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

\[ I_{NS} = \sqrt{2eI_{DC} \Delta f} \]

Detection of signals with levels below the shot noise floor is impractical.
<table>
<thead>
<tr>
<th>Current (mA)</th>
<th>1</th>
<th>5</th>
<th>10</th>
<th>20</th>
<th>50</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17.9</td>
<td>40.0</td>
<td>56.6</td>
<td>80.1</td>
<td>126.6</td>
<td>179.0</td>
</tr>
<tr>
<td>2.5</td>
<td>28.3</td>
<td>63.3</td>
<td>89.5</td>
<td>126.6</td>
<td>200.1</td>
<td>283.0</td>
</tr>
<tr>
<td>5</td>
<td>40.0</td>
<td>89.5</td>
<td>126.6</td>
<td>179.0</td>
<td>283.0</td>
<td>400.3</td>
</tr>
<tr>
<td>7.5</td>
<td>49.0</td>
<td>109.6</td>
<td>155.0</td>
<td>219.2</td>
<td>346.6</td>
<td>490.2</td>
</tr>
<tr>
<td>10</td>
<td>56.6</td>
<td>126.6</td>
<td>179.0</td>
<td>253.2</td>
<td>400.3</td>
<td>566.1</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Resistor, $\Omega$</th>
<th>Bandwidth, MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>18.1</td>
</tr>
<tr>
<td>200</td>
<td>9.0</td>
</tr>
<tr>
<td>500</td>
<td>5.7</td>
</tr>
<tr>
<td>1000</td>
<td>4.0</td>
</tr>
<tr>
<td>5000</td>
<td>1.8</td>
</tr>
</tbody>
</table>

Thermal (Johnson) noise, nA

10/30/2007
Current Acquisition: Sense Resistor

Rsense

50Ω – 20KΩ

MCU

EMI

RFI
Combined noise voltage @ 5mA DC

µV

10000.0
1000.0
100.0
10.0
1.0

1 5 10 20 50 100

50 ohm
5 Kohm
20 Kohm

10/30/2007
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

- Bias quiescent current of MCU by current source
- Virtual Ground
- Quiet common
- R feedback
- EMI/RFI shield

Bias quiescent current of MCU by current source.
Noise of transconductance 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 Transconductance Stage: Impulse Response, 500nA signal
Simulation of Transconductance Stage: Frequency Response, Small Signal
Advantage of transconductance 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