complying with the ISO/IEC 14443 standard. These smart cards use the strong RF carrier signal to derive power for their circuit.

The CleanWave extracts signals which are superimposed on the RF carrier and its side bands.



*Figure 1 Functional overview of the CleanWave.*

The CleanWave has a multi-notch filter to attenuate the common RF carrier (13.56 MHz) and its 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> harmonics (e.g. 27.12 MHz, 40.68 MHz and 54.24 MHz).

For Radio Frequency Analysis (RFA), the CleanWave has a demodulator for signals at 27.12 MHz to extract power information from changes in carrier amplitude.

## How to build a setup

### Required additional equipment:

- Micropross MP300 or MP500 contactless card reader

### Basic setup for RFA

In this setup the CleanWave extracts the RF amplitude (RFA) signal to enable side channel attacks based on the power signal.

An analyst may take advantage of any information leakage in this signal by using power analysis methods.

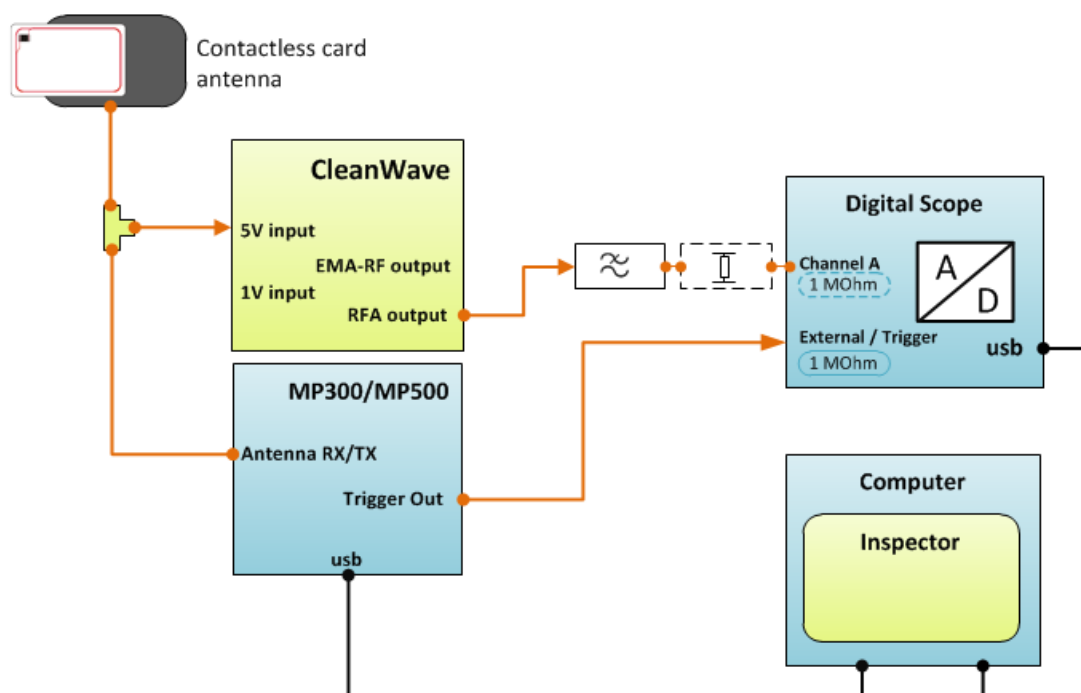


Figure 2 Side channel analysis in the time domain.

## Extended setup for EM-RF

In this setup the CleanWave suppresses the RF carrier frequency and its harmonics from the antenna signal.

An analyst can use the resulting spectrum of this 'clean' signal to detect the clock frequency of the processor, and use this information to enhance the alignment of power measurement traces to a specific clock.

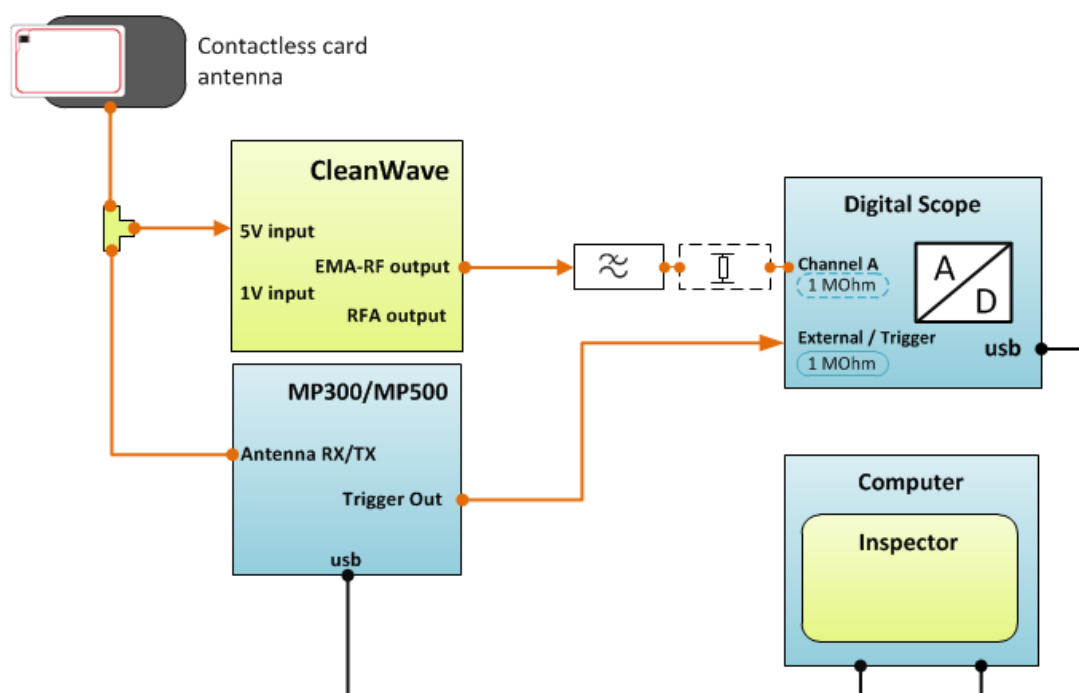


Figure 3 Side channel analysis in the frequency domain.

## **Help and troubleshooting**

### **Still have questions?**

Visit the Riscure Support Portal: <http://support.riscure.com>.

## Technical specifications

### Operational conditions

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



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



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



Unplugging the PSU from the product is not required, but recommended when not used for an extended time.

### Power supply input

- 15 V DC, nominal 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.

## 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].







Figure 4 CleanWave ports and interfaces

Port	Label	Description
A1	<b>15V</b>	15 V DC. Power supply input.
B1	<b>1V input</b>	Input for low amplitude signals (0V .. 1V)
B2	<b>overloaded</b>	Indicator LED. ON means the 1V or 5V input exceeded the range of the analog to digital converter (causing clipping and signal distortion).
B3	<b>5V input</b>	Input for high amplitude signals (0V .. 5V)
B4	<b>probe power</b>	Custom connector to power a probe.
B5	<b>EMA-RF output</b>	Output of multi-notch filter
B6	<b>powered</b>	Indicator LED. ON means the product is powered by 15V.
B7	<b>RFA output</b>	Output of demodulator.

