*Journal of* ELECTRICAL ENGINEERING, VOL 63. NO 7s, 2012, 75-78

# RECONSTRUCTION OF MULTIPLE SIGNALS FROM ELECTROMAGNETIC COIL MEASUREMENT

**Gabriel Války***

This paper deals with electromagnetic coil measurement where a transmission on synchronous bus is captured, amplified and analysed for reconstruction of multiple digital bus signals. This process is performed on handheld oscilloscope for designing a small and portable eavesdropping device that is able to monitor a communication between computer and keyboard by placing this device on keyboard cable. For reconstruction of highly degraded signal, methods of adaptive filtering are applied.

Keywords: coil measurement, measurement automation, adaptive filtering

## 1 INTRODUCTION

Some more advanced electro-technical measurements require set of measurement devices, computer and some bus for interconnection of these devices with PC. There are also computer programs that improve the designer productivity by drawing logical schemes instead of writing code. These programs are for example NI LabView and Matlab Simulink. Measurement setups automated with these tools are usually connected to GPIB bus, and in final stage they cover whole the desk and are not mobile, thus not suitable for in-field use. In this paper we utilize open source all-in-one measurement system DS203 offering sufficient computational power that can be used as 4-channel oscilloscope and signal generator in mobile phone sized gadget. We will explain the process of developing specialized software for this device that captures electromagnetic disturbances picked up by electromagnetic coil placed near PC keyboard cable. Sampled signal will be processed in real time for the reconstruction of the synchronous serial bus of PS2 keyboard protocol and decoded scan-codes will be displayed in human readable form directly on the DS203 screen. In result we will have the device that is able to monitor everything typed on keyboard and this should be useful for evaluating the security competence of workplace.

## 2 DS203 OSCILLOSCOPE

Oscilloscope DS203 is a battery powered gadget with 32-bit microcomputer ARM Cortex M3. For high-speed sampling, Analog Devices AD9288 chip is used. This 8-bit AD converter is controlled by the field programmable gate array lattice iCE65L04 and together sample rate up to 72 Msps on single channel can be achieved. This FPGA is also used as the memory for 4096 sampled values. These values are processed by the microcomputer and displayed on 400x240 pixels 2” colour LCD. For charging, file transfer, uploading new firmware and remote control an USB micro connector is used.

Its firmware is programmed using object oriented C++ language and for compiling and uploading the firmware onto device, no commercial products are required. Firmware [1] offers the ability to control this device remotely from host PC. For this purpose a special utility was developed that communicates with the device using Mass Storage USB Class and forwards all transferred data through network sockets and thus allows to communicate with WebSocket enabled web browsers. This remote control can be accessed also from any programming language that supports network sockets. HTML5 with JavaScript was chosen as the language that is available on any computer platform, is widely used and easy to learn, with ability to create vector graphics and interactive programs.

## 3 DEVELOPMENT PROCESS

The evolution of automated measurement system from ordinary laboratory equipment into standalone DS203 software module can be explained in following steps:

1. Create a measurement setup with ordinary equipment (data acquisition cards, signal generators, power supplies), controlled with any graphical design tool
2. Simplify and fine-tune this algorithm
3. We will use DS203 as data acquisition device or signal generator or controlled voltage source with the same algorithm
4. Instead of graphical design tool, we rewrite the algorithm into JavaScript/html (since JavaScript is similar to C++, but possesses the properties of scripting language, thus the programming process is very fast)
5. If everything is working well, we rewrite the algorithm into C++ language to be able to compile it as a module for DS203 firmware
6. Testing on PC – DS203 firmware is designed to run in virtual environment as Win32 desktop application, the oscilloscope will be sampling software generated waveforms
7. Compiling the module for ARM M3 platform
8. Uploading new firmware onto DS203 device
9. Testing.

* Slovak University of Technology, Faculty of Electrical Engineering and Information Technology, Department of Electrical Engineering, Ilkovičova 3, 812 19 Bratislava 1, Slovakia, gabriel.valky@stuba.sk

ISSN 1335-3632 

## 4 ELECTROMAGNETIC COIL MEASUREMENT

In this paper we are examining the possibilities of eavesdropping of digital communication between keyboard and computer. For simplicity, we focus on PS2 technology, where the cable connecting keyboard with computer is forming a two wire synchronous bus. There are four wires – two for providing power for the keyboard, one clock signal and one data signal. We measure the electromagnetic field that is produced when voltage level on one of these signals changes. The finest resolution of DS203 oscilloscope is not sufficient for such small signal measurement from electromagnetic coil. This problem is solved by amplifying the signal with low-noise amplifier (LNA) with the gain of 60 dB (Fig. 1).

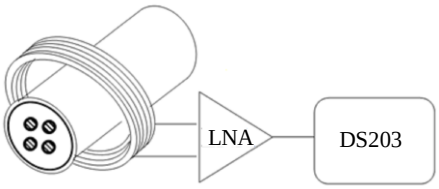


**Fig. 1.** Measurement setup

After configuring the oscilloscope, the algorithm waits for trigger to fire. Subsequently, whole sample memory is downloaded from FPGA into microcomputer memory and modified FIR filter is applied on these data. We try reconstructing the impulses that originate in logical level change on data or clock wire. If this succeeds, and the set of identified impulses can be recovered into possible data and clock signals and scan-code can be calculated, with lookup table this scan-code is converted into an ASCII character and displayed on the device screen. After successful reconstruction we repeat this process to identify the next keystroke. When the reconstruction fails, we modify the filter attributes randomly and try to recover the scan-code in the same way as described before. If the reconstruction succeeds, new filter coefficients are stored for using them as initial guess for reconstructing the next keystrokes. When it is not possible to identify the filter coefficients that would lead to recovery of scan-code after 100 attempts, an error message is displayed. This may be caused by following reasons:

- Signal is too noisy
- Sampled buffer does not cover whole bus transmission
- Unwanted signal caused trigger to fire

This algorithm is depicted in Fig. 2.

## 5 BUS SIGNAL RECONSTRUCTION

Figure 3 demonstrates the original sampled waveform when the left shift key is pressed (scan-code = 12h), waveform after adaptive FIR filtering [2] where the positive and negative peaks can be distinguished, reconstructed bus signals with logical values on falling edge of clock signal.

Adaptive filtering is used to reduce the noise and unwanted oscillations from the original waveform. A series of positive and negative peaks are identified after this filtering and these correspond to the change of logic levels on bus wires. Analyzing the times between these peaks we can identify the peaks belonging to clock signal. These peaks occur in regular intervals and have always opposite polarity. Remaining peaks are used to recover the data signal.

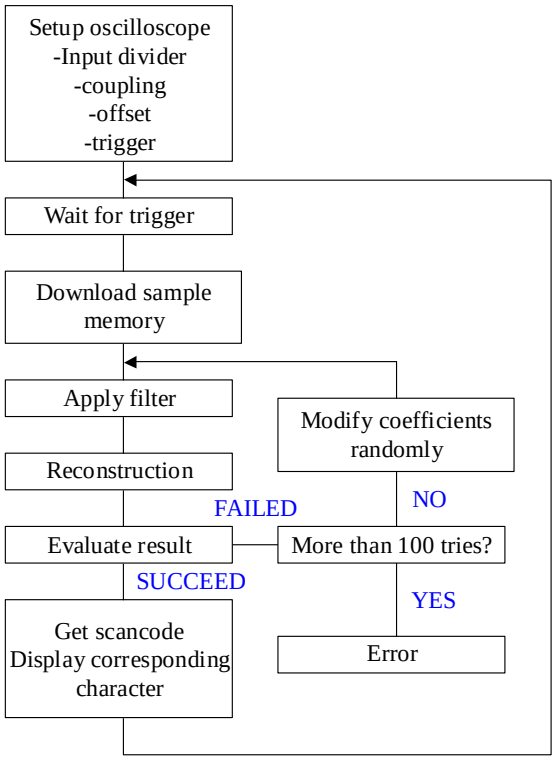


**Fig. 2.** Block scheme of reconstruction algorithm

The attributes of adaptive filter are dependent on the position of coil with respect to the measured cord and are evolving in time. Thus we need some feedback indicating the suitability of filter coefficients. Main task of the filter is providing a signal that can be used to easily identify peaks. Feedback in our case is a real number value representing this ability. This value is also penalized in case an incorrect series of peaks was identified. For this purpose we designed simple algorithm that increments a value when positive peak was found and decrements in case of negative peak. At the beginning this number is set to zero and when it reaches value outside the interval <-2, 2>, it indicates the error. When it is not possible to recover the clock signal or two consecutive data signal peaks have the same polarity, it also means that the filter failed to do its task.

## 6 MODIFIED FIR FILTER

For filtering purposes we designed custom type of filter is based on FIR filter (finite impulse response). Conventional FIR filter [3] (Fig. 4) multiplies its coefficients with values that are sampled in whole-number multiples of sampling period.

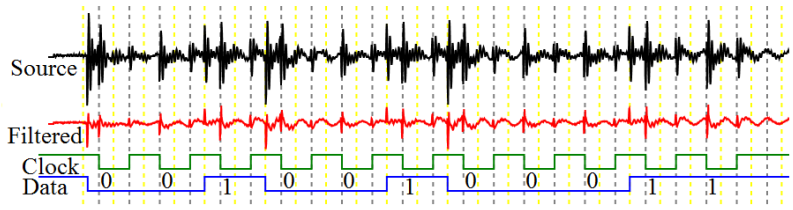


**Fig. 3.** Sample signal, filtered and reconstructed bus signals

In its graphical representation on figure 5 we see its integral parts: Shift register that provides last N samples of sampled signal, corresponding number of multipliers ($N + 1$) and all partial results are summed together with ($N$) adders. Such filter can be characterized by time coefficients $n_0$, $n_1$, $n_2$, ... $n_N$ (for figure 5: $n_0 = 0$, $n_1 = -1$, $n_2 = -2$, $n_3 = -3$, $n_4 = -4$) and multiplier values $h(0)$, $h(1)$ ... $h(N)$ of $N$-th order FIR filter.

Conventional FIR filter did not provide sufficient variability for processing data from our measurement setup. The problem was the low resolution of sampled signals from the coil. Increasing the sampling speed would lead to situation, when whole bus transmission would not fit into oscilloscope memory and also the filtering process would require more computational power. Therefore we were looking for other methods to artificially increase the time resolution of measured samples.

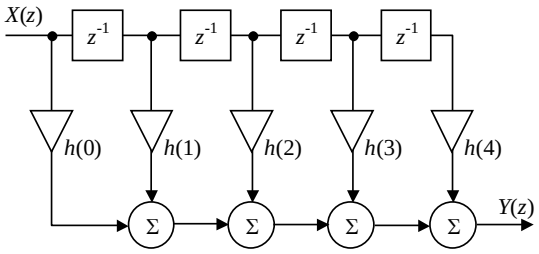


**Fig. 4.** Conventional finite impulse response filter

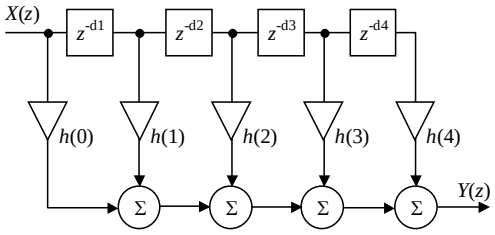


**Fig. 5.** Modified finite impulse response filter

We designed a modified filter, which allows calculation with samples which were not really sampled by ADC, but these values are calculated using interpolation. In conventional FIR filter, the time coefficients are whole non-positive numbers, where our filter allows referring to samples with real number time coefficients. Replacing the shift registers with delay circuits in Fig. 4 we get block scheme of modified FIR filter described in this paragraph (Fig. 5).

For the interpolation of values between samples we used Sinc interpolation [4]. Fig. 6 depicts the approximation of signal value between two samples. Input signal is sampled in regular intervals, the samples $x(n - 1)$, $x(n)$, $x(n + 1)$ are shown as black dots. For the interpolation in point $n + P$, where $P \in \langle 0, 1)$ we overlay the Sinc function over these samples relative to the time point $n + P$. The sample values are multiplied with values of Sinc function in points corresponding to the time when the signal was sampled (shown as circles) and after summing we get the result.

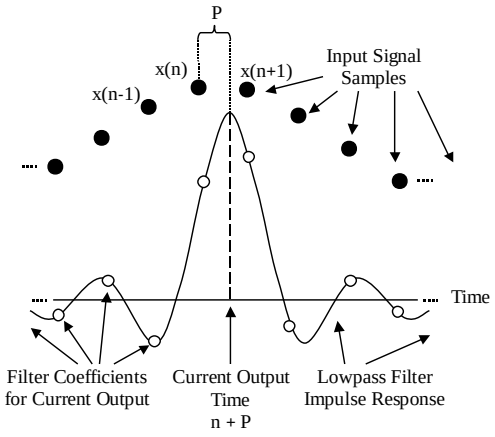


**Fig. 6.** Sinc interpolation

## 7 ADAPTIVE FILTERING

Correct setting of filter is important for successful signal reconstruction of small and noisy signals. Finding the most suitable filter coefficients is a complicated task, since they depend on the keyboard model, computer and position of measurement coil relative to the cable. The ability of self calibrating is thus a necessary part of this measurement system.

After powering on the DS203 with PS2 bus decoder module, it uses predefined filter settings. These can evolve in time to better match specific situation. For each filter setting we can calculate the signal quality indicator which is a real number indicating the ability of isolation logical level changes in coil measurement after filtering. In case we fail to reconstruct the bus signals, the algorithm randomly modifies the filter parameters for finding the best signal quality. The random number generator generates numbers with Gaussian distribution, with $\mu = 0$, $\sigma = 2.0$ for time coefficients and $\mu = 0$, $\sigma = 0.5$ for multiplication coefficients. This ensures that the filter coefficients are modified only partially in most of the iterations, but with smaller probability it is possible to change the attributes to completely another configuration. For the purpose of generating random numbers with Gaussi-

an distribution, we implemented an algorithm based on Box-Muller transformation [5].

## 8 FINAL APPLICATION

Presented solution with block scheme depicted in Fig. 2 was implemented as the application module for DS203. By connecting battery-powered low-noise amplifier between the electromagnetic coil and oscilloscope, we have an apparatus able to monitor keyboard activity and log all keystrokes into the device memory.

Fig. 7 shows the device screen when a message "Ahoj, toto je pokus!" was typed on a keyboard. On the screen we can see current filter settings, quality of signal indicator, count of successful and failed reconstructions, in the grey rectangle the ASCII characters in human readable form are displayed. On the bottom of the screen the last scan-code (or scan-codes) with trigger or calculation state is displayed. All decoded scan-codes, corresponding characters, and debugging information are stored into the internal memory of the device for further processing.

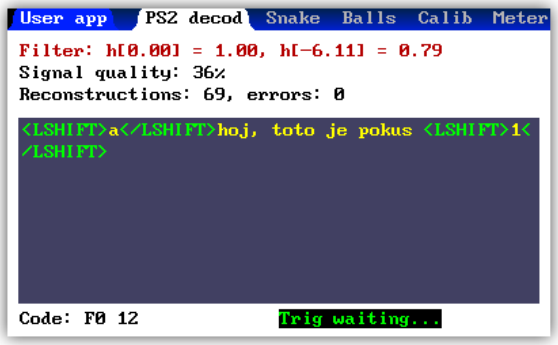


**Fig. 7.** Running DS203 application

## 9 POSSIBLE EXTENSIONS

We were also investigating the possibilities of measuring electromagnetic interference with directional antenna. For evaluation of this approach, we placed the keyboard with tablet computer in an electromagnetically isolated anechoic chamber and in the distance of 3 meters we measured the radiated spectrum by means of the spectrum analyser. Tablet computer with USB-to-PS2 adapter was covered in an aluminium foil for suppressing the tablet radiation into the cabin. Aluminium foil was connected to PS2 connector grounding and also to the cabin ground. At first we measured the spectrum with keyboard kept intact (grey line in Fig. 8). Then we placed a wooden block on arrow down key to keep it sending the scan-code in regular intervals. Many new peaks appeared on the measured spectrum (black line in Fig. 8), some were located around frequencies 33 MHz and some peaks in the range of 100 to 200 MHz. The reconstruction of the keystrokes with heterodyne receiver will be subject of our further research with the aim to create a standalone and portable device able to monitor the typing on the keyboard from larger distance. There are already some publications focused on this task [6], but they require large computational power and complicated measurement equipment and still do not achieve real-time decoding performance.

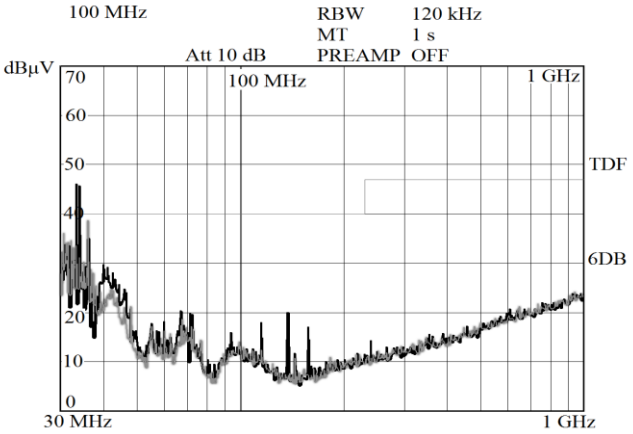


**Fig. 8.** RF emissions from keyboard

## 10 CONCLUSION

In this document we demonstrated how a measurement from the electromagnetic coil can be automated using portable oscilloscope; for the processing of sampled signal we applied adaptive approximation and interpolation methods. This paper also shows how the available microcomputer based mobile devices possess sufficient computational power for advanced calculation, which was previously carried out mostly on personal computers or specialized hardware.

**Acknowledgement**

This work was supported by project VEGA No. 1/0963/12.

### REFERENCES

[1] VÁLKY, G. – KAMENSKÝ, M. – KOVÁČ, K.: Customized firmware for open source oscilloscope, In KOZÁKOVÁ, A. ELITECH´12 : 14th Conference of Doctoral Students. Bratislava, 22 May 2012. Bratislava: Nakladateľstvo STU, 2012

[2] HAYKIN, S.: Adaptive Filter Theory (3rd Edition), Prentice Hall, 1995, pp. 95-110

[3] ONDRÁČEK, O.: Signály a sústavy, STU Bratislava (2008), ISBN 978-80-227-2695-5. (in Slovak)

[4] DEVORE, R. – DAHMEN, W. – KUNOTH, A.: Multiscale, Nonlinear and Adaptive Approximation, Springer (2009)

[5] EVERETT, C.: The generation and Application of Random Numbers, Forth Dimensions (1994), Vol. 16, No. 1 & 2

[6] VUAGNOUX, M. – PASINI, S.: Compromising electromagnetic emanations of wired and wireless keyboards, SSYM'09 Proceedings of the 18th conference on USENIX security symposium (2009), 1-16

Received 8 September 2012

**Gabriel Války** (Ing), born in Galanta, Slovakia in 1985. He received the Bachelor's and Ing. degrees in electrical engineering in 2009 from the Faculty of Electrical Engineering and Information Technology (FEI) of the Slovak University of Technology (STU), where he is currently working toward the PhD. degree. His current research interests include digital signal processing on embedded devices, digital circuits and electromagnetic compatibility testing in the time domain.