PBS&T

Power Signal Acquisition

Analog Side of Digital Security

Valery Ray

vray@partbeamsystech.com

Outline

- Why acquire power data?
- Shot noise and thermal noise
- Basic current acquisition methods
- Advanced circuitry and simulations
- Conclusions

Power signature is useful for

- Simple Power Analysis (SPA)
- Differential Power Analysis (DPA)
- Prevention of self-erase on secure MCUs
- Could be useful for clock recovery???

Fundamental limit: Shot Noise

- **Flow of DC current is a statistical process and carrying intrinsic shot noise**

$$I_{Ns} = \sqrt{2\, e\, I_{DC}\, \Delta f}$$

Detection of signals with levels below the shot noise floor is impractical

Fundamental limit: Shot Noise

Bandwidth, MHz

Current mA		1	5	10	20	50	100
	1	17.9	40.0	56.6	80.1	126.6	179.0
	2.5	28.3	63.3	89.5	126.6	200.1	283.0
	5	40.0	89.5	126.6	179.0	283.0	400.3
	7.5	49.0	109.6	155.0	219.2	346.6	490.2
	10	56.6	126.6	179.0	253.2	400.3	566.1

Shot noise, nA

Technical Difficulty: Thermal Noise

- Resistors generate "Johnson" noise at any temperature above 0°K

$$I_{Nj} = \sqrt{\frac{4\, k_B\, T\, \Delta f}{R}}$$

Detection of signals below the Johnson noise is difficult, but possible by advanced circuitry

Technical Difficulty: Thermal Noise

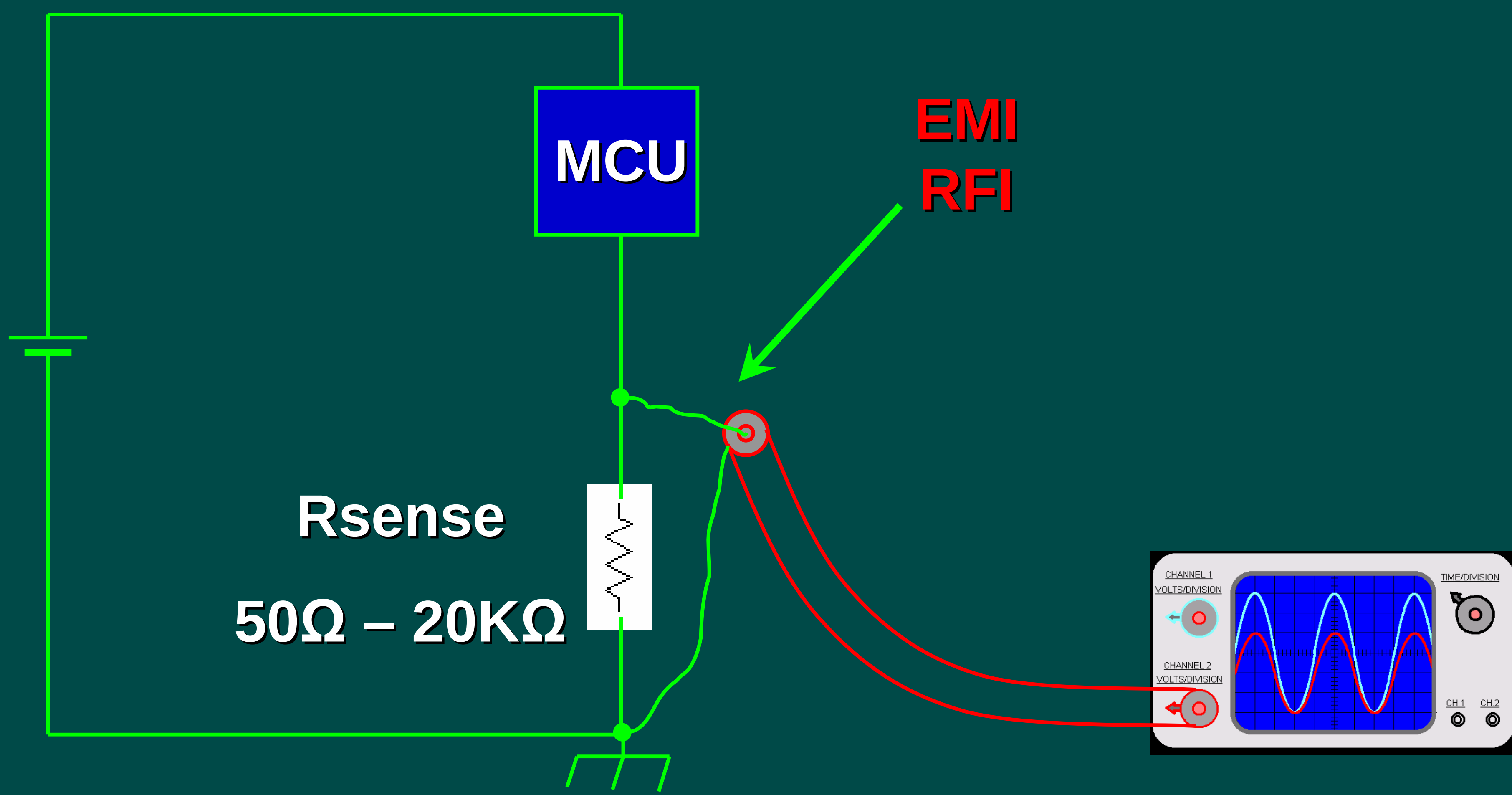
Bandwidth, MHz

Resistor, Ω

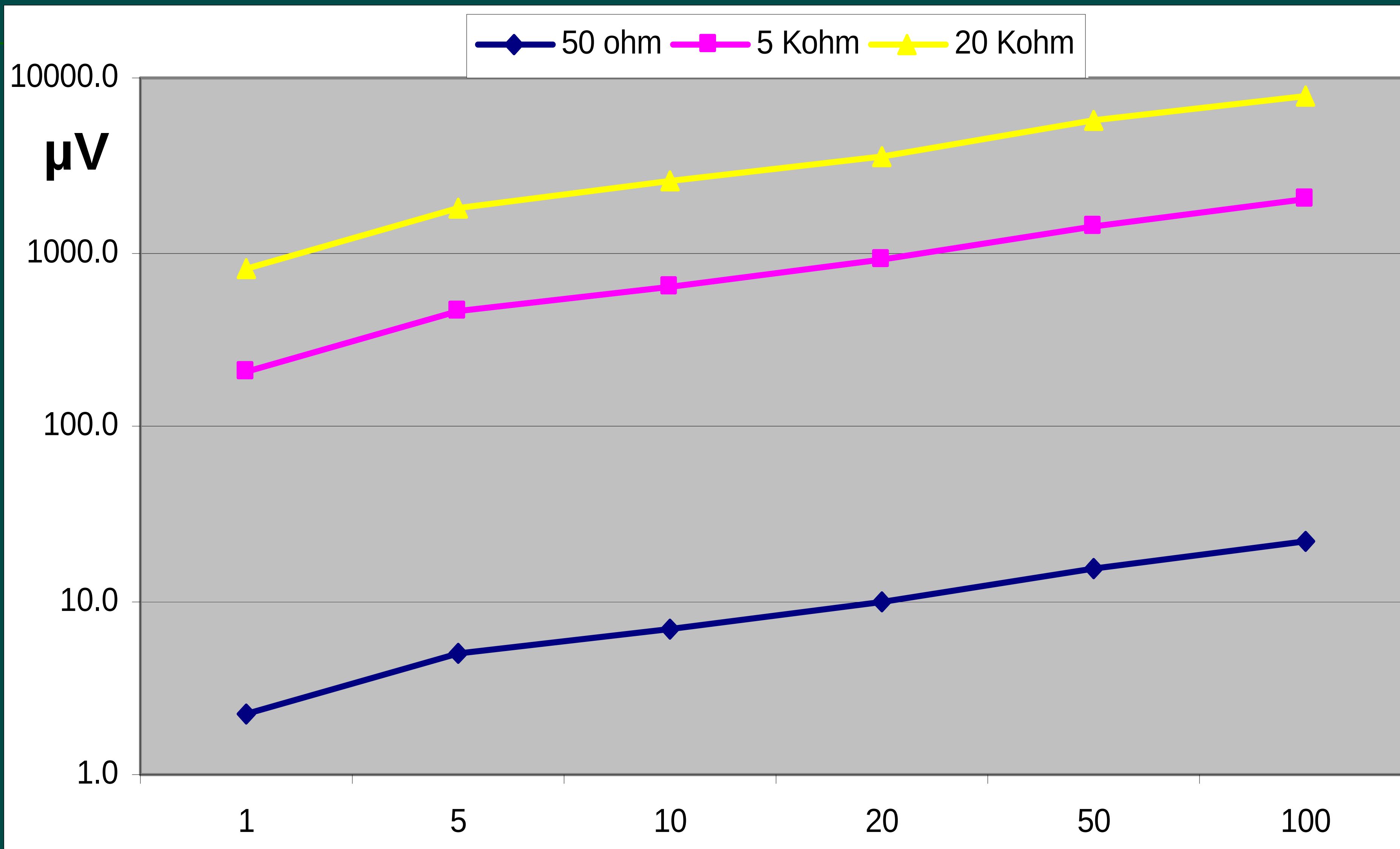
	1	5	10	20	50	100
50	18.1	40.4	57.1	80.7	127.7	180.6
200	9.0	20.2	28.5	40.4	63.8	90.3
500	5.7	12.8	18.1	25.5	40.4	57.1
1000	4.0	9.0	12.8	18.1	28.5	40.4
5000	1.8	4.0	5.7	8.1	12.8	18.1

Thermal (Johnson) noise, nA

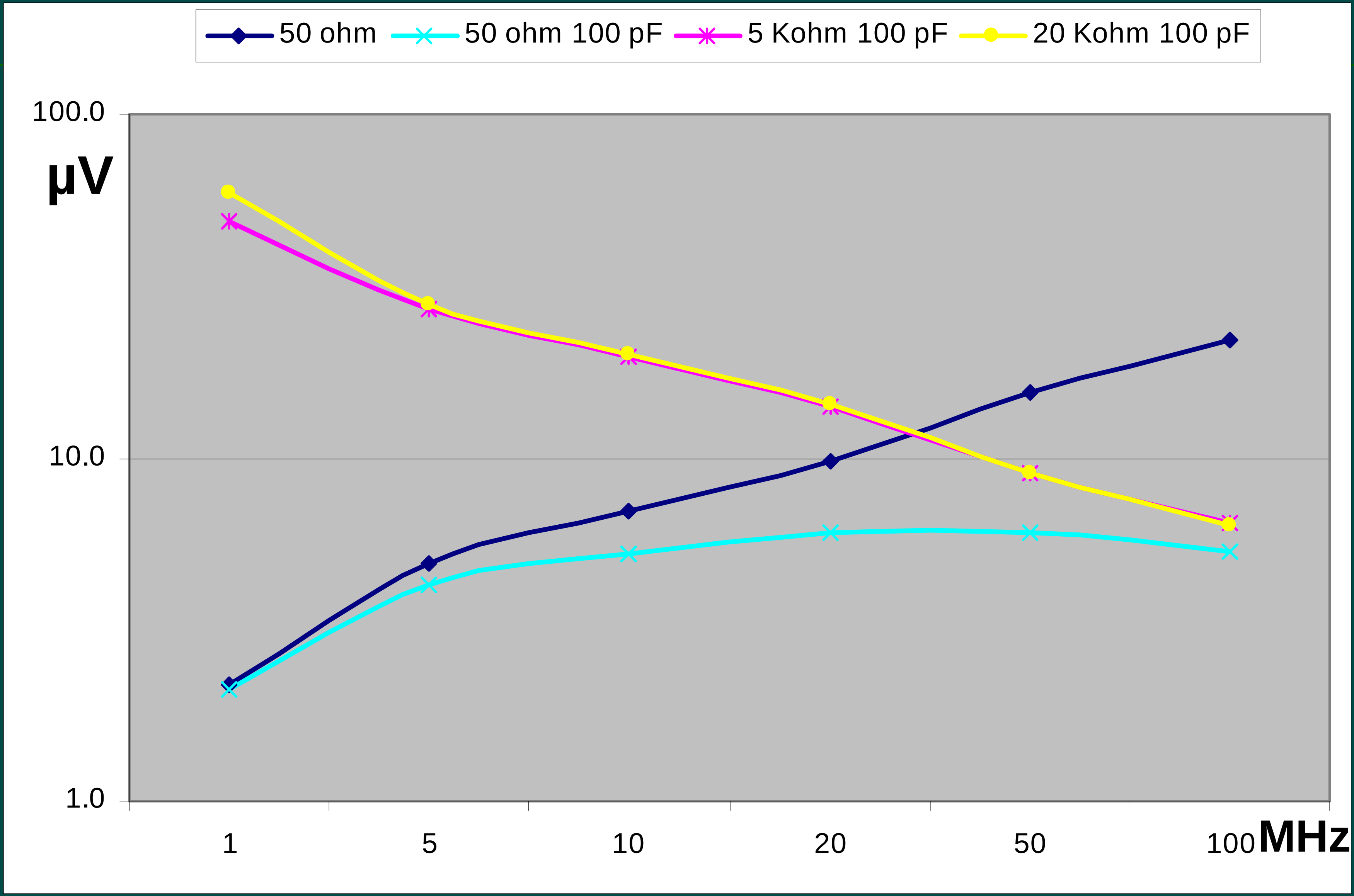
Current Acquisition: Sense Resistor



Combined noise voltage @ 5mA DC



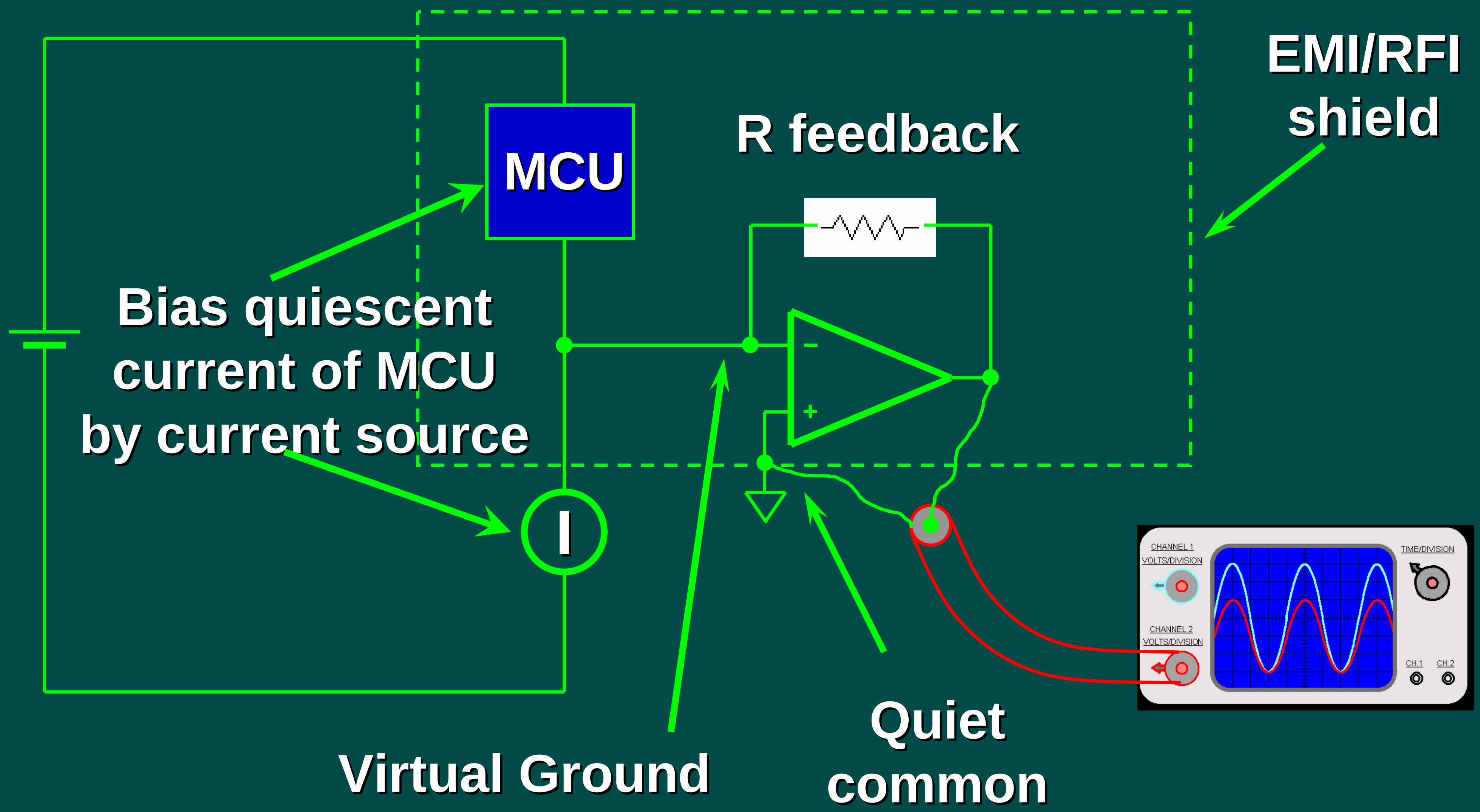
Bandwidth Limitation @ 5mA DC



Limitations of Sense Resistor

- Limited bandwidth
- Signal suppression due to voltage feedback
- MCU “common” is not grounded
- Low level signals are too weak for direct measurements

Transconductance Amplifier

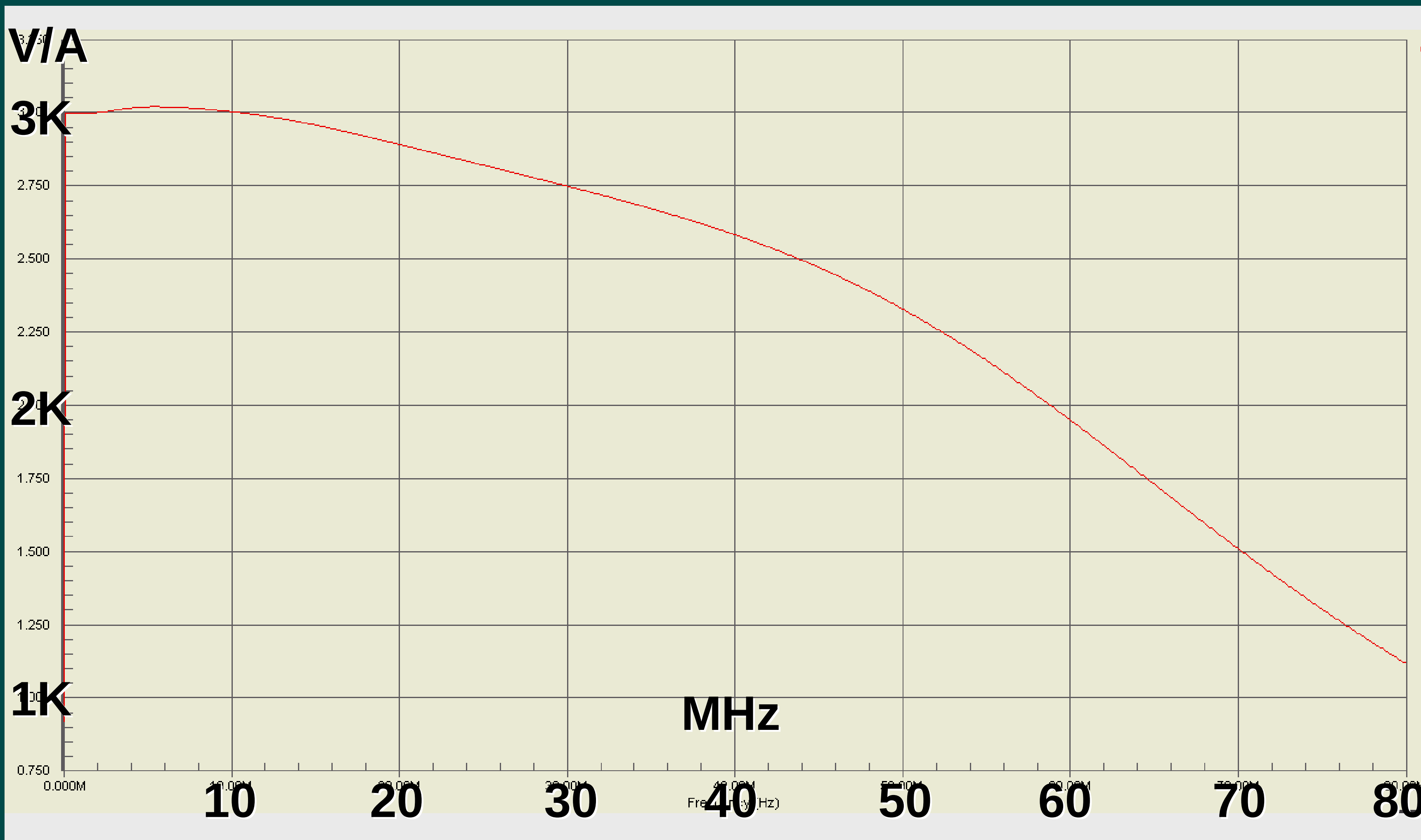


Noise of transcoductanse stage

- **Mainly defined by the operational amplifier;**
- **Amplifiers with noise specifications in the range of single nV and nA are available off the shelf;**
- **Noise contribution from metal film feedback resistor is minimal**

Simulation of Transconductanse Stage: Impulse Response, 500nA signal

Simulation of Transconductanse Stage: Frequency Response, Small Signal



Advantage of transconductanse stage

- Common of MCU is held at ground potential
- Measurement is referenced to quiet ground
- Current signal is amplified by the first stage and converted to voltage at the same time
- Useful bandwidth extends to ~ 50 MHz range and noise floor close to shot noise limit is possible

Difficulties of low current detection

- EMI, RFI – acquisition setup must be shielded
- Power filtering down to shot noise floor
- Decoupling from digital circuitry – interface to MCU must be optically coupled
- Differential measurements to prevent noise injection through ground loops

Conclusions

- Current measurements based on series resistor are limited in sensitivity and bandwidth
- Power channel information leakage from MCU may be happening at signal levels below sensitivity of series resistor approach
- Methods with higher sensitivity to low signals are needed to enable full evaluation

Conclusions

- Shot noise is a fundamental limitation for the current measurements
- Acquisition of current data with levels down to shot noise floor may be possible with low-cost circuitry and off-the-shelf components
- Increased sensitivity of current acquisition could allow development of improved countermeasures to power analysis

www.partbeamsystech.com