# Using EMC testing equipment as a new side channel acquisition technique

Hardwear.io NL 2022

# Who are those guys ?

**Benjamin VERNOUX**

Embedded Hardware / Firmware / Host tools
SDR: AirSpy R0-R2/Mini
HydraBus v1 / HydraNFC v1&v2…
HydraUSB3 v1

**Nicolas OBERLI**

Embedded security by day

- Security evaluations
- Side channel, fault injection, …

Hardware hacking by night

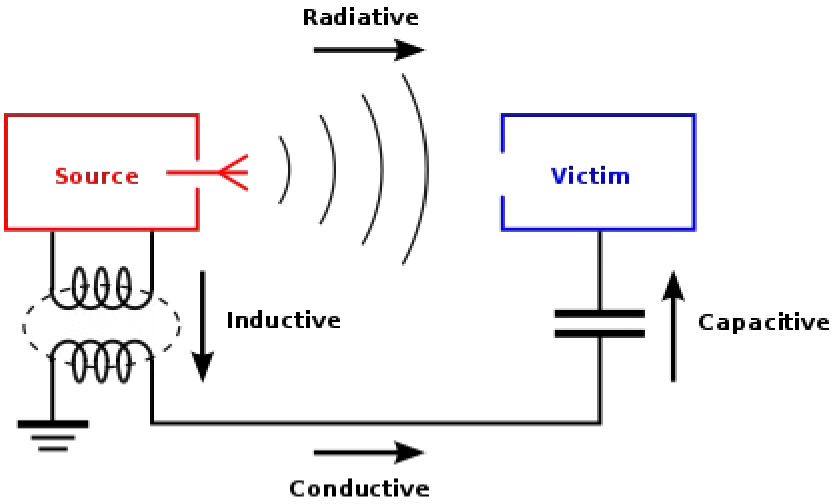
- Same, but cheaper

HydraBus

# EMC ?

- ElectroMagnetic Compatibility
  - Wikipedia : “ability of electrical equipment and systems to function acceptably in their electromagnetic environment”
  - Does the device under test (DUT) behave normally in case of electromagnetic interference (EMI) ?
  - Does the DUT generate EMI ?
- Mandatory for commercial products

# Types of EMI coupling




- **Radiative Coupling** – When an unwanted signal is transferred from source equipment to victim equipment by radiation through space.
- **Inductive Coupling** – The source and the victim are coupled by a magnetic field.
- **Conducted Coupling** – When there is a conduction route along which the signals can travel. This may be along power cables or other inter-connection wires. The conduction may be in one of two modes:
- **Capacitive Coupling** – The level of disturbance depends on the voltage variations (dv/dt) and the value of the coupling capacitance between the disturber and the victim.

https://magnoteknik.com/sources-of-electromagnetic-interference-emi

# Types of EMI coupling “Radiative”

Radiated emissions testing involves measuring the electromagnetic field strength of the emissions that are unintentionally generated by the DUT

Near Field Probes

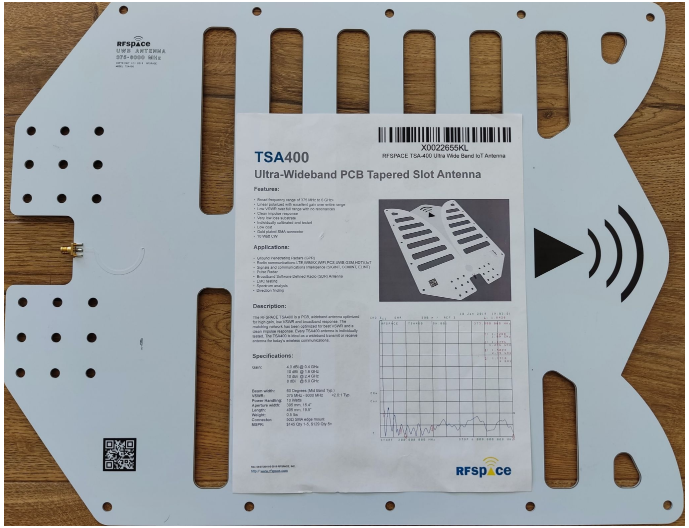
Tekbox TBPS01-TBWA2 EMC near field probe set

Radiated Emissions measurements from <1MHz up to 6GHz with preamplifier (20dB or 40dB)

Can be used with an Oscilloscope or a Spectrum Analyzer

# Types of EMI coupling “Radiative”

## Ultra Wide Band Antenna / Log-Periodic Antenna




**375MHz - 6GHz RFSPACE TSA400**
**(Gain >4dBi)**


**380MHz - 6GHz DEEPACE KC-R100B**
**(Gain >5dBi)**

# Our assumption (and why we are here today)

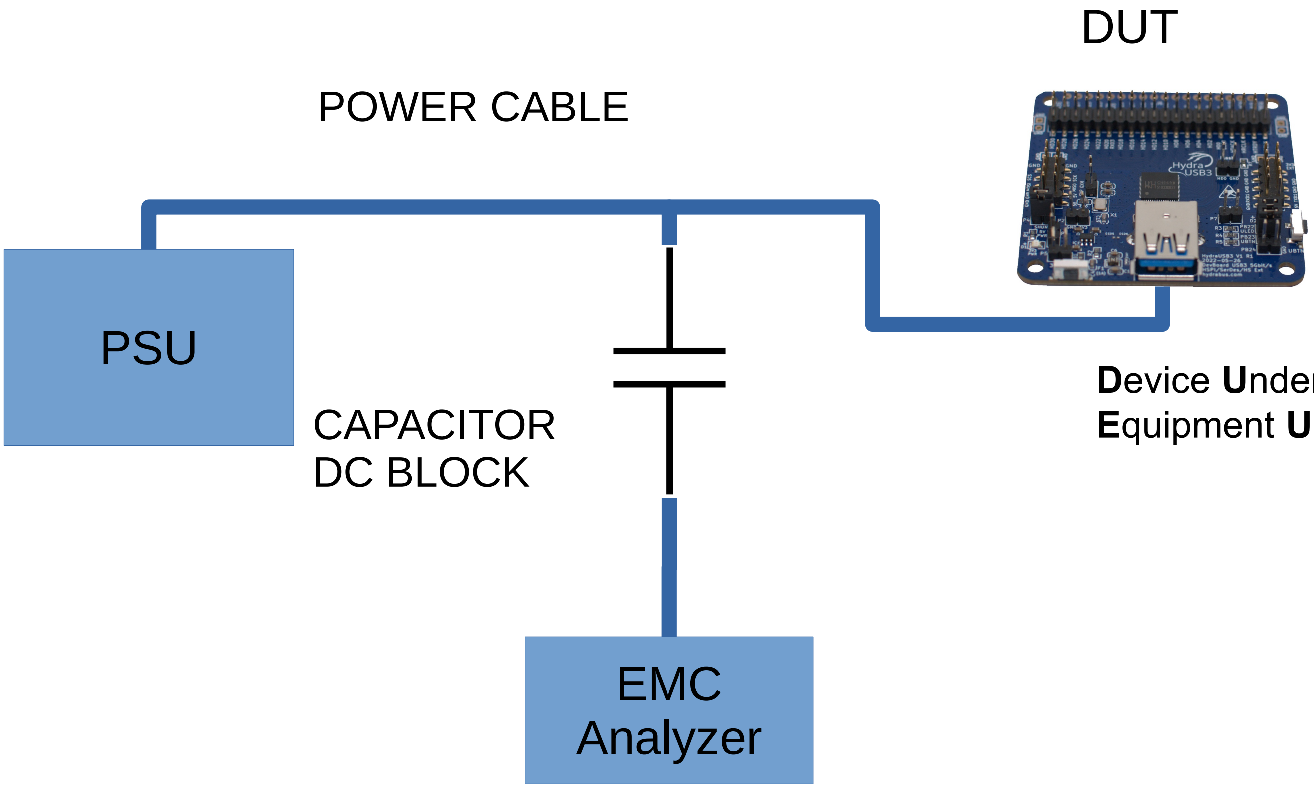
- Radiated and induced EM emissions can already be used to perform SCA
- Can conducted EM signals do the same ?

- Couldn't find any reference in academic papers
  - Usually a bad sign

- Only one way to find out: testing !

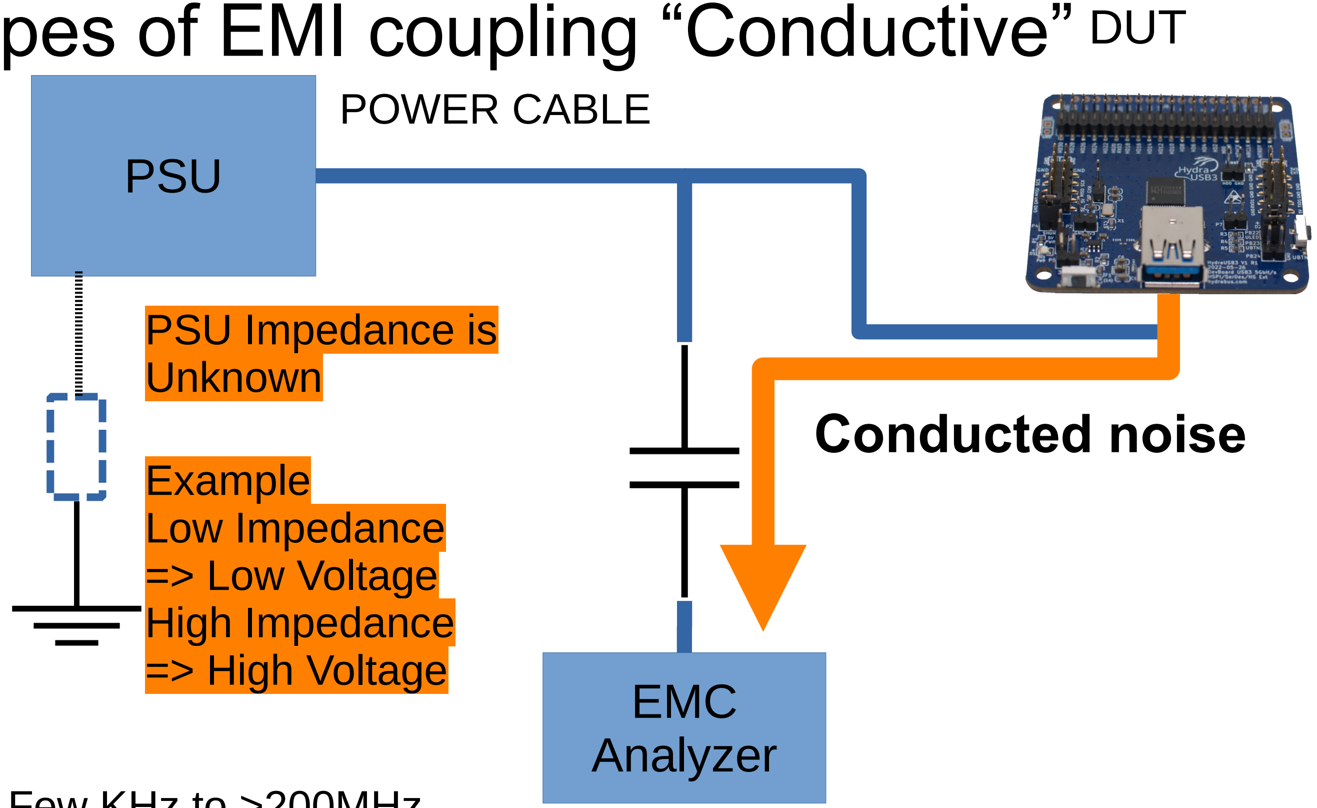
# EMI coupling “Conductive”

# Types of EMI coupling “Conductive”




**D**evice **U**nder **T**est (**DUT**),
**E**quipment **U**nder **T**est (**EUT**)

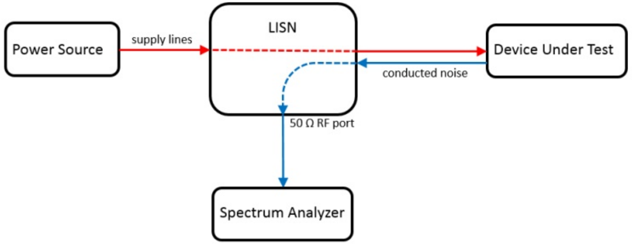
# Types of EMI coupling “Conductive”



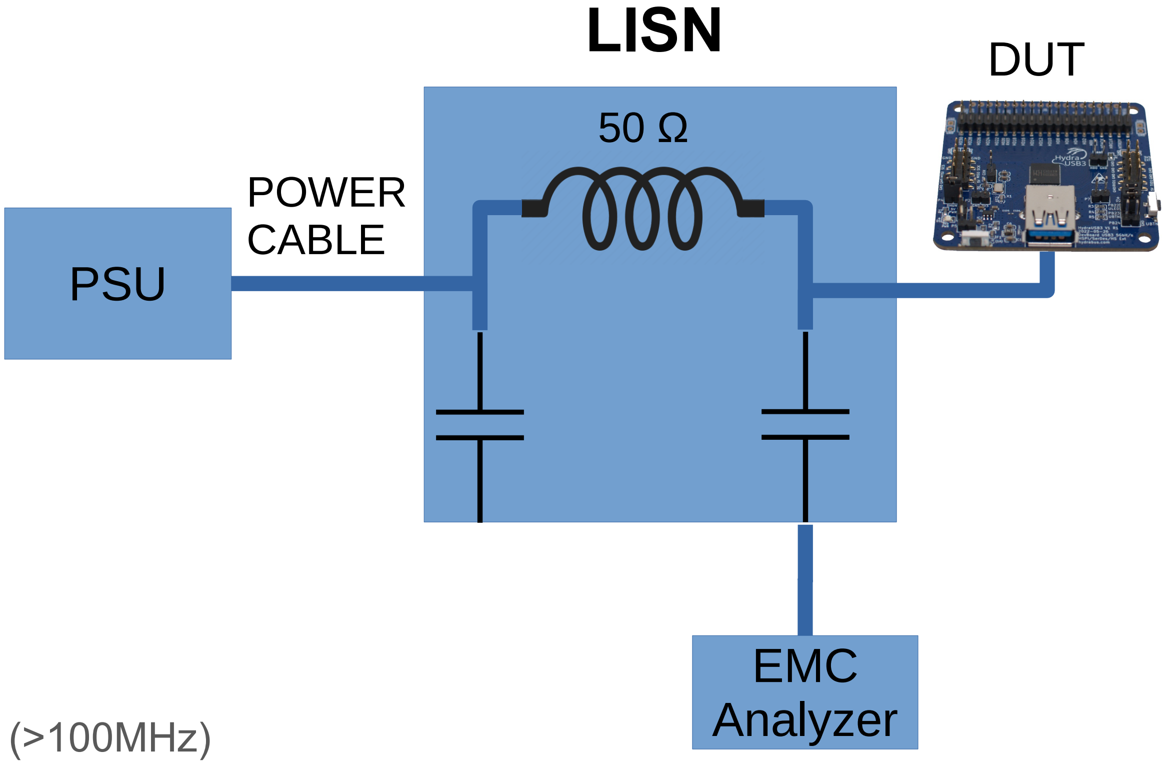

Few KHz to >200MHz

# LISN

- Line Impedance Stabilization Network
  - Low pass filter (cutoff freq 250Hz in our design) typically placed between a power source and the supply terminals of a device under test (DUT).
- Used in EMC testing
  - Provides a well-defined RF-impedance to the DUT (50 Ω)
    - To have lowest loss / maximum power transfer in RF (captured with Scope/SA)
  - Filters power supply noise
- Provides measurement port for RF noise



# LISN

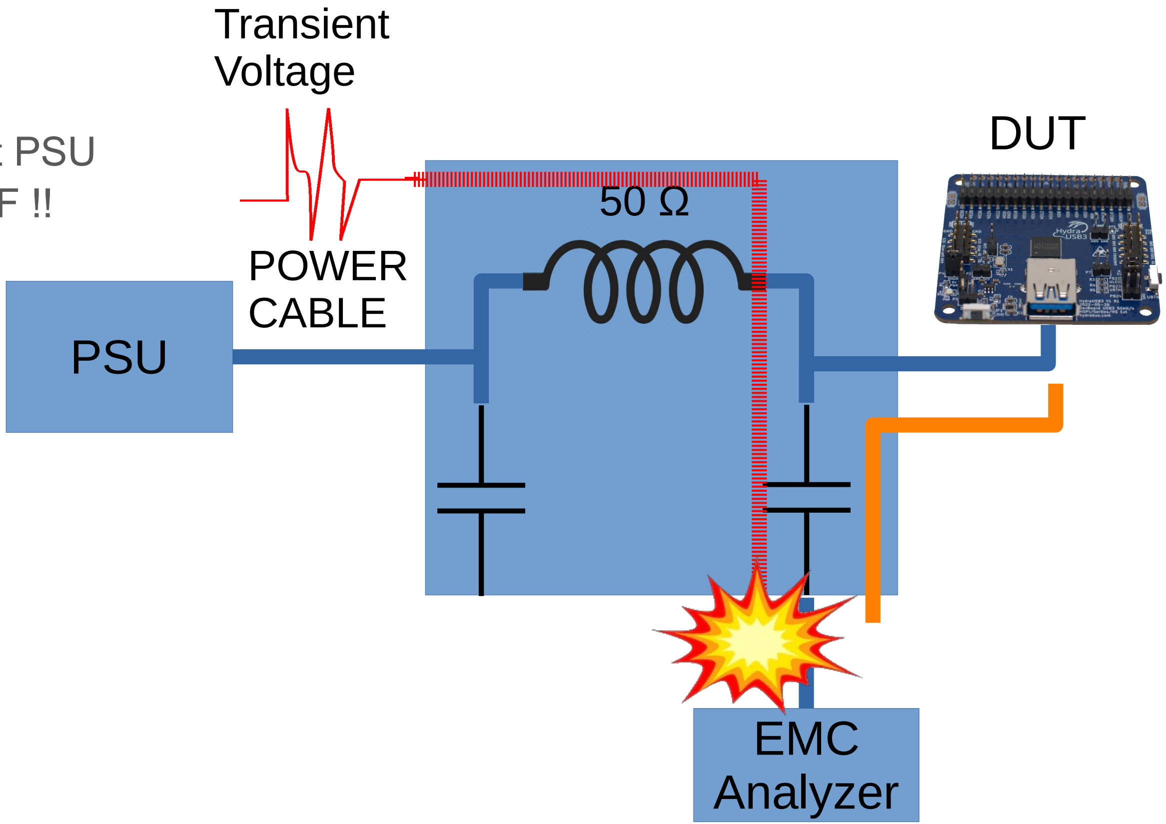



"DC" LISN
**L**ine
**I**mpedance
**S**tabilization
**N**etwork

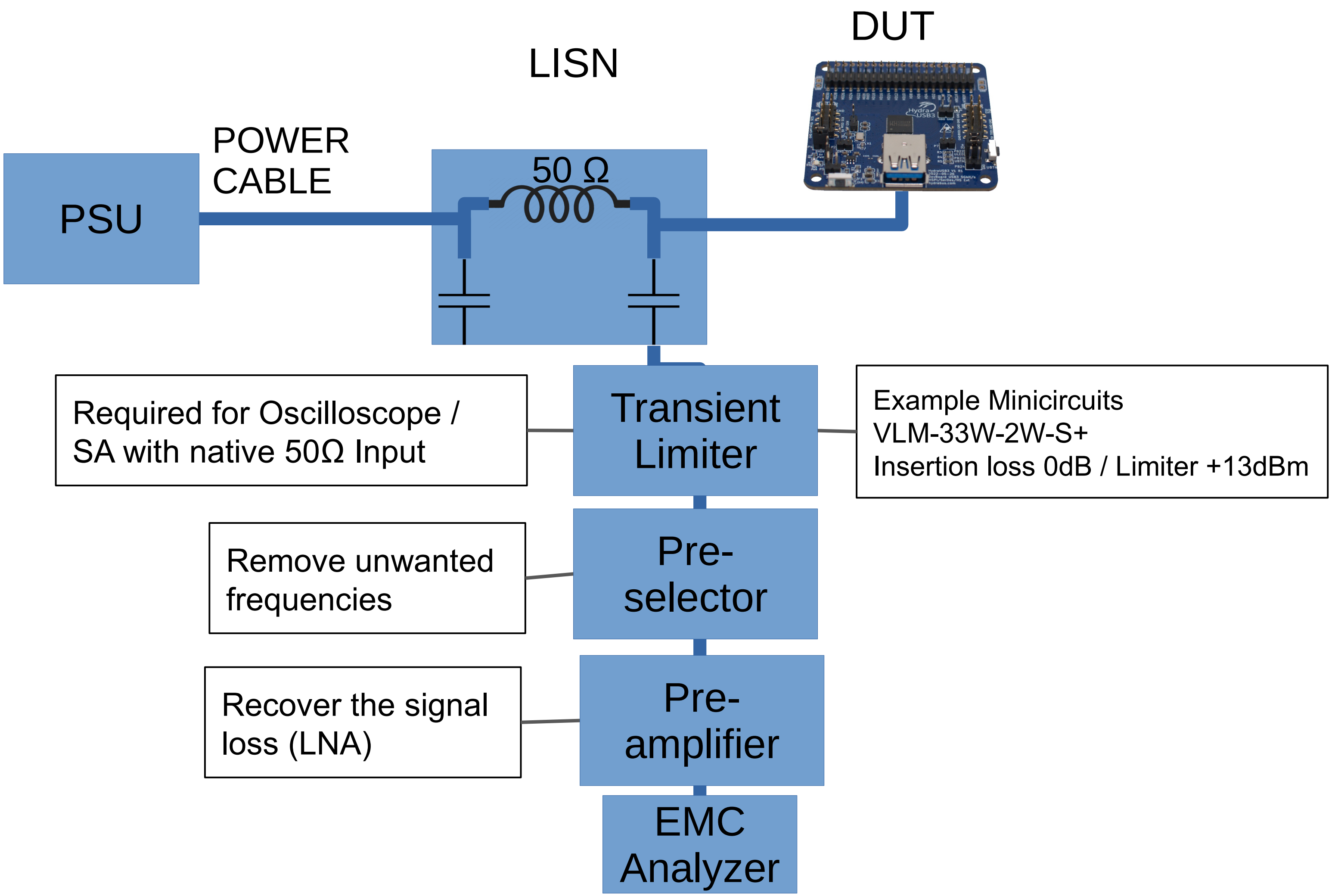
50 Ω Impedance (>100MHz)
Aim is to even exceed 200MHz

# LISN

WARNING about PSU SWITCH ON/OFF !!



# LISN


DUT
LISN
POWER
CABLE
PSU
50 Ω
Required for Oscilloscope /
SA with native 50Ω Input
Transient
Limiter
Example Minicircuits
VLM-33W-2W-S+
Insertion loss 0dB / Limiter +13dBm
Remove unwanted
frequencies
Pre-
selector
Recover the signal
loss (LNA)
Pre-
amplifier
EMC
Analyzer

# DIY LISN

- Commercial LISNs are quite costly (400+€)
  - Well known DC 5µH LISN are TekBox DC LISN 5uH (cost 249USD/unit) => Dual DC LISN requires 2x so > 500 USD

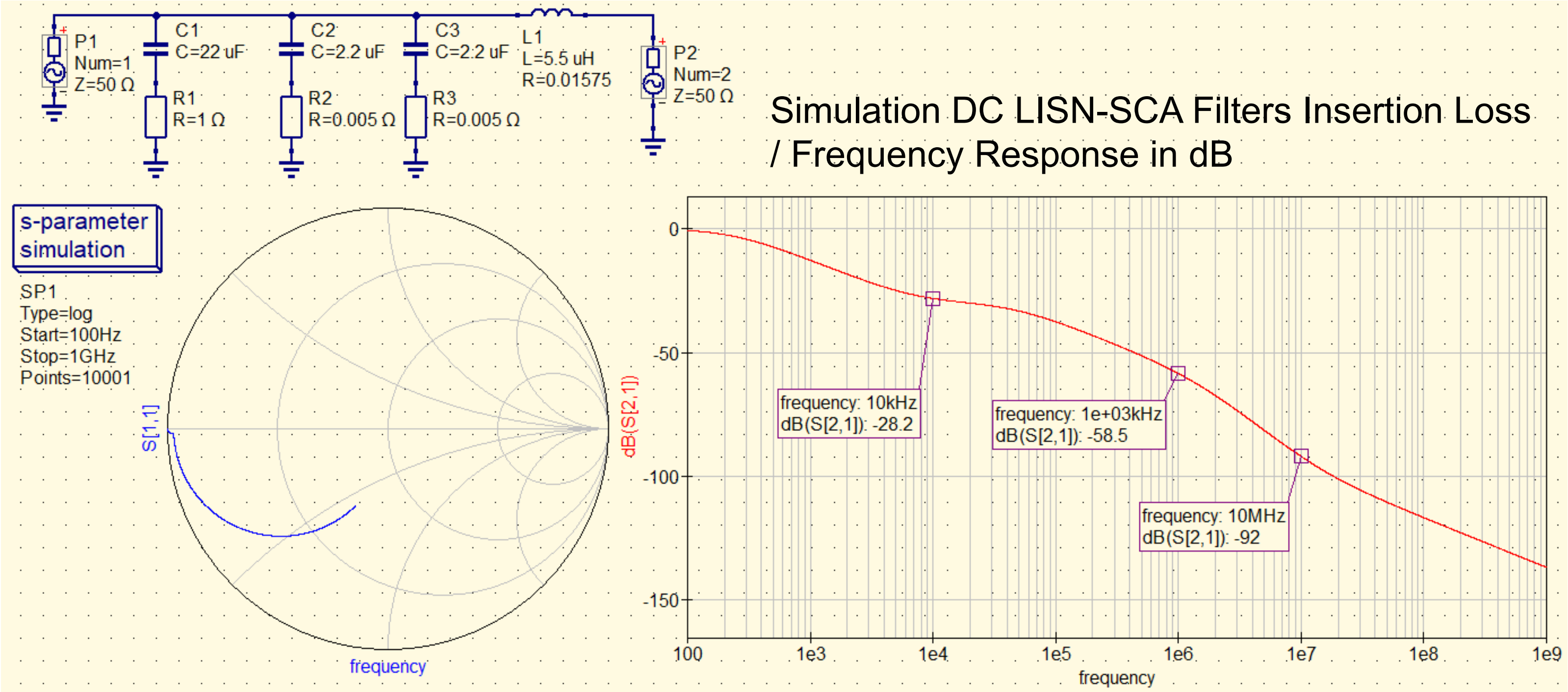
- Let’s build our own !
  - Fully Open Hardware Dual DC LISN available on Github

# LISN for SCA

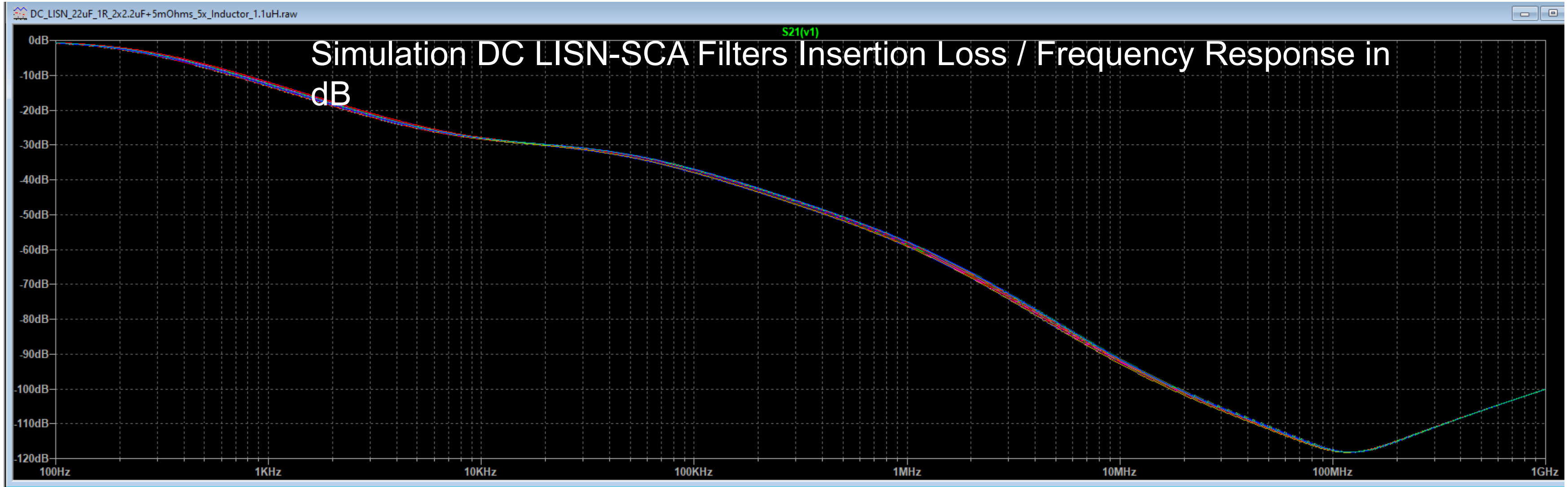
- LISNs usually have attenuators to avoid damaging measurement tools
    - Might dampen the signal
    - Standard LISN output is 50Ω matched
        - Cannot use oscilloscope 50Ω termination
            - Requires a Transient Limiter to avoid potential permanent damage to the Oscilloscope Input
        - Must use an 50Ω Impedance Adapter to connect to oscilloscope 1MΩ Input

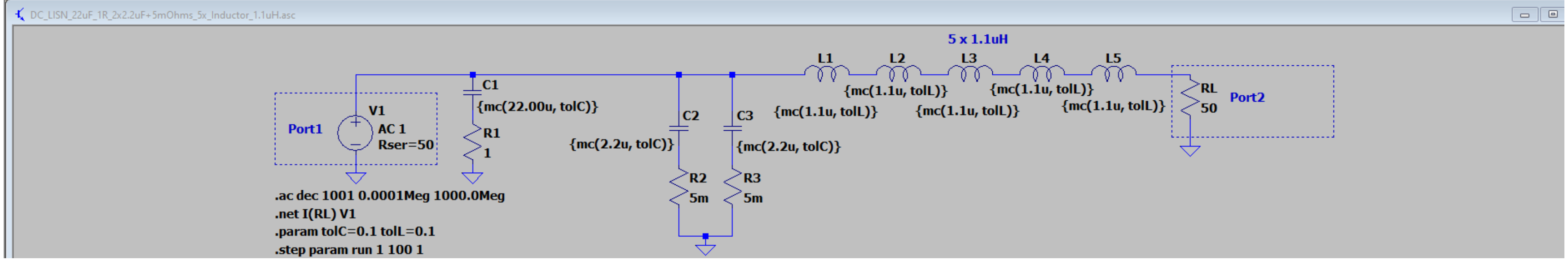
- Solution: remove the attenuator and add input protection
    - We’ll be using an oscilloscope anyways

# Conception of a DC-LISN SCA
# Simulation LP Filters+5µH Inductors (QucsStudio 4.3.1)

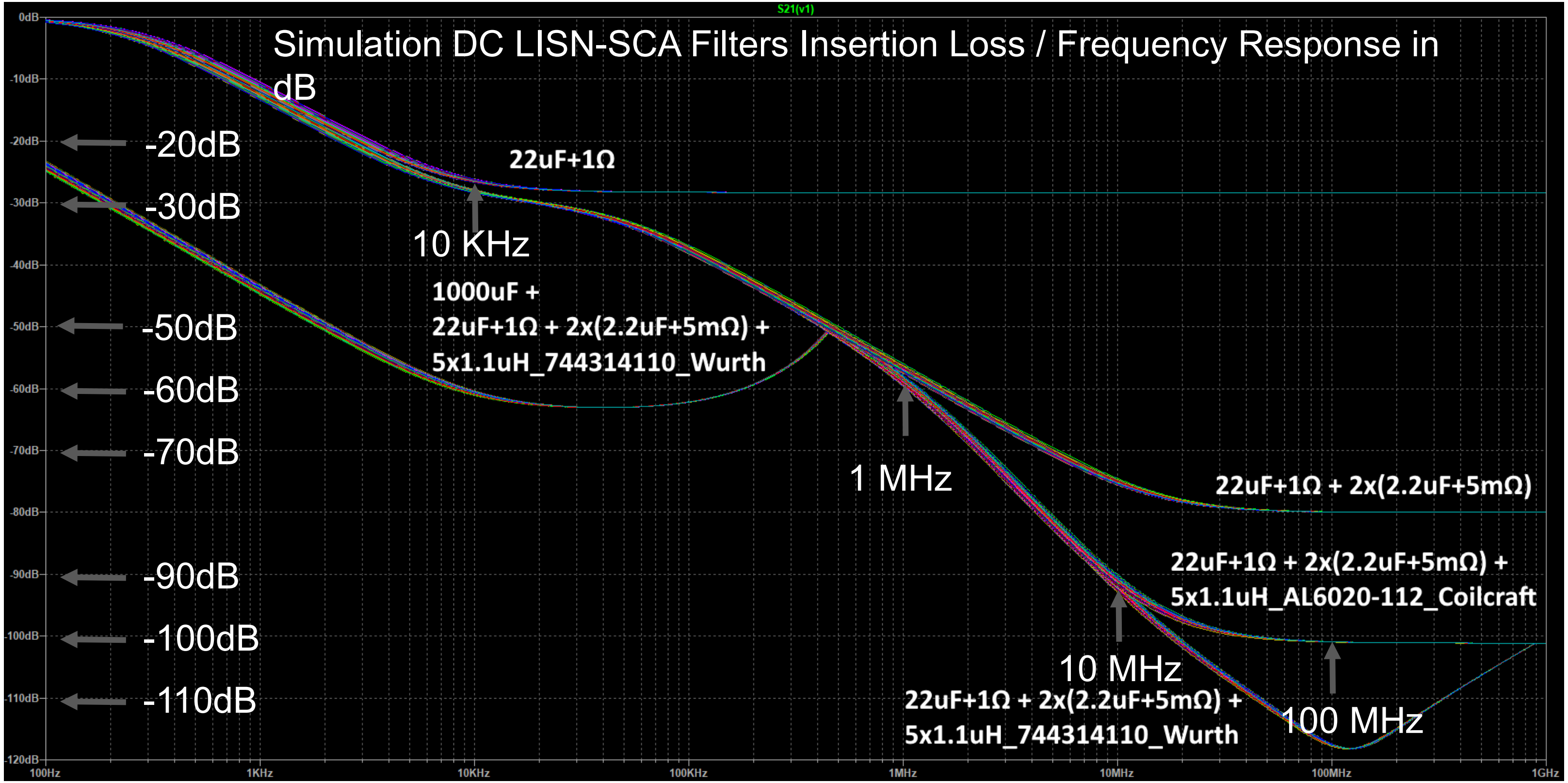


# Conception of a DC-LISN SCA Simulation LP Filters+5µH Inductors (LTSpice)

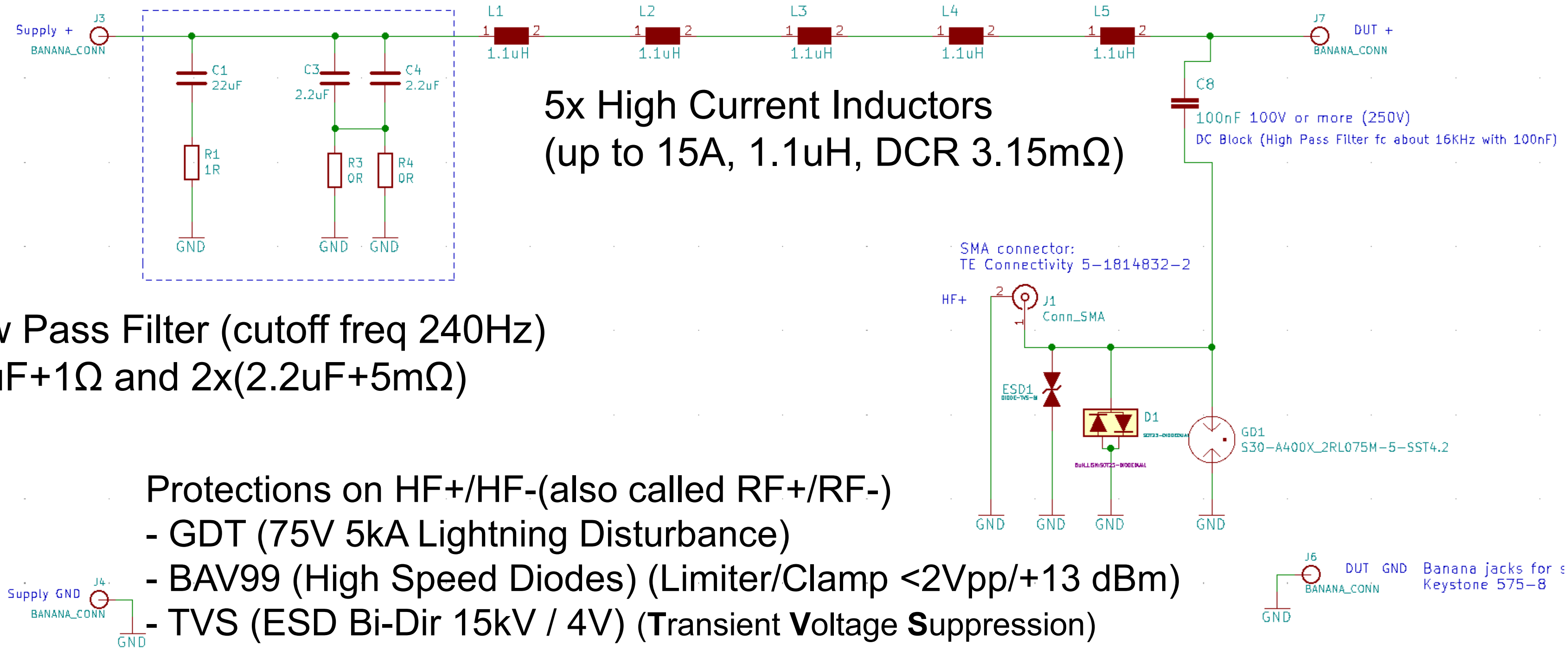


# Conception of a DC-LISN SCA
# Simulation LP Filters+5µH Inductors (LTSpice)



# Conception of a DC-LISN SCA Schematic (KiCad 6)




5x High Current Inductors
(up to 15A, 1.1uH, DCR 3.15mΩ)

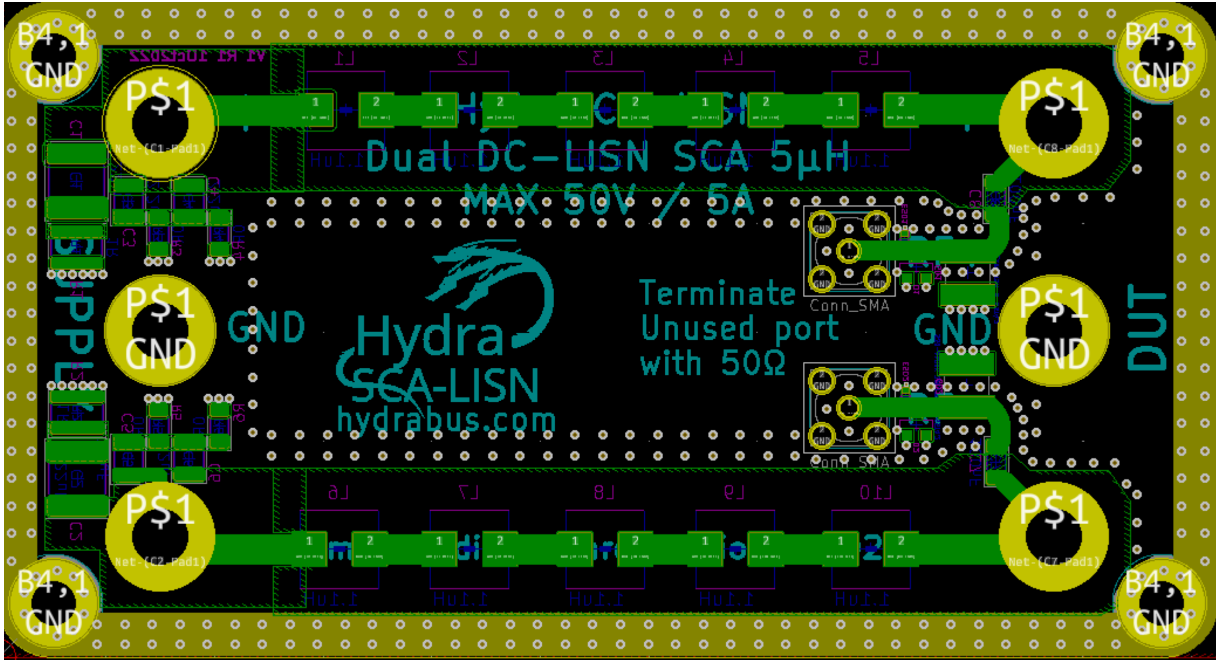
Low Pass Filter (cutoff freq 240Hz)
22uF+1Ω and 2x(2.2uF+5mΩ)

Protections on HF+/HF-(also called RF+/RF-)
- GDT (75V 5kA Lightning Disturbance)
- BAV99 (High Speed Diodes) (Limiter/Clamp <2Vpp/+13 dBm)
- TVS (ESD Bi-Dir 15kV / 4V) (**T**ransient **V**oltage **S**uppression)

ESD suppressor and Transient Limiter to < 2Vpp(+13 dBm)

- Tested with SigGen & PSU 40V DC Supply (Switch ON/OFF)...

# Conception of a DC-LISN SCA PCB (KiCad 6)




PCB 2 Layers 1.6mm(Core 1.5mm)
FR4-STD (Er 4.6)
Saturn PCB Toolkit V8.21

**Conductor Impedance => Impedance 50 Ohms**

**Computation for Inductances traces ("L1-L5" / "L6-L10") Microstrip**

Conductor Width: 2.8mm
Conductor Height: 1.5mm
Z0 computed: 50.1 Ohms
L0 computed: 3.0880 nH/cm
C0 computed: 1.2321 pF/cm

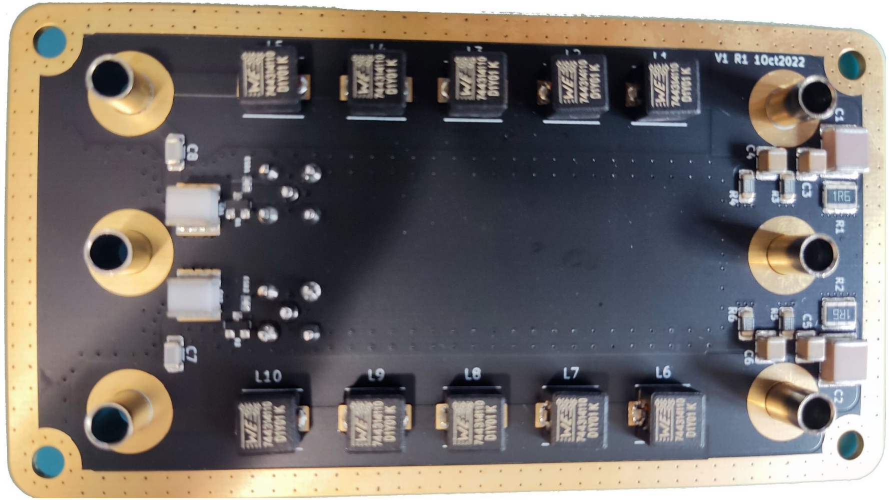
**Computation for RF traces ("RF+"<=>"DUT+" / "RF-"<=>"DUT-")**

**Coplanar Wave**

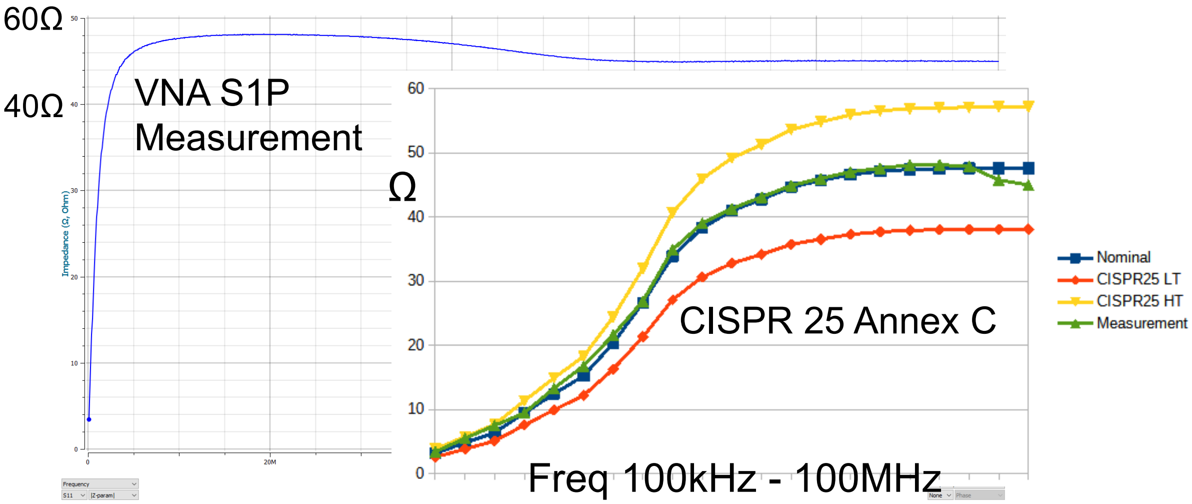
Conductor Width: 1.88mm
Conductor Height: 1.5mm
Conductor Gap: 0.47mm
Z0 computed: 50.12 Ohms

# Conception of a DC-LISN SCA Final Board

- HydraSCA-LISN have Input protections/Limiter to protect Oscilloscope (or Spectrum Analyzer) Input even with native 50Ω
  - About +10 dBm Limiter

# DC-LISN SCA Measurements with VNA (Impedance)


Measurement Impedance(Z) (100kHz - 100MHz)

3.4Ω at 100 kHz => 11Ω at 350 kHz

>21Ω at >700 kHz => 32Ω at 1.2 MHz

>40Ω at 2MHz => >44Ω at 5MHz

>47Ω from 7 MHz to 40 MHz

45Ω from 60 MHz to > 100 MHz

# DC-LISN SCA Measurements with VNA (Filters/Isolation)

## Measurement of Isolation (Filter) between SUPPLY +/GND & DUT +/GND




SUPPLY + / GND => VNA Port1
DUT + / GND => VNA Port2

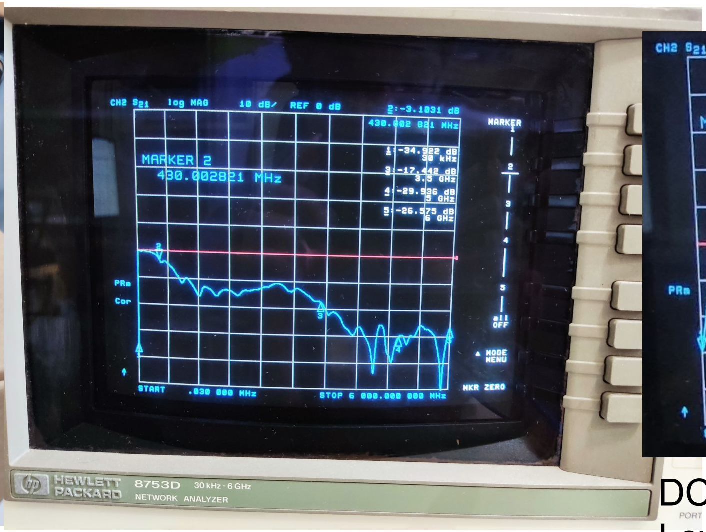
Measurement Filters/Isolation

1 => -33 dB at 30 KHz
2 => -68 dB at 1.5 MHz
3 => -58 dB at 4 MHz
4 => -61 dB at 60 MHz
5 => -49 dB at 110 MHz

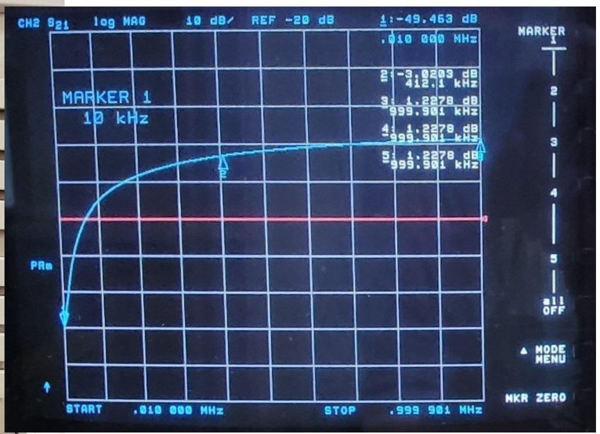
# DC-LISN SCA Measurements with VNA (Insertion Loss)

Measurement of InsertionLoss/Bandwidth & cutoff Frequency between DUT +/GND & HF+


HF+ => VNA Port1
DUT + / GND => VNA Port2

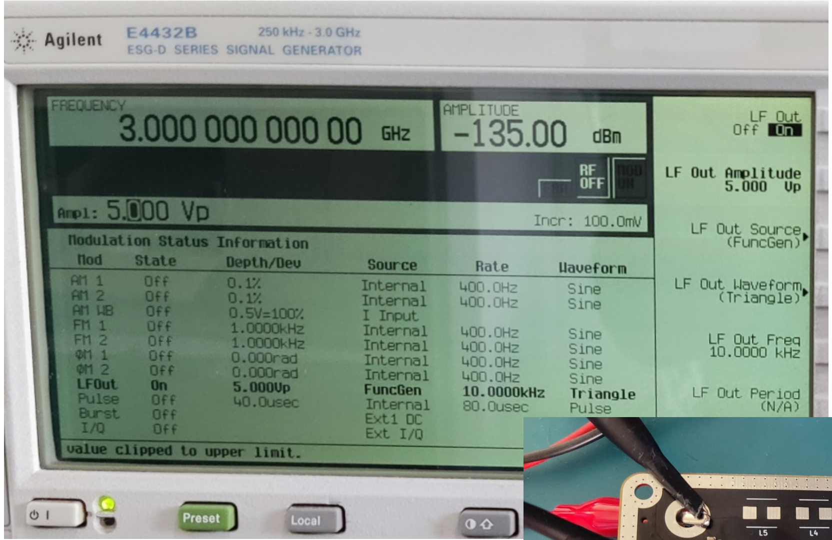



Bandwidth measurement
> 430MHz (-3dB)

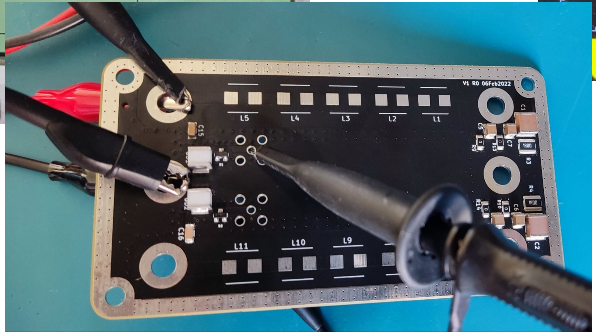



DC Block + Protections (HF+)
Low Pass Filter cutoff freq > 400 KHz
(Simulation 16KHz 100nF Capacitor)

# DC-LISN SCA Measurements Limiter/Clamp





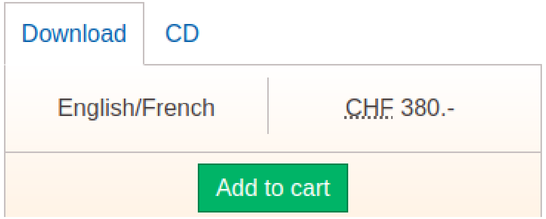


LISN SCA
Signal Input 10Vpp 10kHz Triangle
RF Protection clamp signal to <2Vpp (<1.8Vpp max about +10dBm) to protect sensitive Oscilloscope Input (50Ω native) or Spectrum Analyzer Input

# Measurement setup

# Measurement setup

- Standardized by IEC : CISPR 25
  - Not free :(
  - Old version can be found using google dorks




- Gives lots of information about measurement setup
- Tekbox documentation provides the same information we need

# Measurement setup - cont.

- Stay as close as a standard EMC measurement setup

- Earthing
- Ground plane
- Cable lengths
- Support

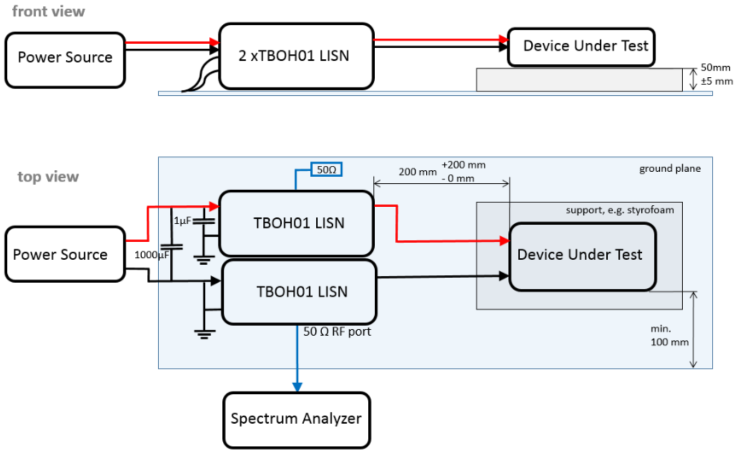



*Figure 10: conducted emission measurement, voltage method, DUT with power return line remotely grounded*

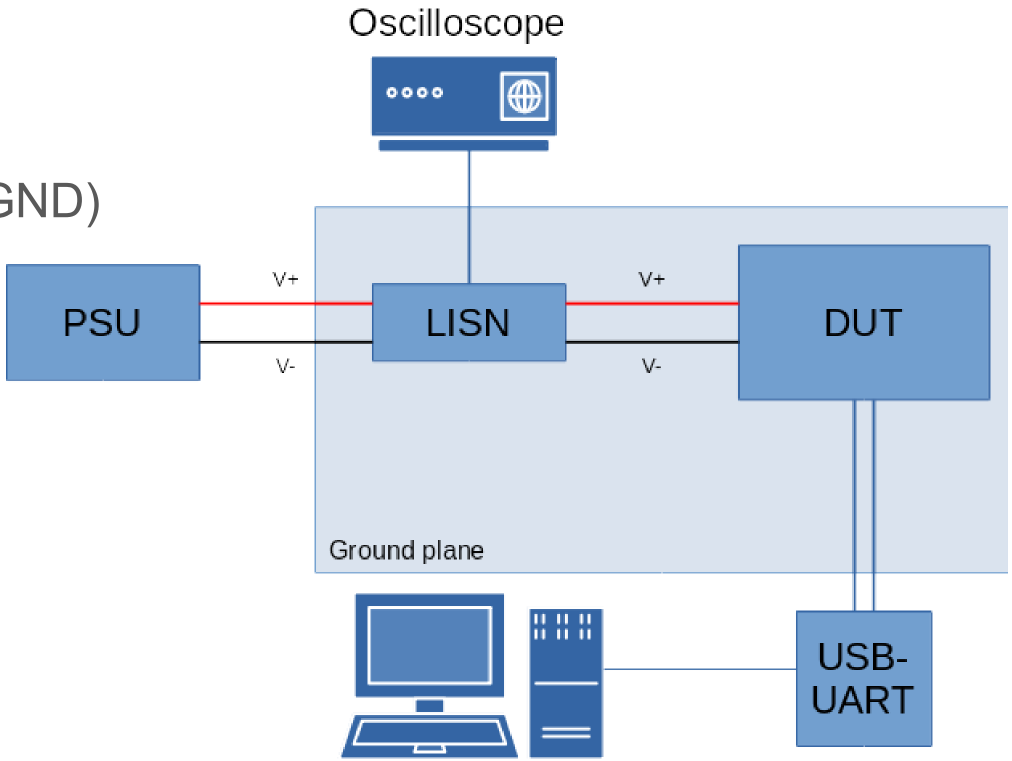


https://www.tekbox.com/product/TBOH01_Manual.pdf

# Test setup

- STM32 “bluepill”
  - Decoupling capacitors removed
- LISN on both power rails (+3.3V/GND)
- Rigol MSO5000 oscilloscope
  - 350MHz / 4GSPS

- Ground plane connected to earth
- LISN <-> DUT cables max. 20cm




Objection!

# Objection !

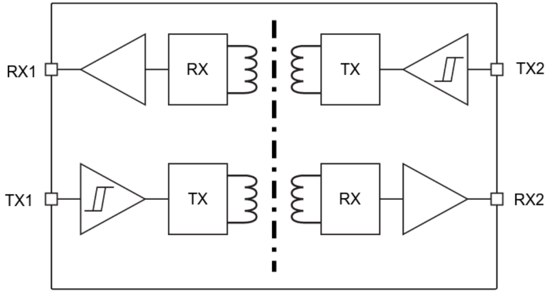
- Need UART to communicate with target
- Means we will bring in conducted EMI from PC to DUT

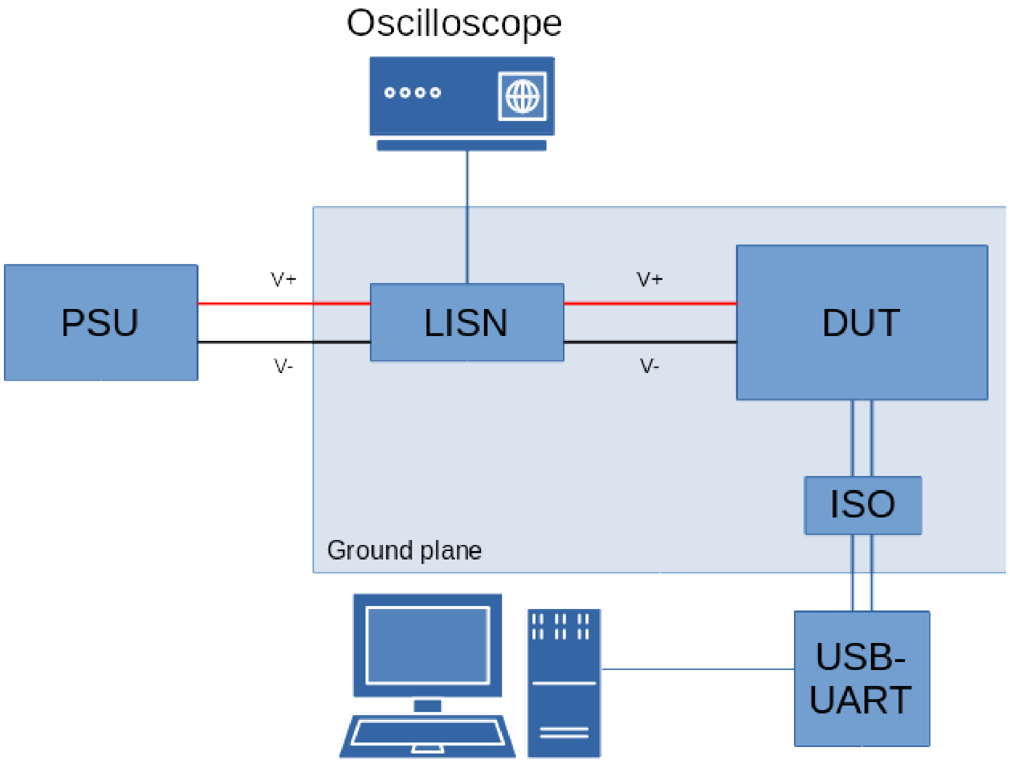
- More noise means lesser correlation on traces

# Communication isolation

- Easy solution : optocouplers
    - Salvaged from old PSU
    - Works @9600bps
- Better solution : digital isolator
    - Faster communication is possible

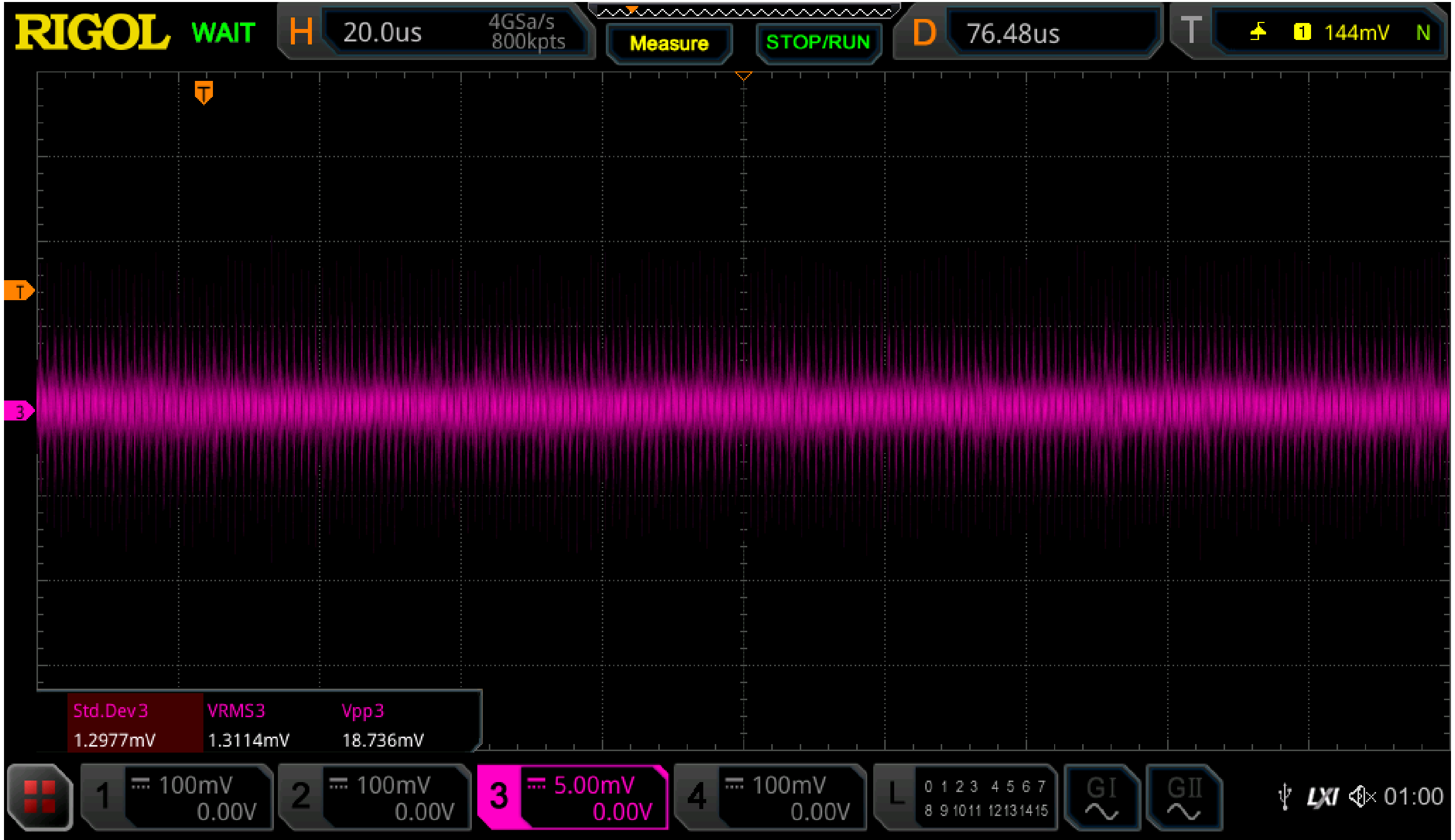
Figure 1. Block diagram



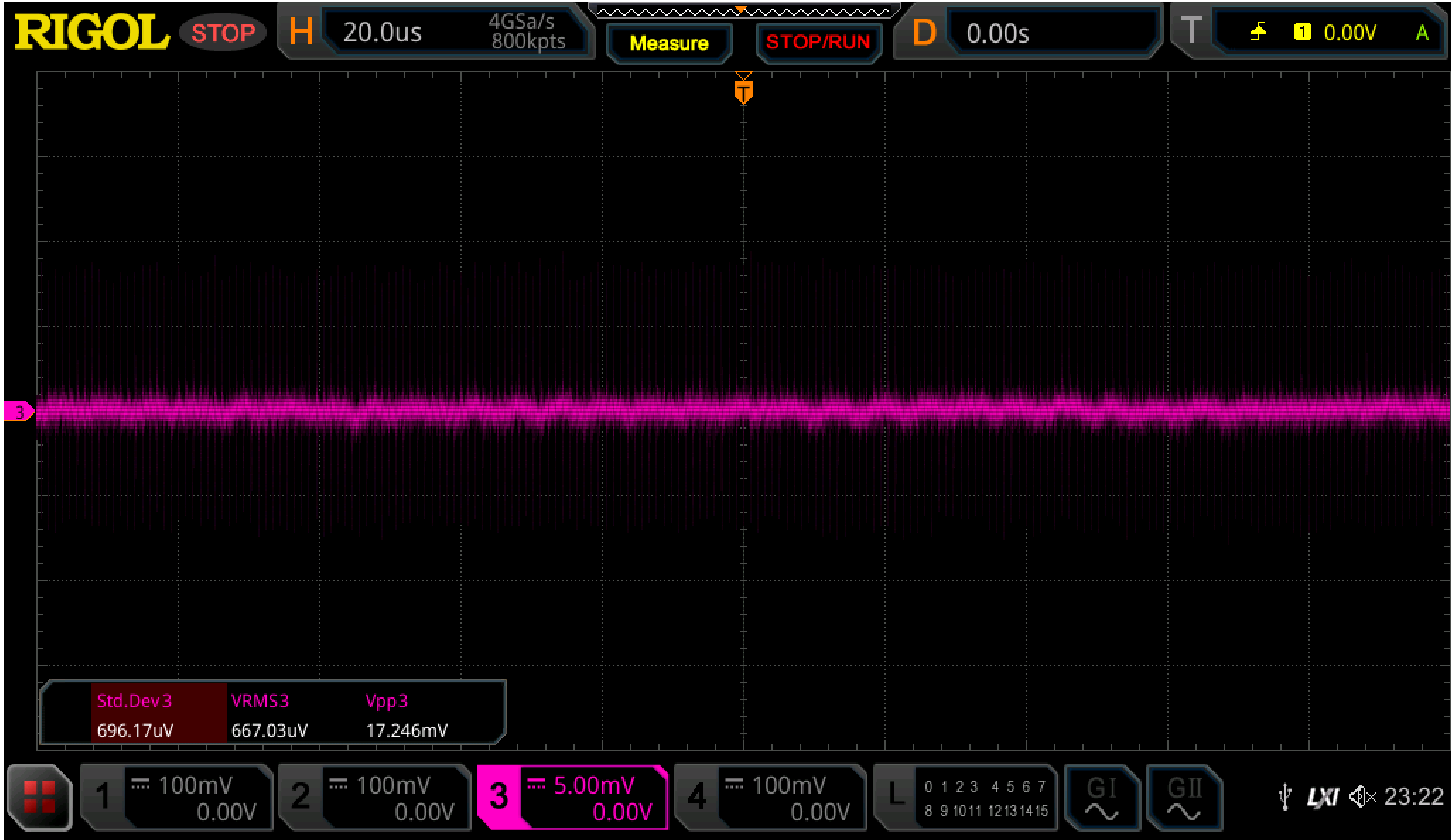
# Direct connection

# Isolator

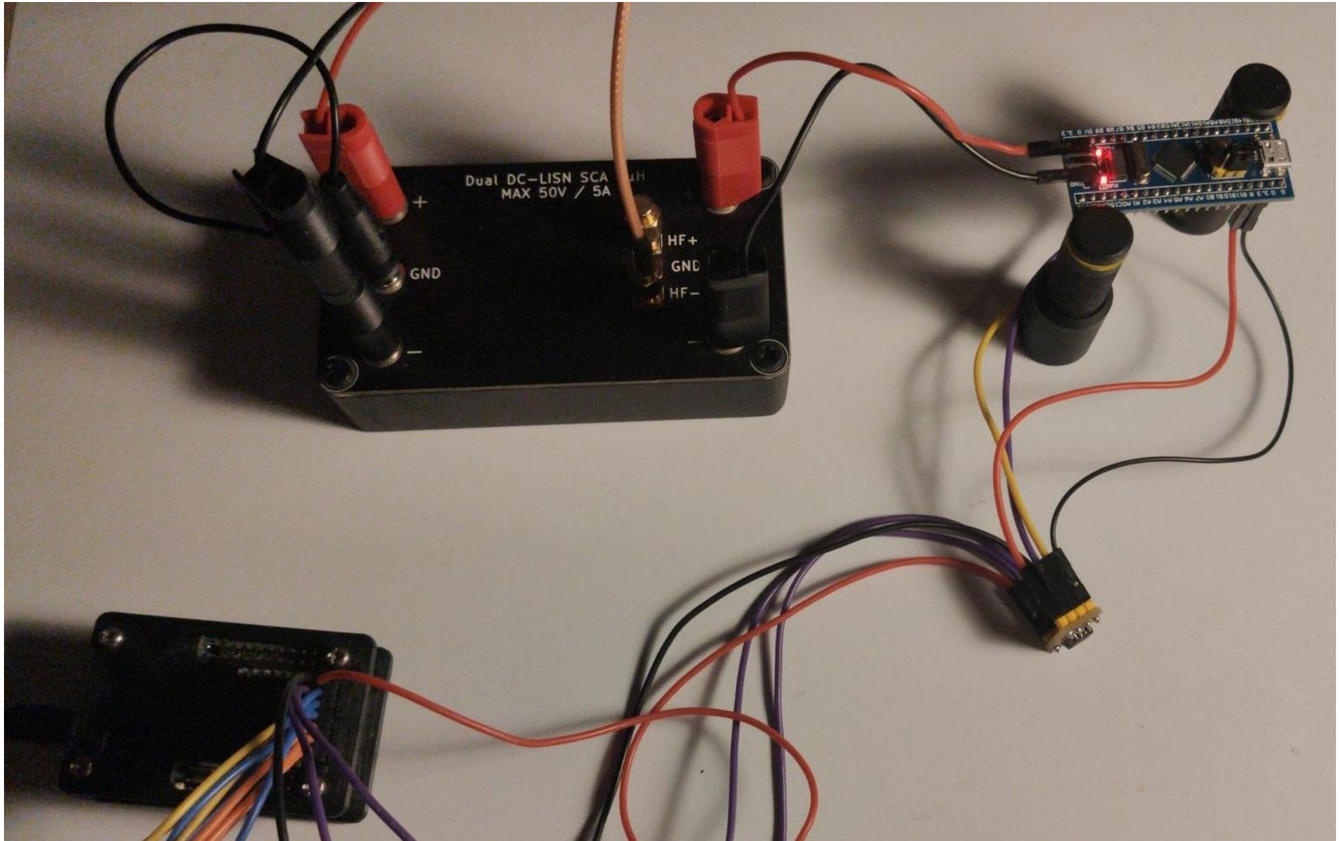


RIGOL
WAIT
H
20.0us
4GSa/s
800kpts
Measure
STOP/RUN
D
76.48us
T
144mV
N
Std.Dev3
1.2977mV
VRMS3
1.3114mV
Vpp3
18.736mV
1 100mV 0.00V
2 100mV 0.00V
3 5.00mV 0.00V
4 100mV 0.00V
01:00

# Isolator + ground plane



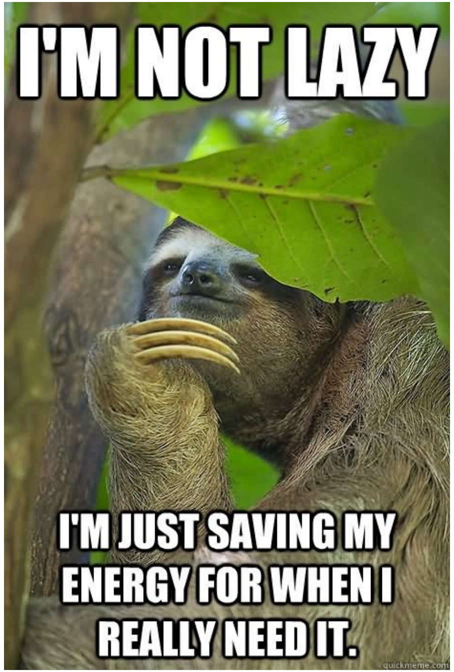
# Final setup



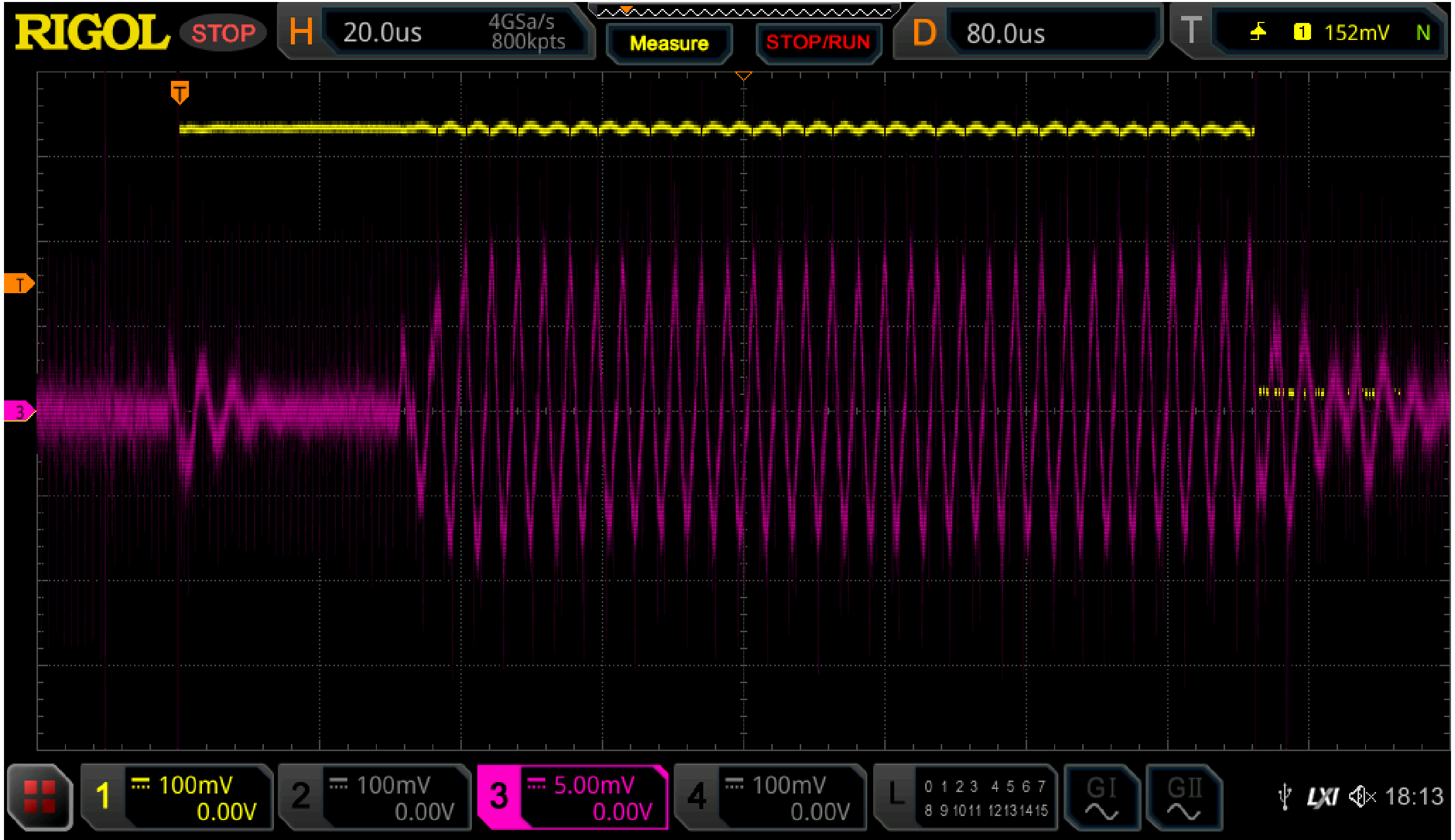
# Software side

- Software SM4
    - GPIO as trigger
    - 16 bytes of input
    - 16 bytes of output

- If everything goes well, we should see the 32 rounds



# We have a signal !

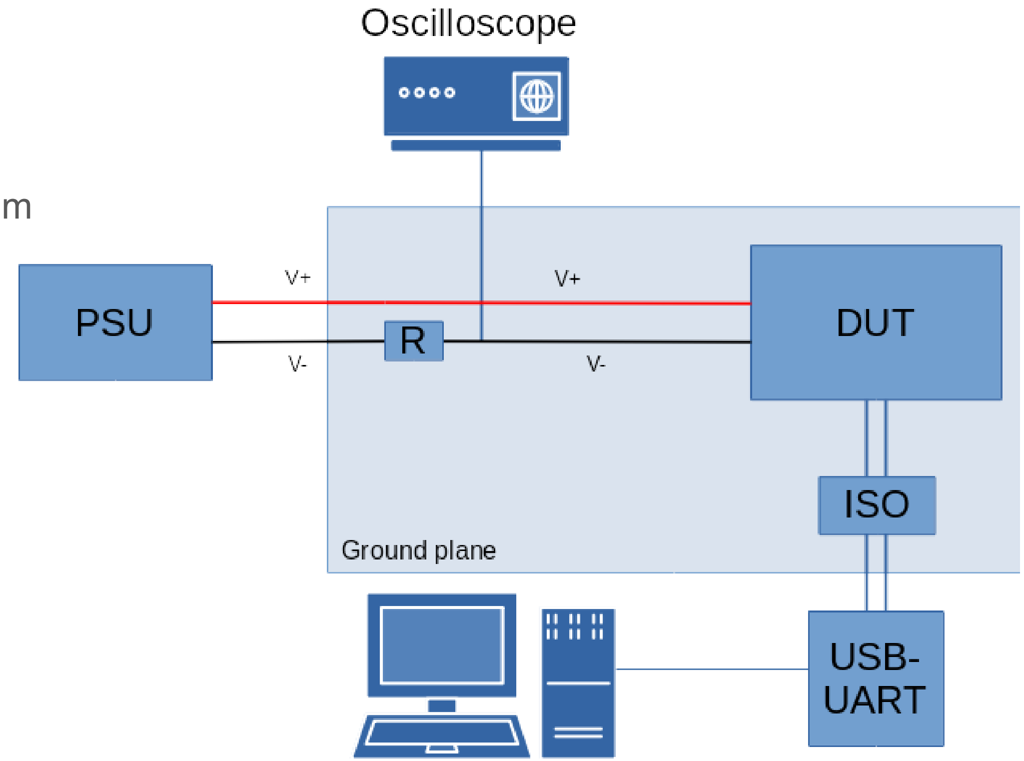


# So far so good

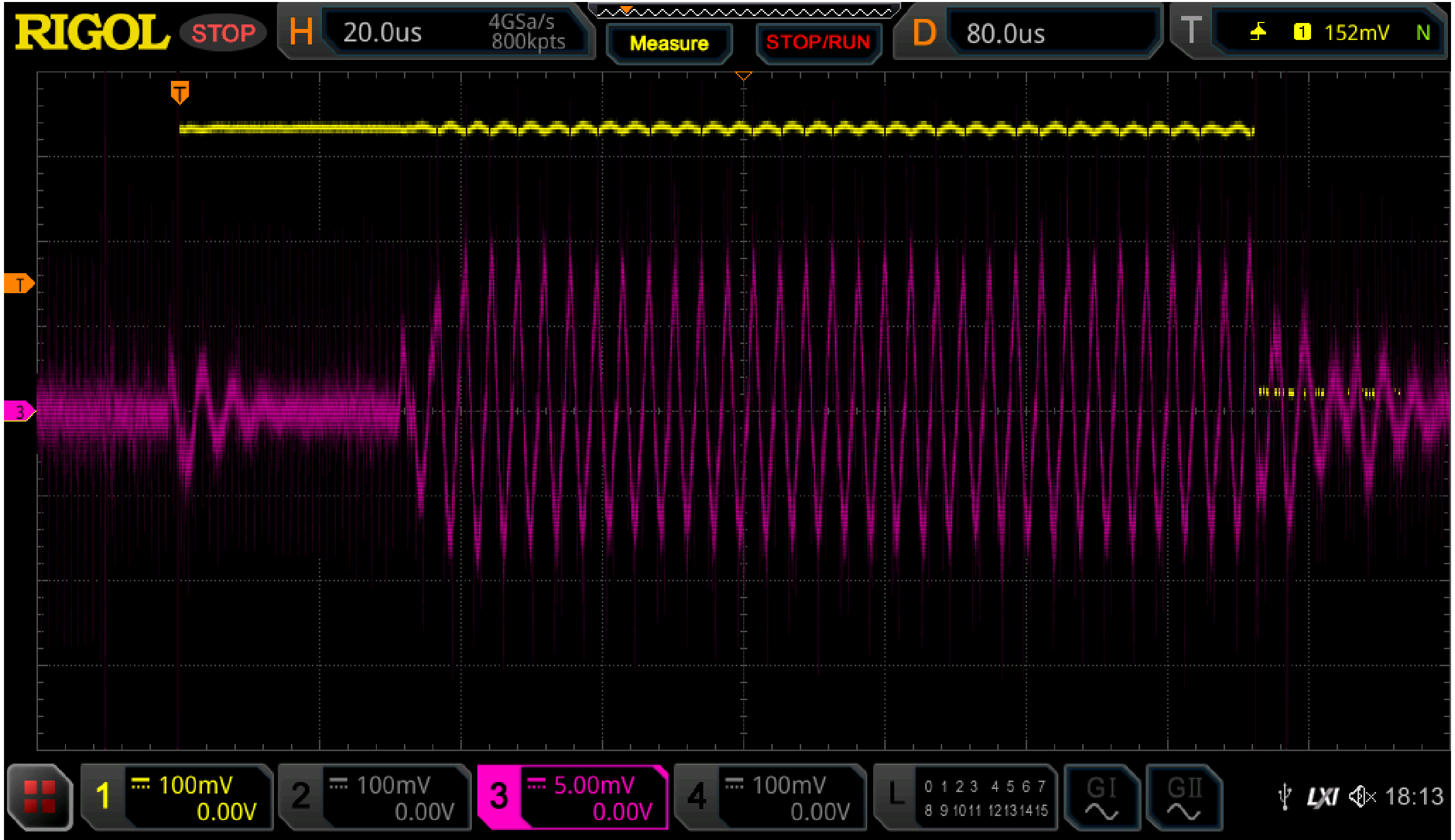
- Traces seem to be useable
- Can we compare this technique with others ?
- Shunt resistor is a good candidate
  - Similar placement in the circuit
  - Affordable / easy setup

# Shunt resistor setup

- SM4 on STM32
- 1 Ohm resistor placed on GND
  - FYI: LISN line resistance is 0.16 Ohm
- Everything else unchanged



# Setup 1 - LISN

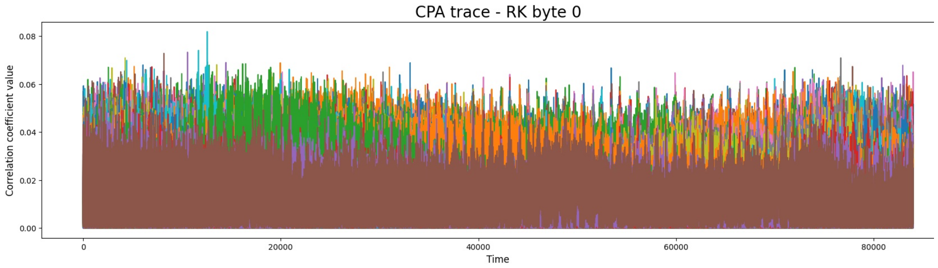


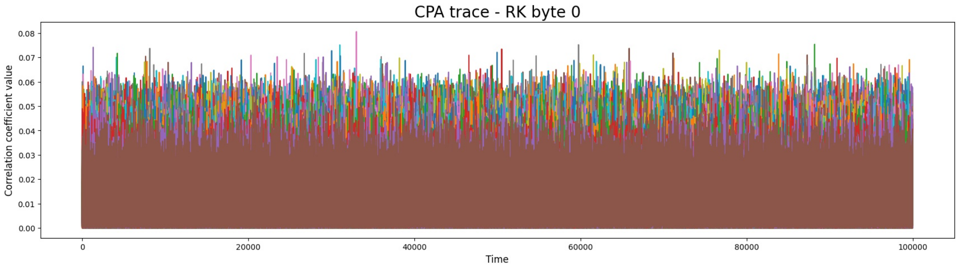
RIGOL
STOP
H
20.0us
4GSa/s
800kpts
Measure
STOP/RUN
D
80.0us
T
152mV
N
1
100mV
0.00V
2
100mV
0.00V
3
5.00mV
0.00V
4
100mV
0.00V
L
0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15
GI
GII
18:13

# Setup 1 - Shunt

# CPA

- 5000 traces acquired
  - Random plaintext
  - No resync
- Results on first round :
  - LISN : 3/4 bytes recovered. Last byte is the second candidate
  - Shunt : No correlation



# Exploiting signals

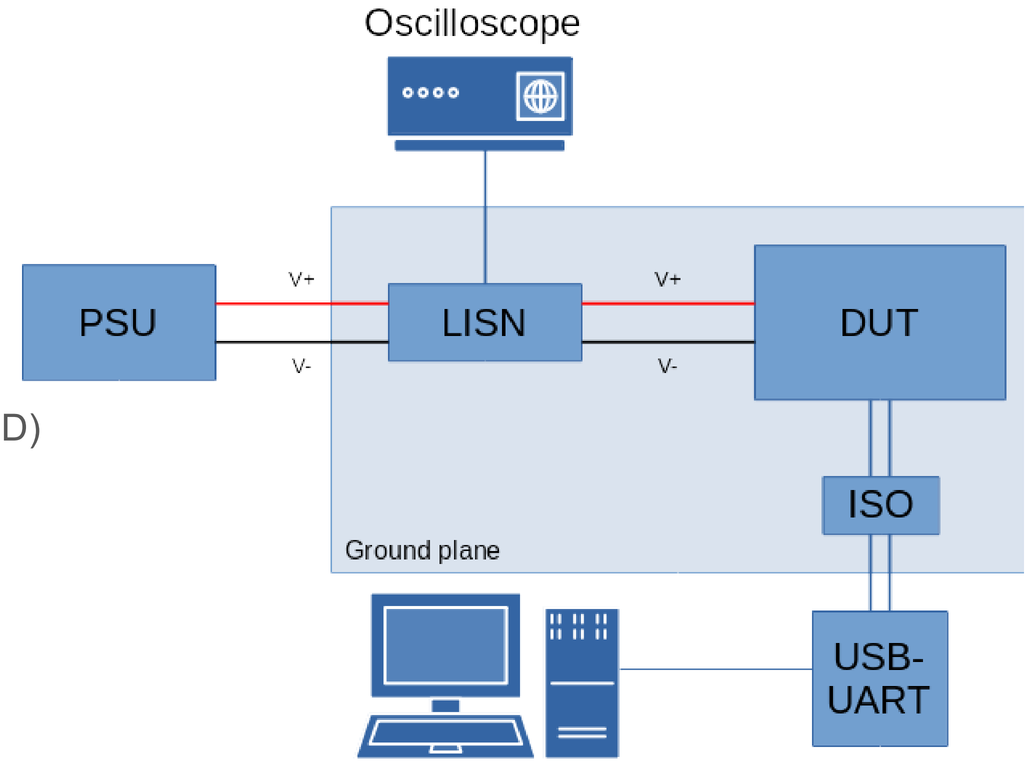
- LISN provides a better dynamic range compared to shunt
  - Allows key recovery with less traces
- Signal is also less noisy
  - Can also be due to my cheap power supply

- Quite old chip, CPU leaks a lot

- Would it be the same with a more recent chip ?
- Does the technique work with decoupling capacitors ?

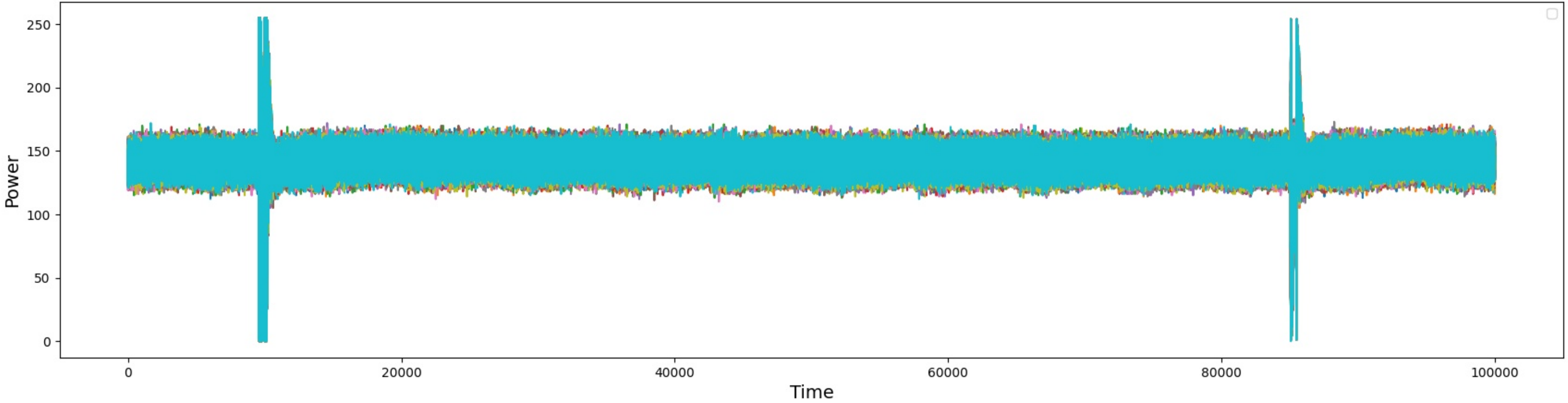
# Second test setup

- ESP32-C3 devkit @160MHz
  - Capacitors NOT removed
- Simple firmware
  - software AES (tinyAES)
  - GPIO as trigger
- Acquisition
  - LISN on both power rails (+3.3V/GND)
  - 1 Ohm resistor on VDD
- Rigol MSO5000 oscilloscope
  - 350MHz / 4GSPS



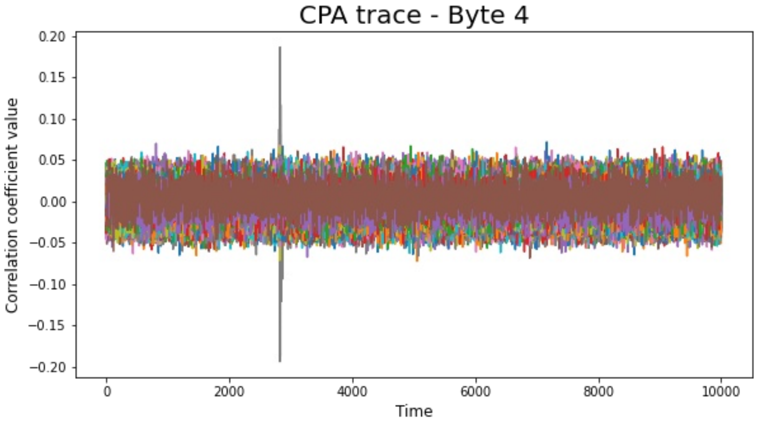
# Acquisition

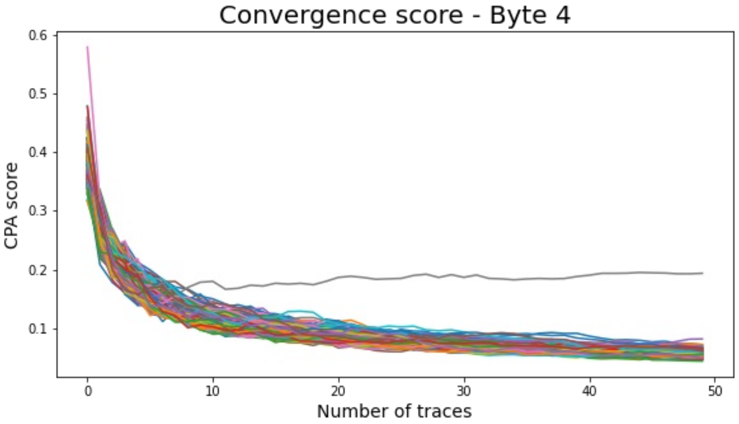
- 50’000 averaged traces
- Random plaintext
- No resynchronization



# Initial results

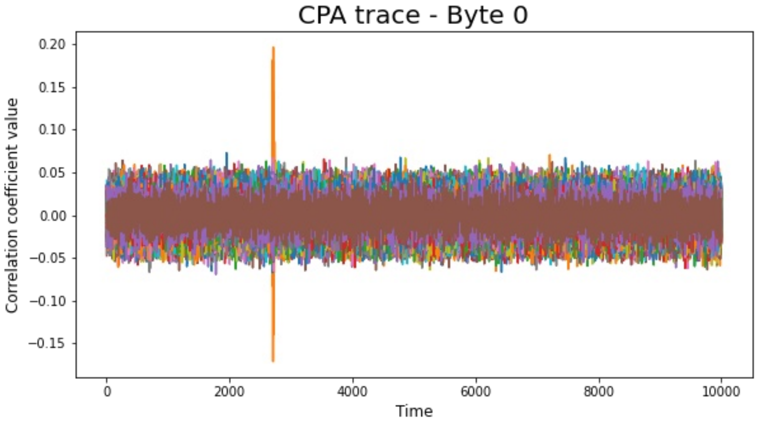
- Applying CPA on both trace sets reveals the key
- Not enough information to quantify each trace set quality

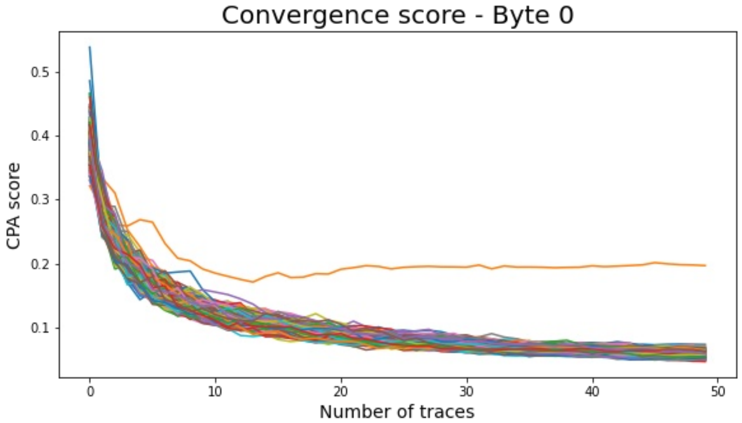


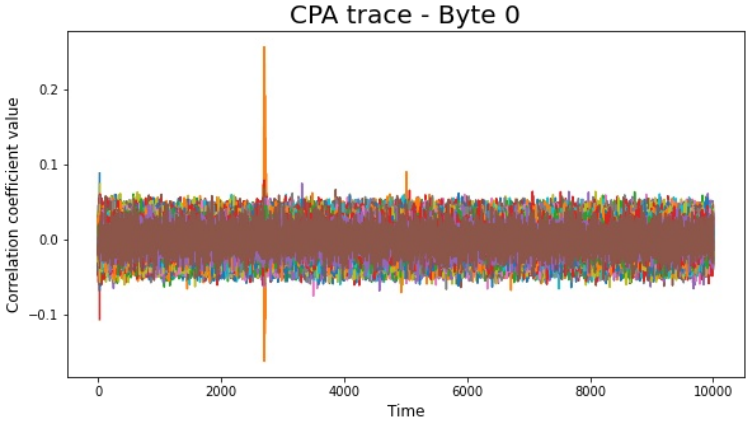
# LISN vs Shunt

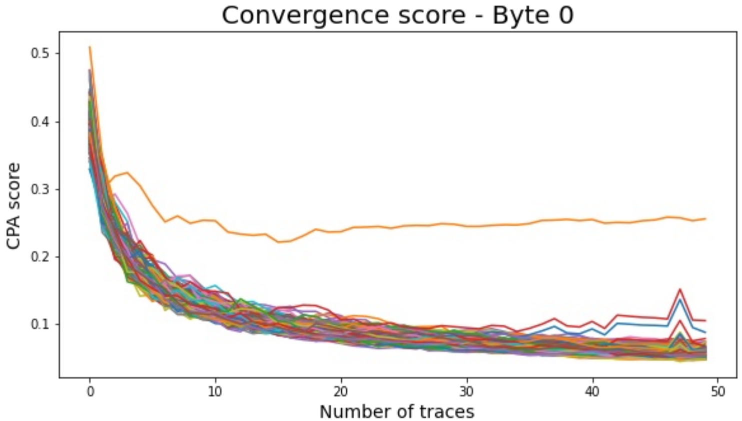
LISN




Shunt

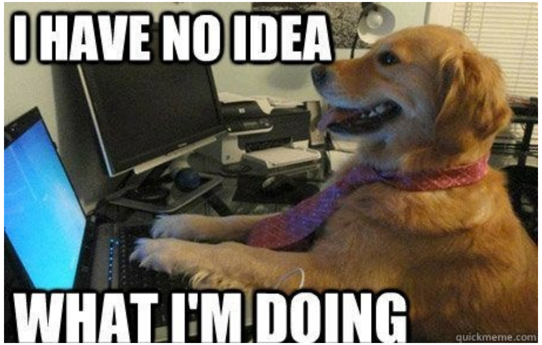


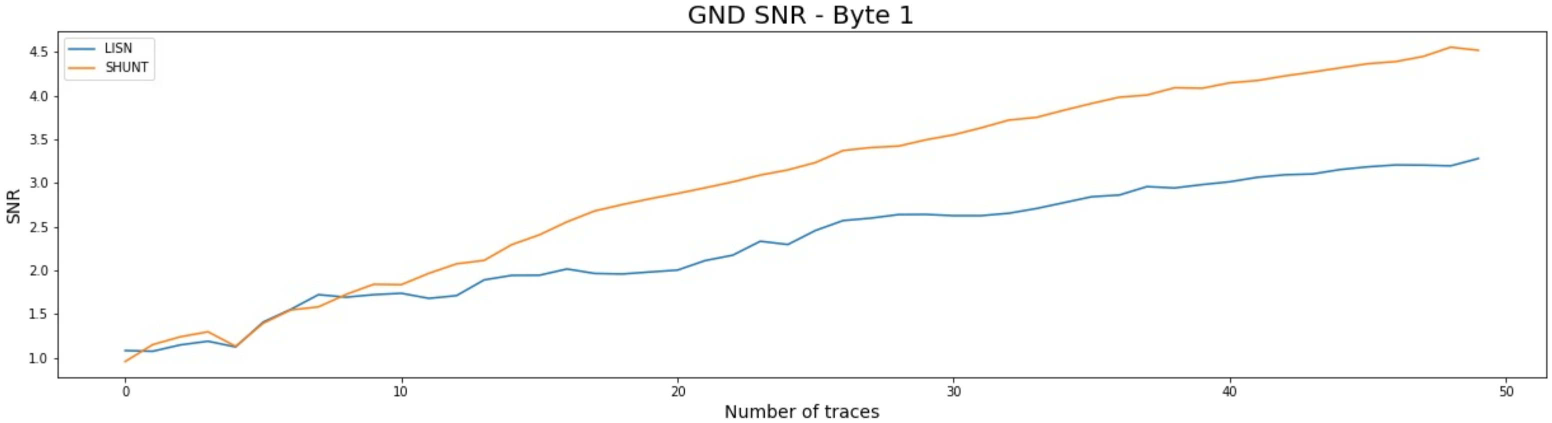
# Comparing CPA techniques

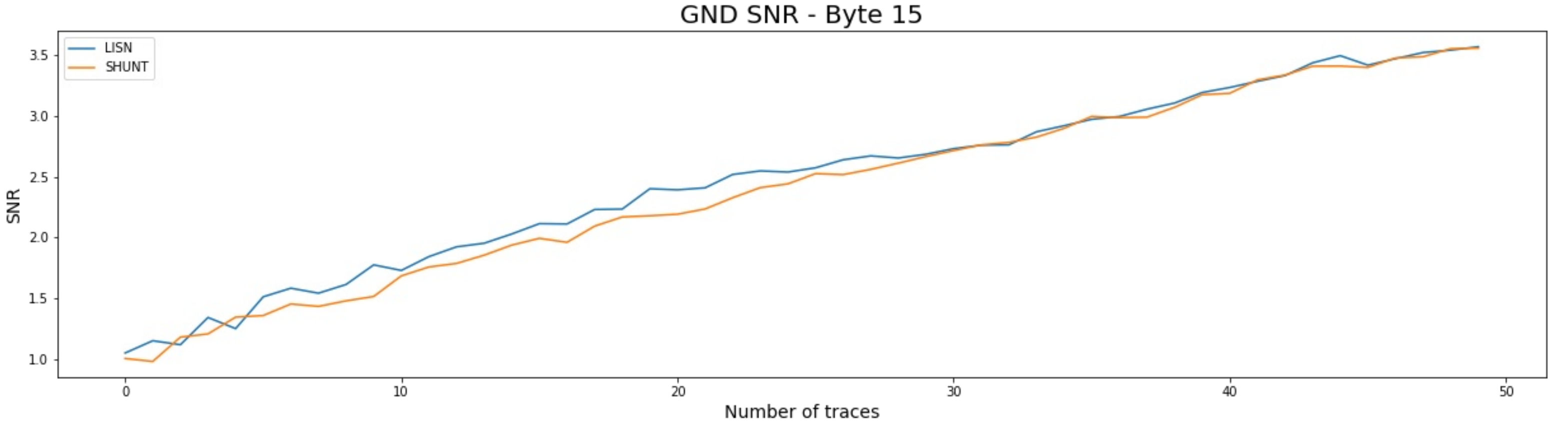
- No “official” way to compare sets of traces
- Ended up with some kind of “Signal over noise ratio”
- <correct guess correlation value> / mean(<other correlation values>)

- Gives a rough estimate of measurement quality

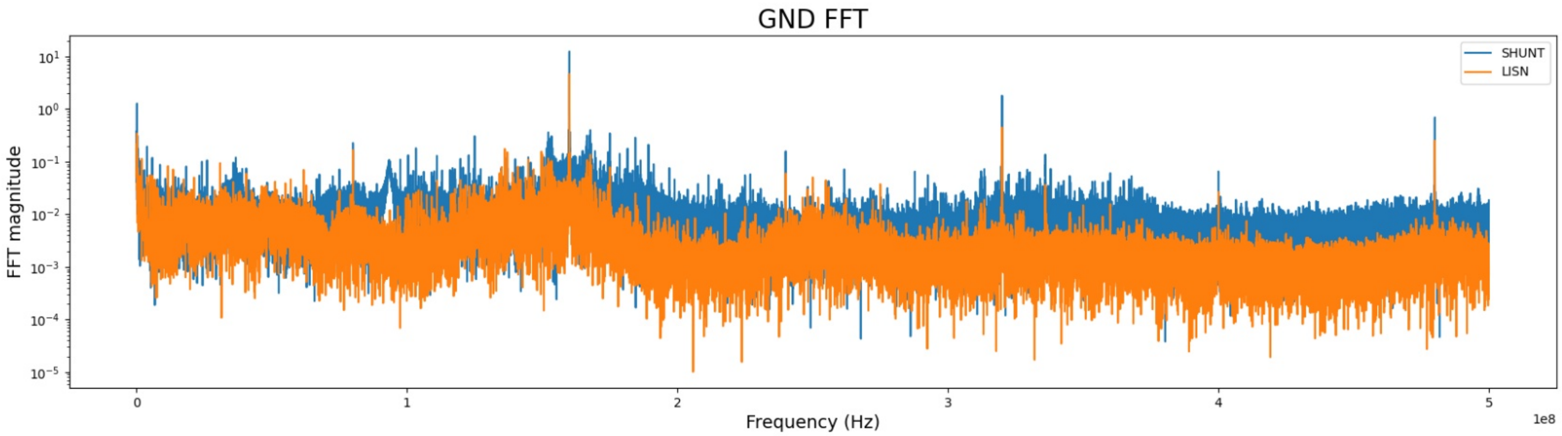


# “SNR” comparison



# FFT comparison

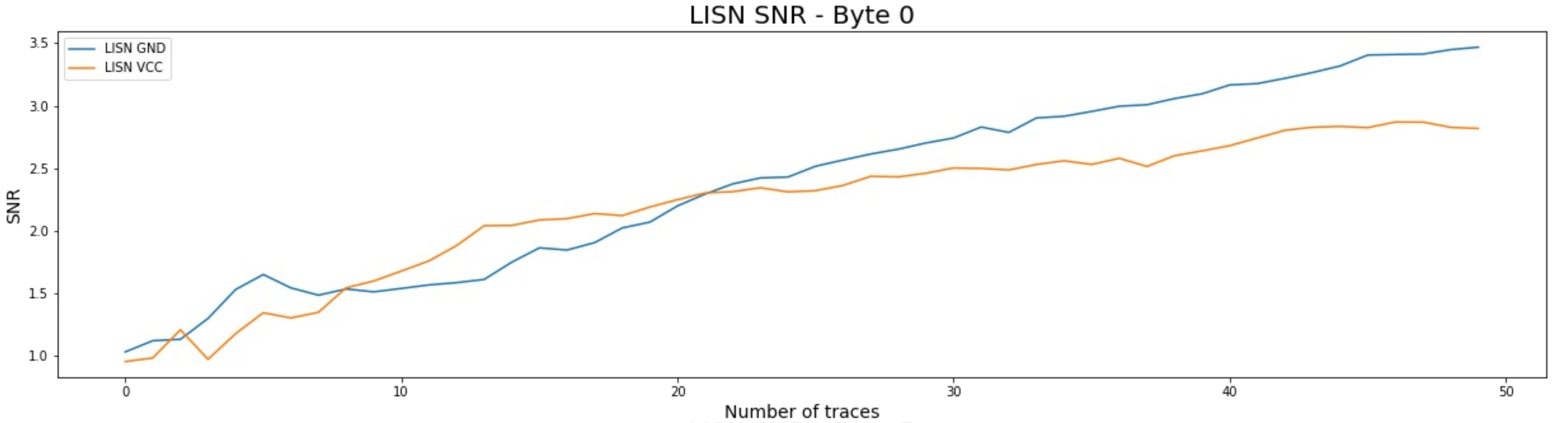


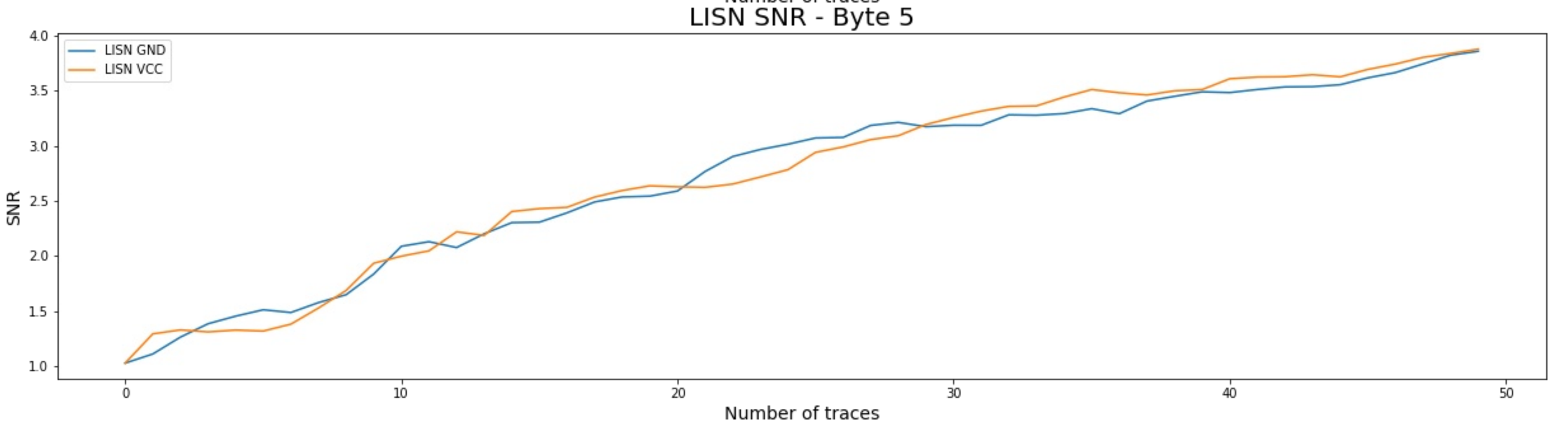
# VCC vs GND

- LISN provides measurement ports on both VCC and GND
- Did same acquisition on each measurement port
    - 50’000 averaged traces, random plaintext

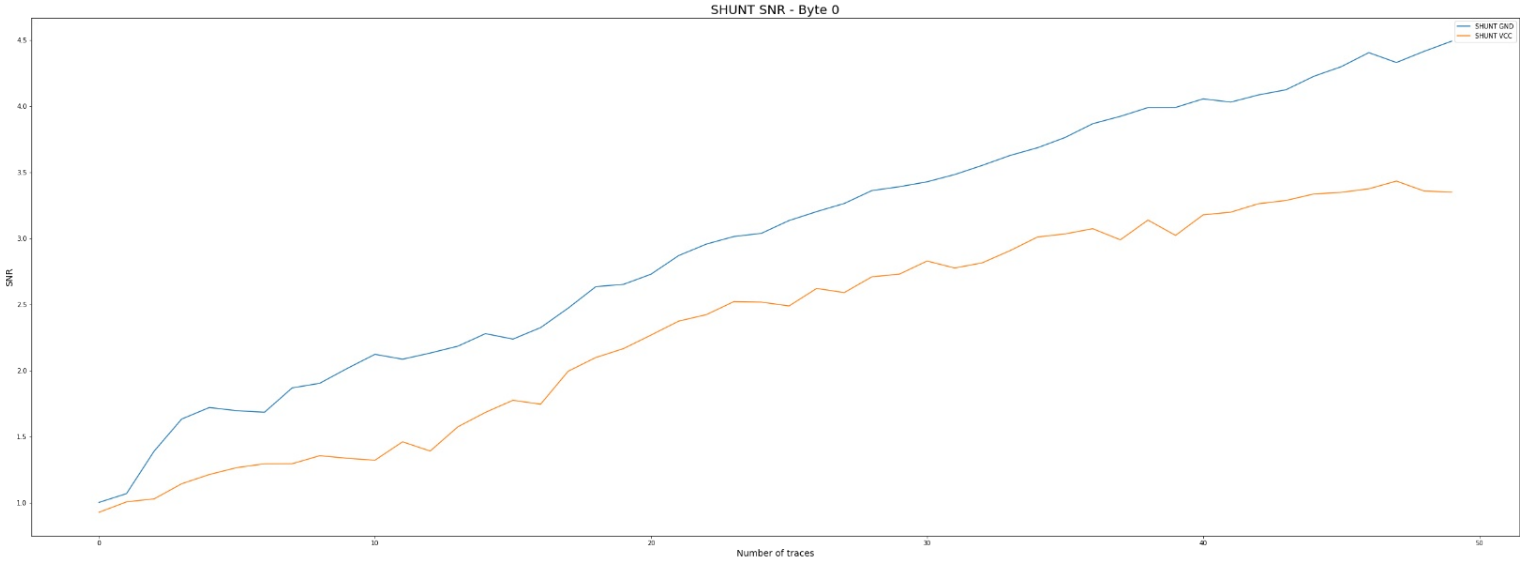
- Measuring on GND provides slightly better results

# “SNR” LISN - VCC vs GND



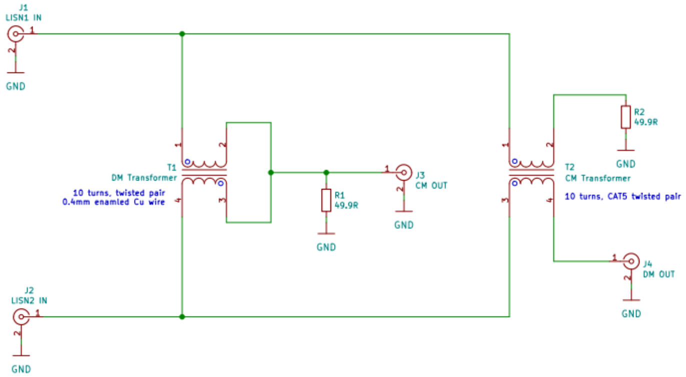
# VCC vs GND - Shunt



# Common mode / Differential mode

- Monitoring both VCC and GND allows to perform differential analysis

- Custom built CM/DM separator





**Differential (Normal) Mode Noise and Common Mode Noise explanation**

https://techweb.rohm.com/knowledge/emc/s-emc/01-s-emc/6899

# CM / DM difference

- Tested on both setups
    - DM signal traces do provide some correlation
    - CM does not
- Might need more tests, as the separator only dampens the other signal


# Conclusions

- LISN provides a different way of acquiring side-channel information
- In practice, similar performance as a shunt resistor
  - Lower inline resistance. Could be useful for specific targets (non intrusive)
  - Signal is already AC-coupled
  - Measure is made on both lines
- EMC testing methodology allows to enhance signal quality by diminishing noise

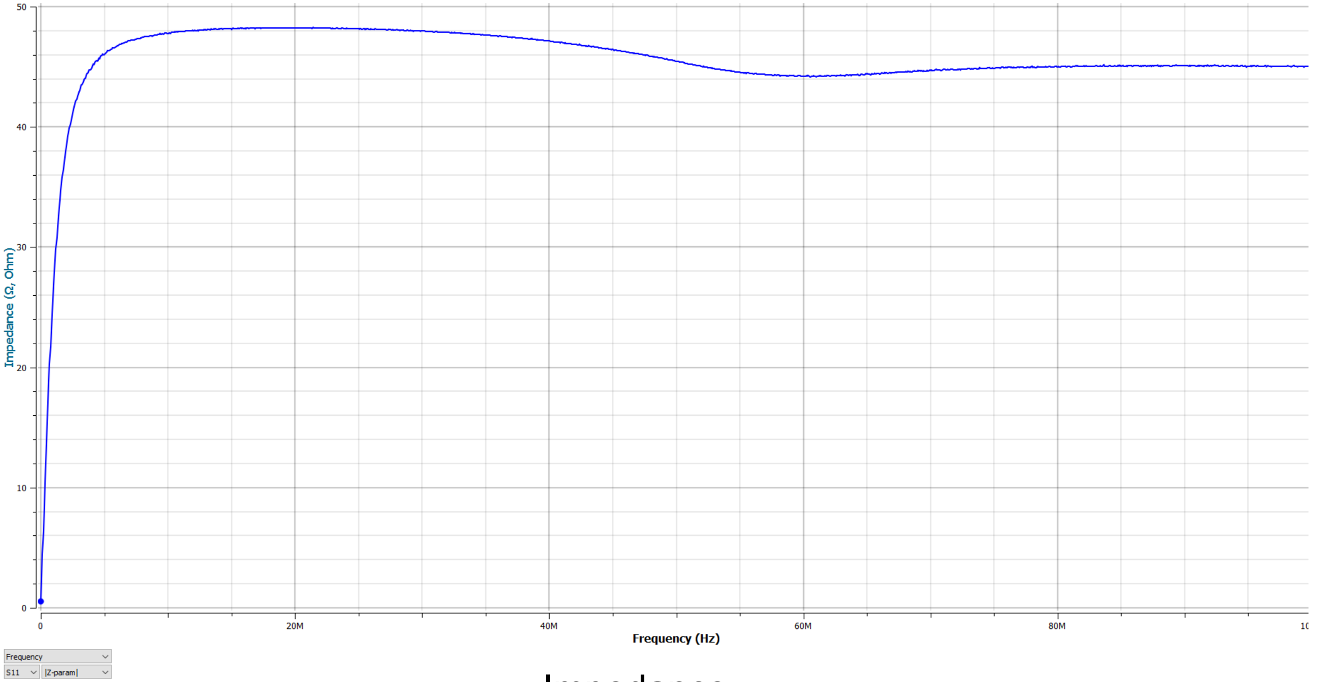
# HydraSCA-LISN Limited Edition hardwear.io NL 2022

Exclusively for hardwear.io NL 2022

We have 8 units available, find us after the talk !

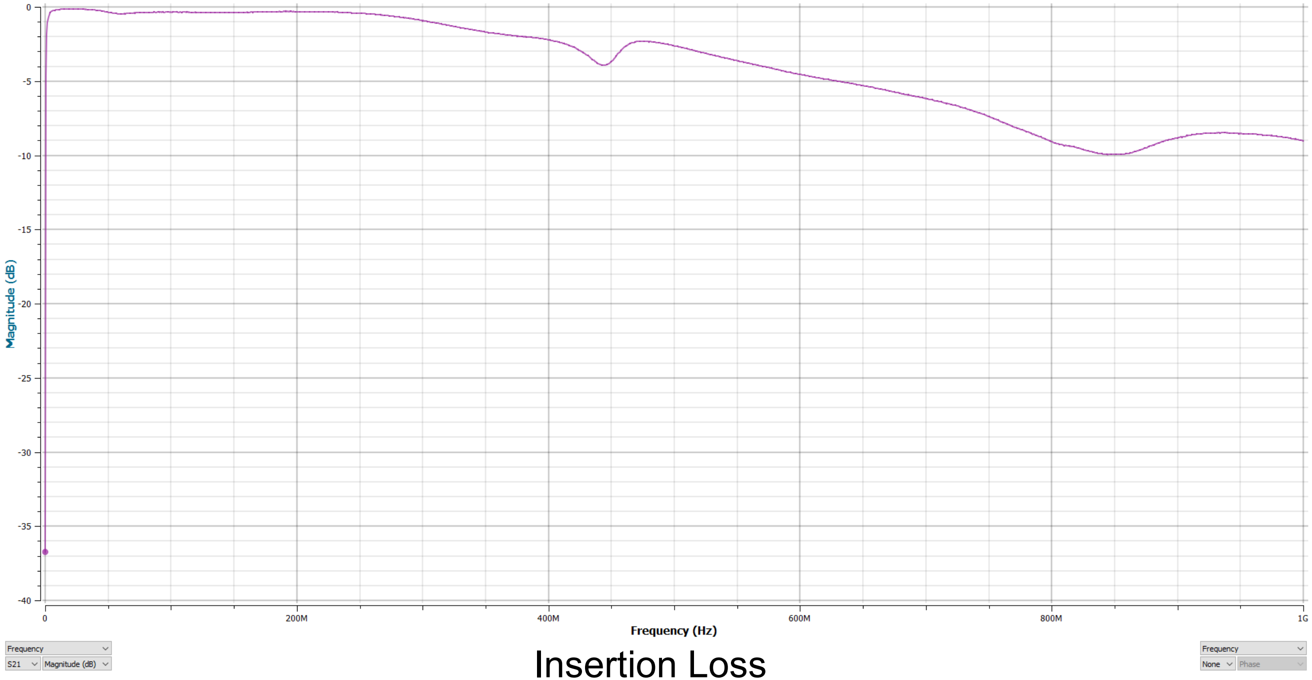
## HydraSCA-LISN V1 R1

# BONUS

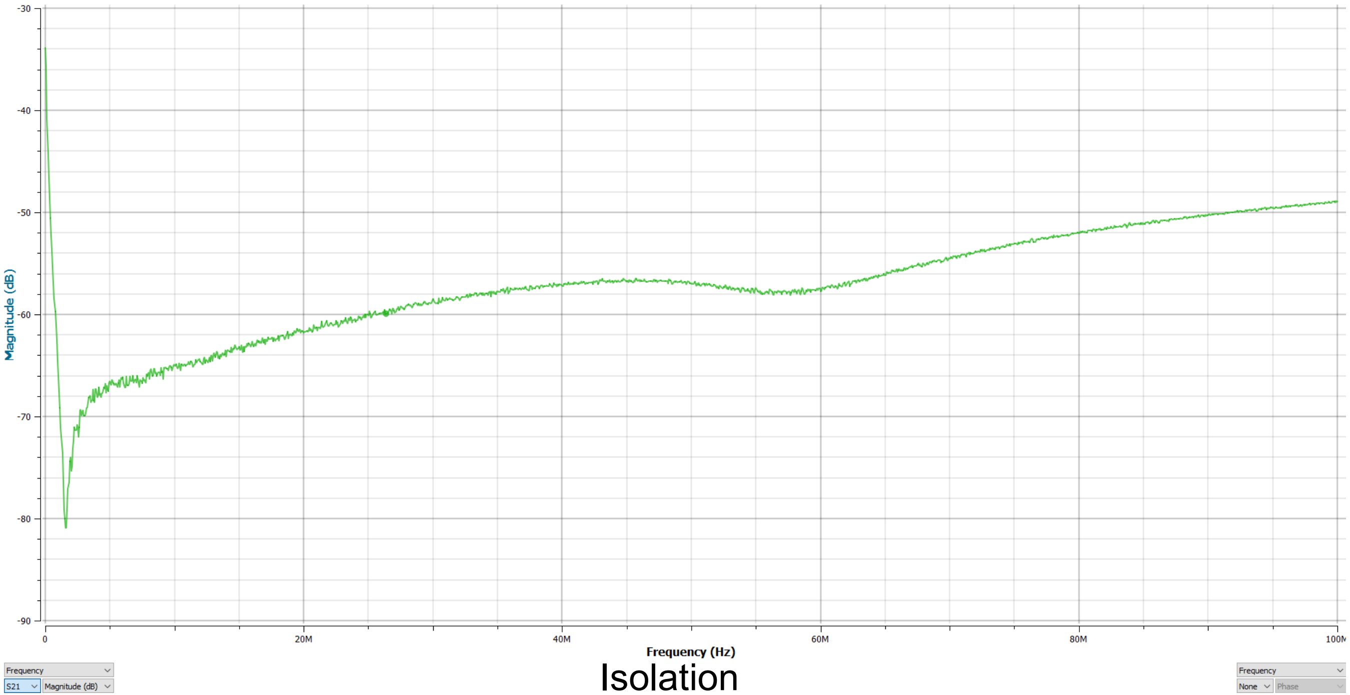

Impedance

# BONUS


Insertion Loss

# BONUS


Isolation