

riscure

Transceiver

datasheet

v1

Contents

Page 3

The story

- Why we started it
- The challenges it solves
- Unique selling points
- Who should use it

Page 8

Example use case

- Precise pattern for fault injection

Page 12

Technical details

- The techniques explained
- The package
- Technical specifications

The story



Why we started it

Observations

We started this development when we heard from users:

1. For perturbation I want to **improve input signal** for icWaves triggering in noisy situations.
2. I would like to do “**side channel at a distance**” (tempest). This applies to traditional high-end crypto chips but also to new technologies such as tags for counter fitting, IOT devices, car keys.
3. We also want an **extendible platform** for communication with wireless high level frequency chips (e.g. UHF).

Alternatives	Limitations
Low cost RF scanners (Euro 50 – 250)	Not sharp enough output signal (e.g. for triggering) because filter bandwidth is too narrow
icWaves internal filter (~ Euro 30,000)	Fixed bandwidth (1 MHz), limited range up to 400 MHz, slightly floating signal
High-end signal analyzers or measurement instruments (> Euro 150,000)	Can do the job but they offer much more than needed and it is expensive to scale over multiple test benches



So we took a device with software defined radio (SDR) and advanced it by:

1. Making a high performance connection between digital & analogue boards
2. Pre-programming the device with a bitstream for narrow-band filtering & AM demodulation
3. Pre-configuring Software Defined Radio with only the parameters you need
4. Adding tutorials relevant to side channel testing

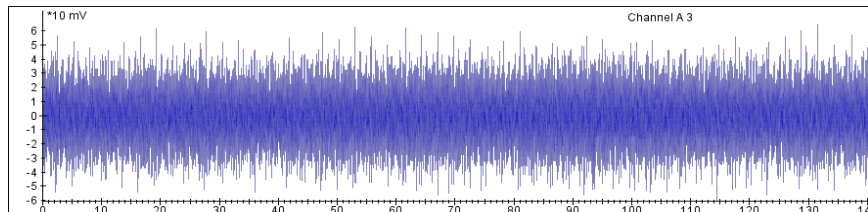
The device operates standalone and is controlled via its own software interface. It does not require integration with Inspector SCA or FI software.

By the way: it is still flexible to use for other SDR applications, it is not locked for this use case.

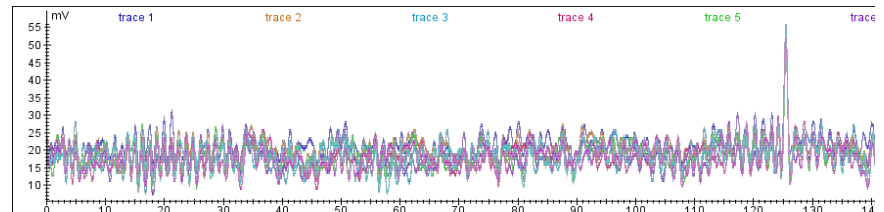
The challenge it solves

Challenges that can be solved with the Transceiver:

1. **Trigger generation in noisy scenarios**
the Transceiver can filter → real time can be used for icWaves trigger input (clear pattern).
2. **Mistakenly approve a leaky but noisy chip**
In noisy devices and chips the Transceiver can (easily) reveal signals from the crypto processor where so far only noise was seen. Applies to those devices which so far relied on obscurity by noise.
3. **Post-processing takes long**
Post-processing of traces can take e.g. 2 days. For SCA measurements that start with random delays it can bring a strong time reduction on post-processing.
4. **Dummy operations as countermeasure**
Countermeasures that rely on confusing the attacker (noise, dummy crypto rounds, etc) can be recognised real-time with the Transceiver so they lose their strength.
5. **When far-field measurements are needed**
It is sometimes hard to get near a target (e.g. shielding, active mesh). Side channel measurements at a longer distance (e.g. 10 cm – 1 m) are possible with the Transceiver's sensitivity. This moves side channel testing into the tempest domain.



Filtering real-time
with Transceiver



Unique selling points

Even higher than most
oscilloscopes



1. **Great value for money**, making this type of device affordable for every evaluator
 - Short latency for real time scenarios
 - Complete filter range
 - Bandwidth filter up to max 160 MHz
 - Demodulator for clean analogue output
2. **Little setup time** with Riscure tutorials and pre-configured SDR kit
3. Clean signals can be directly fed into icWaves for triggering in noisy environments (**analogue** output)
4. **Runs independently** – it comes with its own software

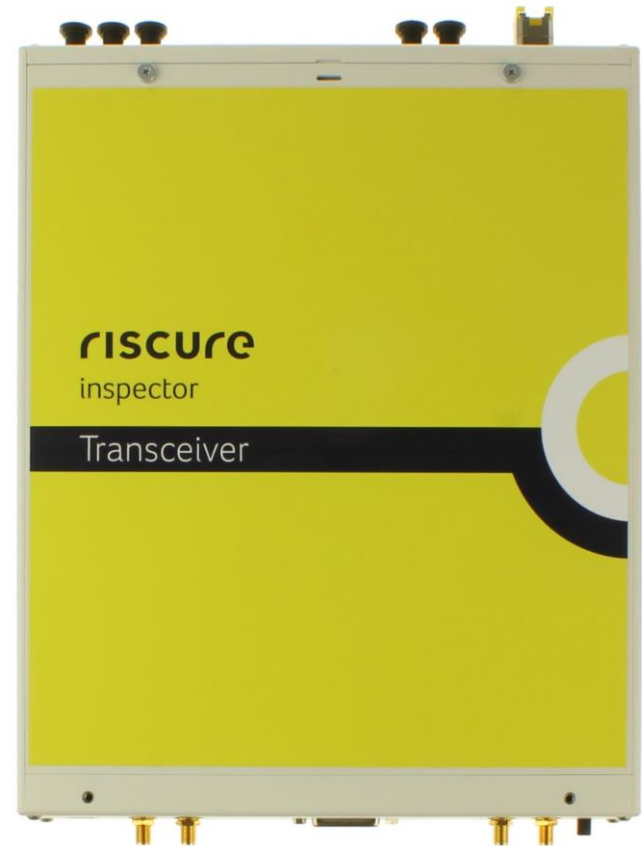
1. Filter range	Very large range: 10 MHz – 6 GHz
2. Bandwidth filter	Easy to set narrow band filter between 0.4 – 160 MHz
3. Latency	Short latency for triggering: 1 – 20 micro sec
4. Demodulator	Integrated demodulator creates stable and clean patterns
5. Output	Analogue



Who should use it?

Security evaluators that perform side channel testing on

1. **Advanced high security** smart cards
2. **Devices with tamper detection** that are hard to take near field measurements on. E.g. payment terminals
3. **System on Chips (SoC)** that are typically noisy and high performance
4. **IOT and other new** technologies with high frequencies



Example use case

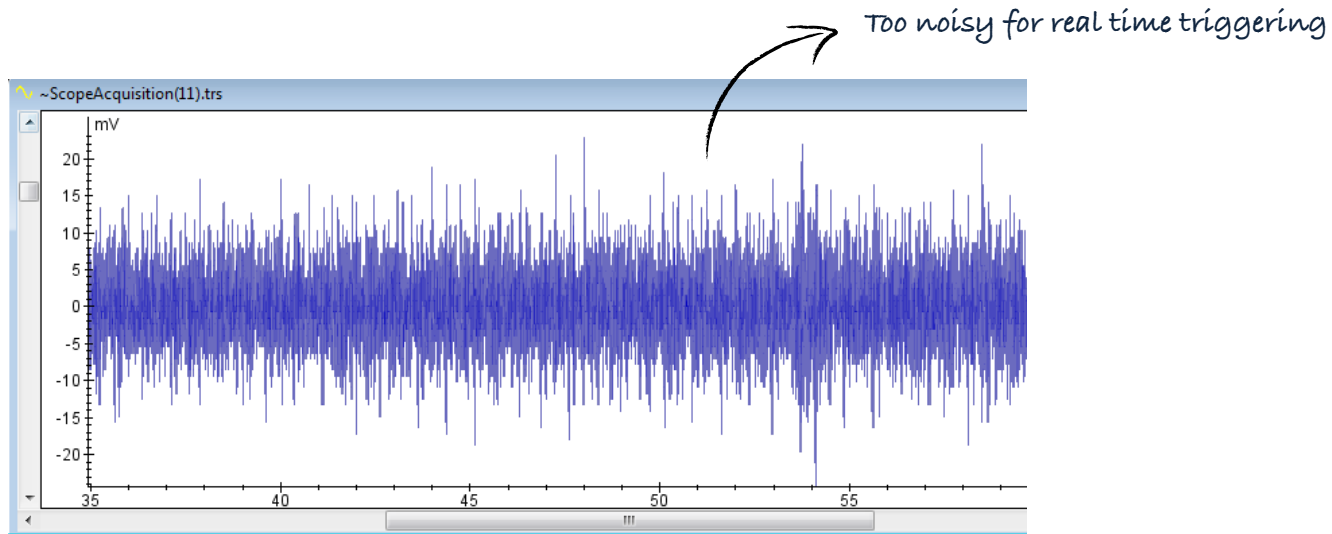


Use case – precise pattern for FI

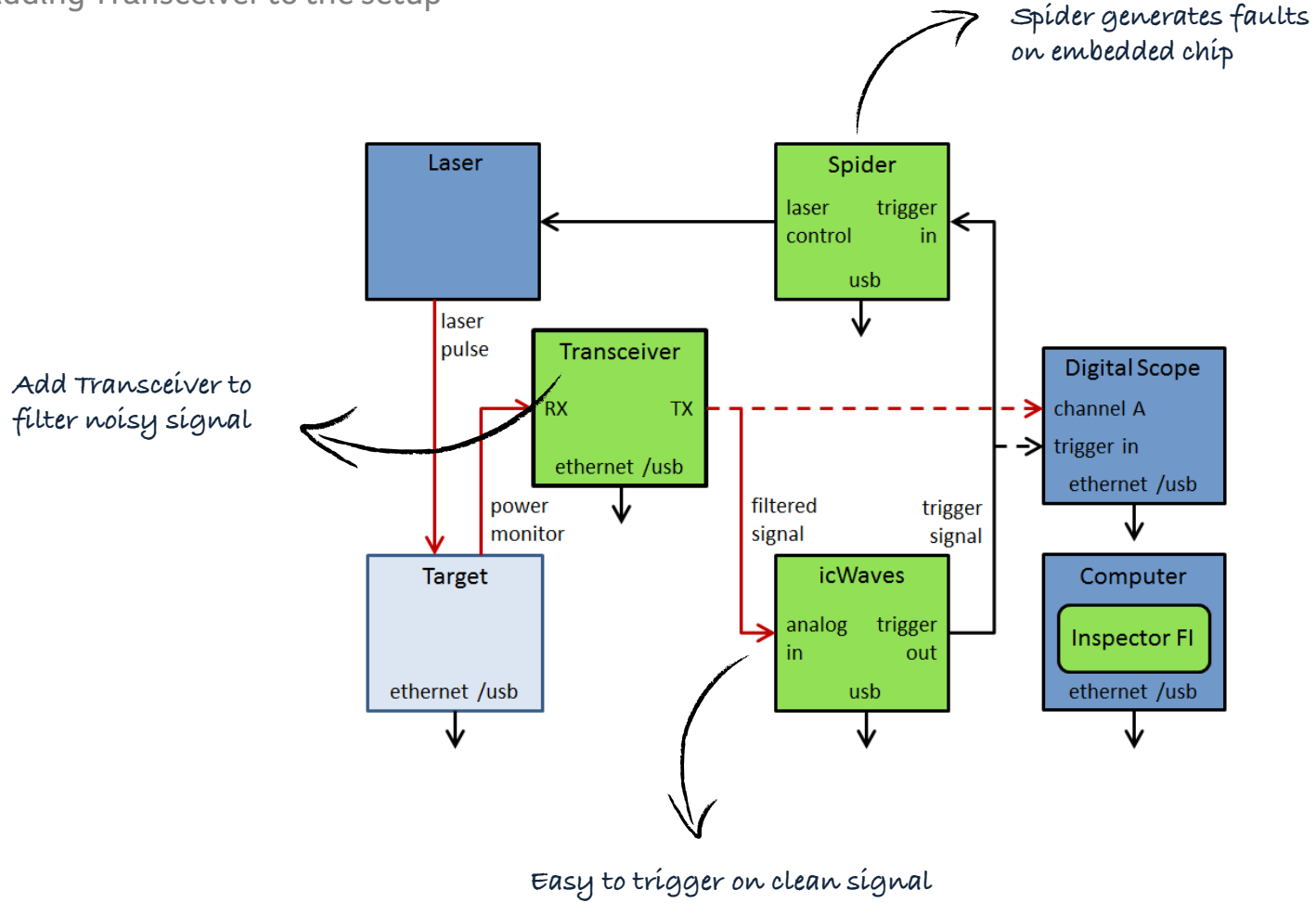
The test scenario

1. Crypto chip fault injection with diode laser on hardware AES. Running at 30 MHz, AES takes $< 1 \mu\text{s}$. We have no trigger available from the chip.
2. As a countermeasure, significant random process interrupts occur before the AES. We observe interrupts between 0 and 100 microseconds.
3. We monitor power consumption (e.g. with EM Capacitor Set) to trigger the laser. However the power signal is noisy, so hard to find a good pattern for icWaves trigger.
4. In a test project, the large parameter search space in fault injection is already a challenge. The 100 microseconds jitter makes it very inefficient and time consuming:

99% of the time you miss the AES operation



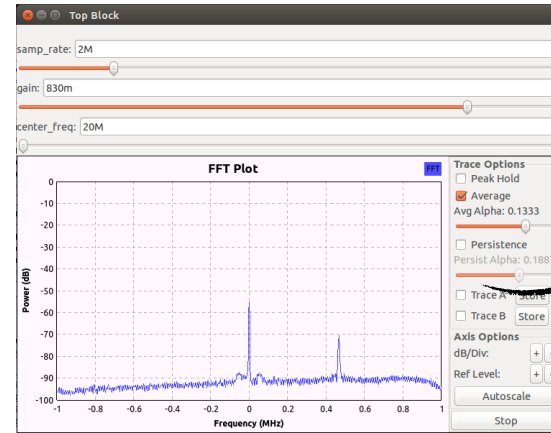
Adding Transceiver to the setup



Steps for FI testing

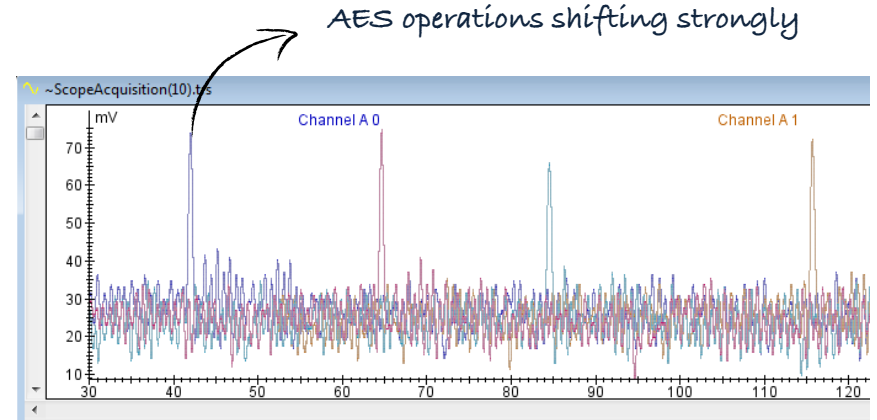
1. Tuning Transceiver

- Analyse the real time FFT plot from Transceiver for the right center frequency of random process interrupts
- Analyse output signal from Transceiver to set the right bandwidth
- Set these parameters. Transceiver filters continuously.



Tuning with FFT plot

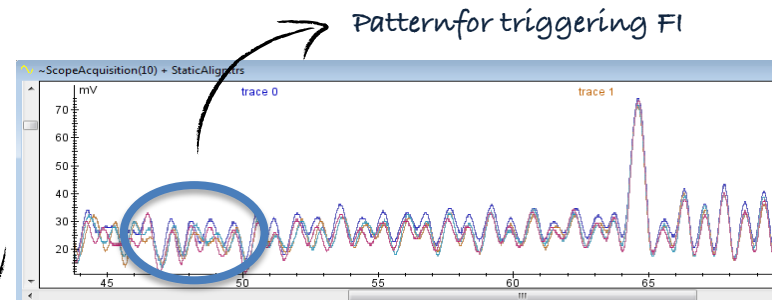
- ### 2. Capture a pattern that is now visible with icWaves, and load it for triggering a fault during the AES operation.



AES operations shifting strongly

- ### 3. Run the fault injection test cases, adjusting

- laser power
- location
- pulse duration
- timing off set
- etc



Pattern for triggering FI

From 1% to 100% hit rate on AES

Technical details



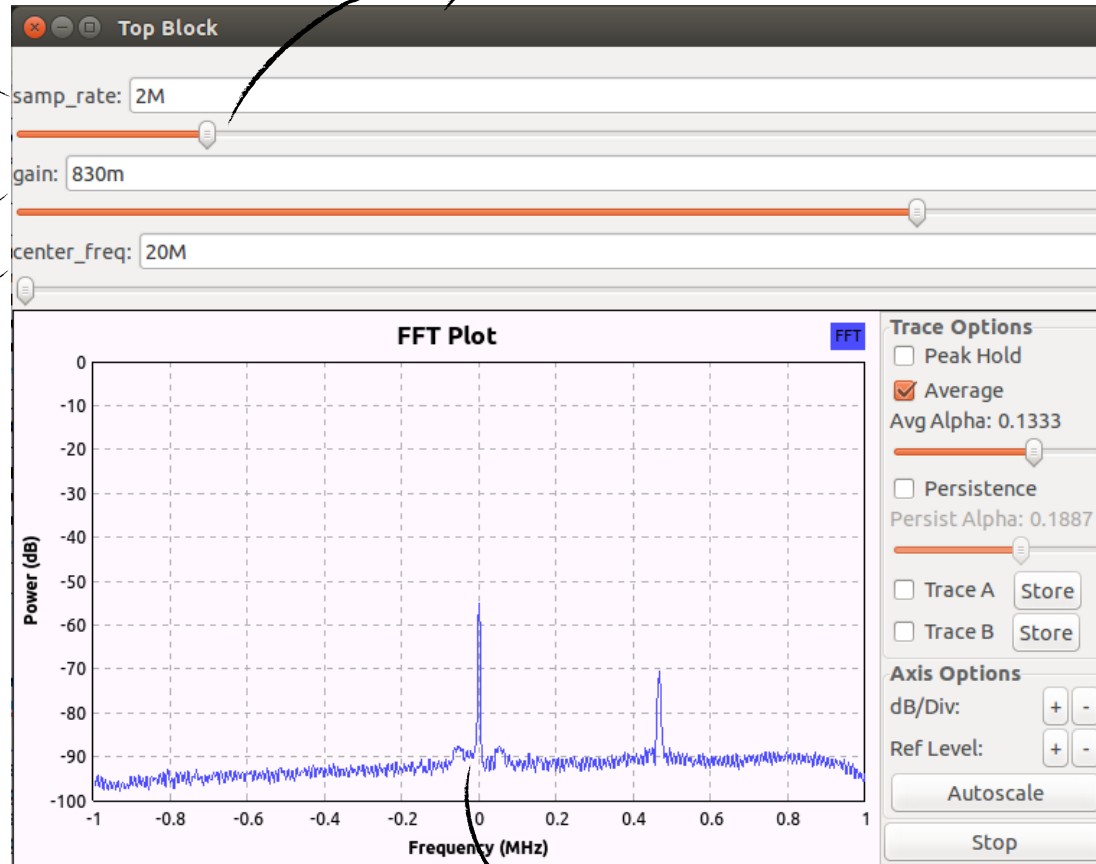
User control

Changing sliders have real-time effect

Bandwidth

Gain

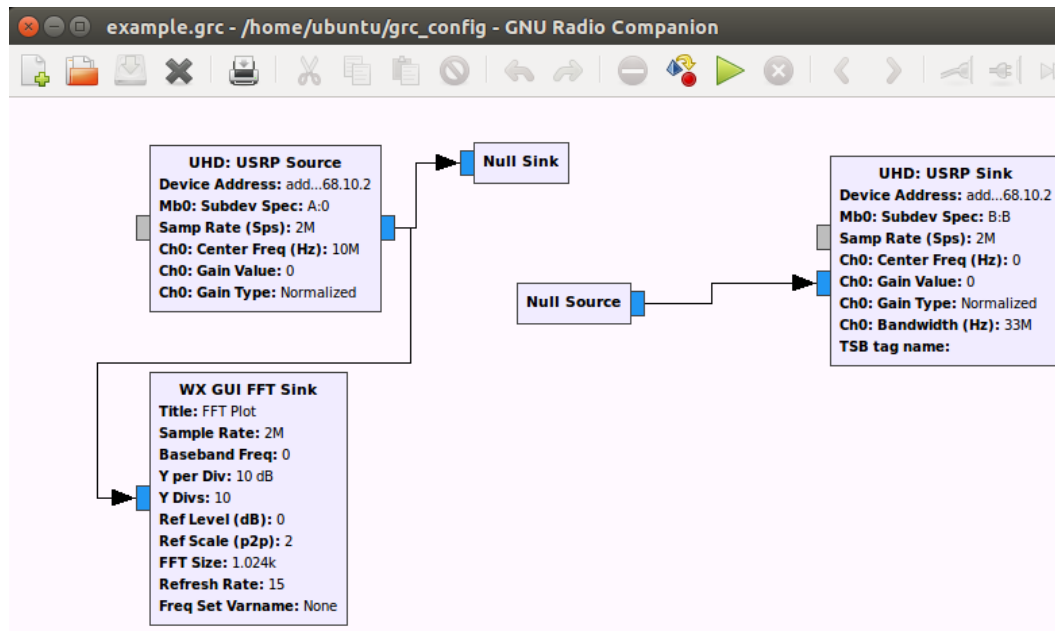
Band center frequency



FFT plot for tuning center frequency

Extendible platform

GNU radio software allows for **custom development** by the user

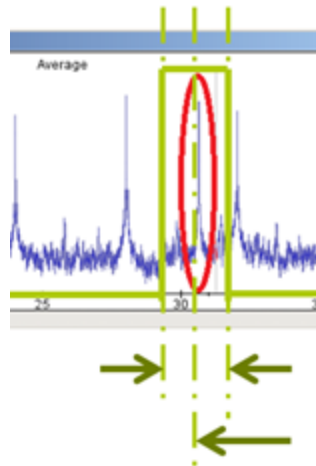


Transceiver design

The Transceiver performs two steps in real time:

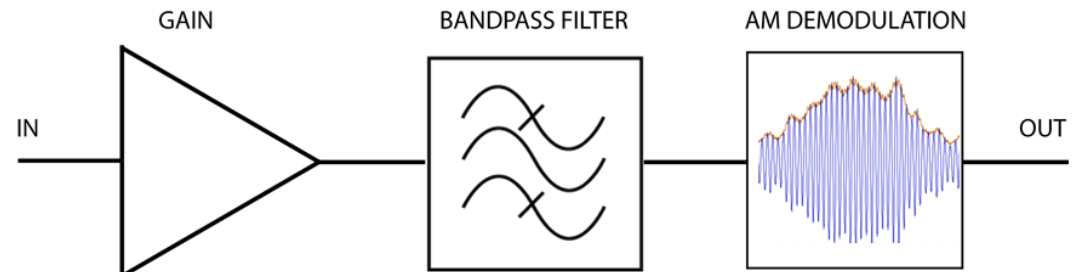
1. Bandpass filter

To improve the signal-to-noise ratio by concentrating on the frequency range of interest



2. AM demodulation

Further lowers the frequency range. This allows the signal to be processed by an oscilloscope or trigger device at a lower sample frequency and with less samples without losing information.



Technical specifications

Specs







- Input signal level: Max -15 dBm into 50 Ohms
- Input signal frequency range: 10 MHz to 6 GHz
- Band pass center frequency: 10 MHz to 6 GHz
- Band pass width: 390 kHz to 160 MHz


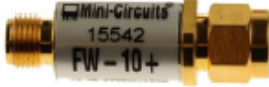
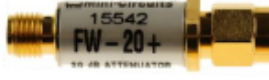



- Sample frequency ADC/DAC: 200 Ms/s
- Output signal level: Up to 15 dBm into 50 Ohms
- Output signal frequency range: 0 – 30 MHz
- Hardware platform: Ettus USRP X310 with UBX-160, LFTX and LFRX daughterboards

Latency table

Sample frequency / Bandpass width [MHz]	Signal throughput delay [μ s]
200	1.0
100	1.3
50	1.6
20	2.1
8	2.8
4	6.6
2	17.3

Package

Qty (1)	Description	
1	Transceiver	
1	12V DC Power Supply Unit, input 100 - 240 V, AC 50 - 60 Hz with country specific power cable.	
1	Ethernet cable	
1	SFP+ to Ethernet adapter	
2	SMA (Plug) to BNC (Jack) adapter	
2	SMA (Plug) to SMB (Plug) adapter	

Qty (1)	Description	
1	64 GB Flash Stick	
1	10dB attenuator	
1	20dB attenuator	
1	SMB to SMB cable, 3 feet	
1	SMB to BNC cable, 3 feet	
1	USB 3.0 to Ethernet adapter	

Please contact Riscure for more information.

You can reach us by email : inforequest@riscure.com,

by phone : +31 15 251 4090 US: +1 650 646 9979

Or on the web: riscure.com.

riscure

