Highly reliable data logging in embedded systems

György Györök[1], Bertalan Beszédes [1]
1 Óbuda University, Alba Regia Technical Faculty, Budai Str. 45, H-8000 Székesfehérva´r
{gyorok.gyorgy, bertalan.beszedes}@amk.uni-obuda.hu

Abstract— **In civil and industrial areas often a task to log the data of an embedded system. In some applications the redundant data storage and archiving is required. In the field it can be occur, that the device suffers some electromagnetic impact. It can cause for example, some high current industrial device, a near lightning strike, a transient electromagnetic disturbance, EMP jamming, etc. It can cause damage in the data measured by the embedded system. In this paper shows an architectural solution to keep the data safe, or flag the exact part of the data, which can contain errors.**

I. INTRODUCTION

An Embedded System in general, is a computer system that performs a specific function as part of a more complex electrical or mechanical system. This is different from a Personal Computer which is a general purpose computing device that can be used for many different applications.

Embedded systems mostly performs a very simple task. In many cases an inexpensive microcontroller can be used for applications, where may not require a large amount of computing power. For higher end applications, a digital signal processor, an FPGA [2], or a mainstream processor may be needed.

A. Applicability Area

The application area of embedded systems run from consumer applications to mission critical industrial applications, some of them requires a data storage.

To give a few examples for mission critical consumer systems, it would be cellular base stations, aircraft flight control systems, process control systems and many others. [3] Some industrial storage applications:

- Data logging
- Video capture systems
- Oil and Gas Exploration
- Outdoor Signage
- Avionics and Satellite Systems
- Mining Vehicles and Equipment
- Heart Rate Monitors
- Defibrillator
- Cellular Base Stations
- Central Office Systems

B. Data Storage Devices

Regardless of the specific application carried out by the embedded system, a thorough analysis by the system determine the requirements of the storage solutions. Flash storage devices is the most common for these applications.

In the market there is a lot of product, which can meet the requirements, like:

- CompactFlash
- PC Card (known as PCMCIA ATA Memory Card)
- IDE DOM (Disk-On-Module)
- USB DOM
- USB Flash Drive
- SDChip
- microSD Card
- SD Card
- CFast
- mSATA
- Slim SATA
- M.2
- Slim SATA
- SATA II/III SSD
- IDE SSD

These devices come in a wide variety of interfaces, technologies (SLC - Single Level Cell, pSLC – Pseudo SLC, MLC - Multi Level Cell, TLC - Tri Level Cell), power needs (3.3V - 12V) and used communication protocols. The architecture described below can be used for all mentioned solutions.

C. Application area

In this paper shows an application where the system also need to be protected against their user, who can try to manipulate the logged data.

One of the tasks of security guards is to walk around the guarded area on a specified route. On this route there are local check in stations, where the guard need to touch his RFID card, to prove the area had been checked [11]. These check in data are logged in a solid state data storage device. If the security guard would like to ease his work, the stored, logged data can be modified by him.

If there is a backup data storage, which is responsible for archiving the – possibly encrypted – logged system data, and the security guard have no chance to access to this only writable data storage, the data modifications can be observed and traced. This method is increasing the protection level of a building or an area.

978-1-5386-4772-1/18/$31.00 ©2018 IEEE

II. ELECTROMAGNETIC INTERFERENCE DETECTION

A. Sensor Network

Any external effects that can disturb electrical circuits by way of induction or radiation. Magnetic and electric field probes are low-cost to use. It only need to fit the probes to the input of the microcontroller. This can be done a proper interface module, which contains an amplifier, a level shifter, a peak detector and a protecting circuit (shown on Fig. 1).

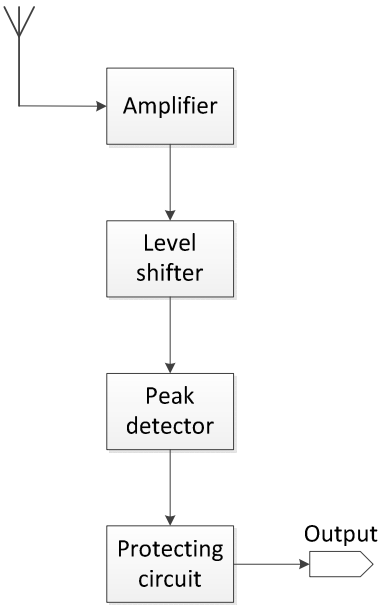

Figure 1. Sensor interfacing module block diagram

To detect electromagnetic fields [4], one possibilities are E-Field probes (Fig. 2. a) (or a simple antenna), which respond primary to electric fields – which are produced by voltage changes – and basically insensitive to field orientation. Another possibilities are the H-Field probes (basically a grounded loop), which respond primary to magnetic fields – which are produced by current changes – and they are sensitive to orientation. H-Field (Fig. 2. b) probes are only respond the current that is in the same plane as the loop, it means it can detect current changes only from two directions. To detect – and log – the incoming direction of the magnetic field, it need to use at least three H-Field probes. (An unshielded loop can detect both electric and magnetic fields, shown on Fig. 2. c) [3] The power lines also important to measure, Fig. 2. d shows the testing loop [5]. The power line cable passed through in a split RF suppression ferrite cylinder (with clip-on housing), along with the loop of coax, with center conductor bonded to shield (using a shield clamp).

B. Measurement Principle

It is expedient to give an external interrupt for the microcontroller, if any of the probes are detected higher electromagnetic interference than it is allowed. This function is realized by the precision, high output impedance peak detector circuit, and the reference comparator. If the reference level is scalable – the reference voltage of the comparator is programmable by the microcontroller –, than the electromagnetic interference detector is customizable, and can take adaptive features also [6].

EMIRR is measured in decibels (dB), similar to power-supply rejection ratio (PSRR) and common-mode rejection ratio (CMRR) parameters, for a specified operational amplifier. EMIRR is a logarithmic ratio where higher decibel values correspond to better rejection and higher immunity. EMIRR is calculated by the following:

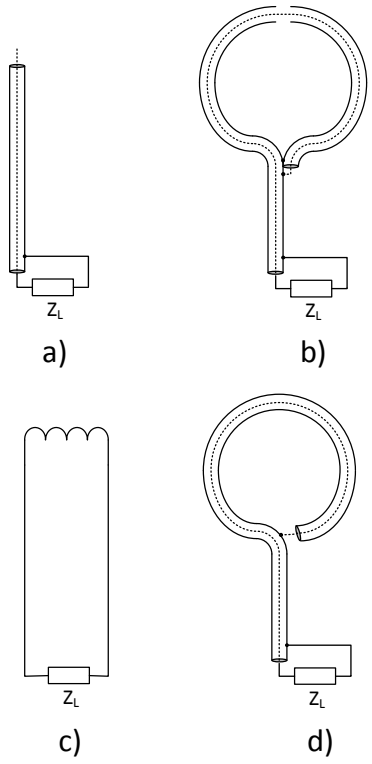

Figure 2. Sensor interfacing module block diagram

$$EMIRR[dB] = 20 \cdot \lg\left(\frac{V_{RF\_p}}{\Delta V_{OS}}\right) + 20 \cdot \lg\left(\frac{V_{RF\_p}}{100mV_p}\right), \quad (1)$$

where V_{RF_p} is the peak value of the RF voltage, ΔV_{OS} is the DC offset voltage shift, that takes place in response to the applied RF. The second term from the equation, references the EMIRR to an input signal of 100 mV_p. [7] The quadratic relationship between V_{RF_p} and ΔV_{OS} is can be seen in equation 2, after equation 1 is solved for ΔV_{OS}:

$$\Delta V_{OS} = \left(\frac{V_{RF\_p}}{100mV_p}\right) \cdot 10^{-\left(\frac{EMIRR[dB]}{20}\right)}. \quad (2)$$

C. *Coupling to the Controller*

After an interrupt the microcontroller can measure the voltages on the peak detectors, through an analog multiplexer, one by one, and log the values [8]. It is an important parameter of the peak detectors, that how long should they hold the last peak value. It must be at least as long to take, as the minimal time from the moment the microcontroller gets the interrupt, until finishing the peak detectors voltage measurements and logging the values. [9] After measurement, the microcontroller can decide to archive or not the system data to the galvanically isolated and shielded backup data storage, or to flag it or not as a questionable credible data. The analog multiplexer saves pins from the microcontroller, extra pins only need for select the required measurable sensor. It is also can be decreased, if the controller uses a bus to adjust the multiplexer. [10] The sensing system architecture can be seen in Fig. 3.

III. REALIZATION OF THE BACKUP DATA STORAGE

In the case of security systems, it is important to defend against deliberate manipulation, or some improper operation by the user [11]. If this occurrence is inevitable, it need to be ensure, the archiving of the system data for an inaccessible data storage. It is also need to endure the isolated mains electricity supply for this module [12].

The local data storage of the embedded system also can suffer data loss because of external electromagnetic interference. The backup data storage need to be shielded from these impacts, it should be cover with metal, to realize a faraday cage. Against conducted disturbances, the data transfer lines of the backup storage also need to be galvanically isolated. If there are no metallic wire connection between the main embedded system and the backup data storage, the power supply must be ensure for the backup storage, with a local – also shielded – battery and power supply [13].

A. *Isolated Backup Data Storage*

Galvanic isolation is feasible with optically coupled channels. It can be realized by infrared communication, optocouplers or optical fibers. IR technology is more cost effective and immune against interference, instead of Bluetooth, LoRa or Wi-Fi to transport information over the air. IR light is one of the shortest wavelength of the electromagnetic scale, it can ensure enough bandwidth for any communication protocol – used by the data storages. The application uses LEDs to send, and phototransistors to receive IR data – covered from external light. These parts are cheap and simple to use even multiple channels. With a dedicated IR receiver for a predetermined frequency the transmission bandwidth can be higher, than with an IR transistor of IR diode.

B. *Hardware Architecture*

It is possible, to add an optional alarm sending module

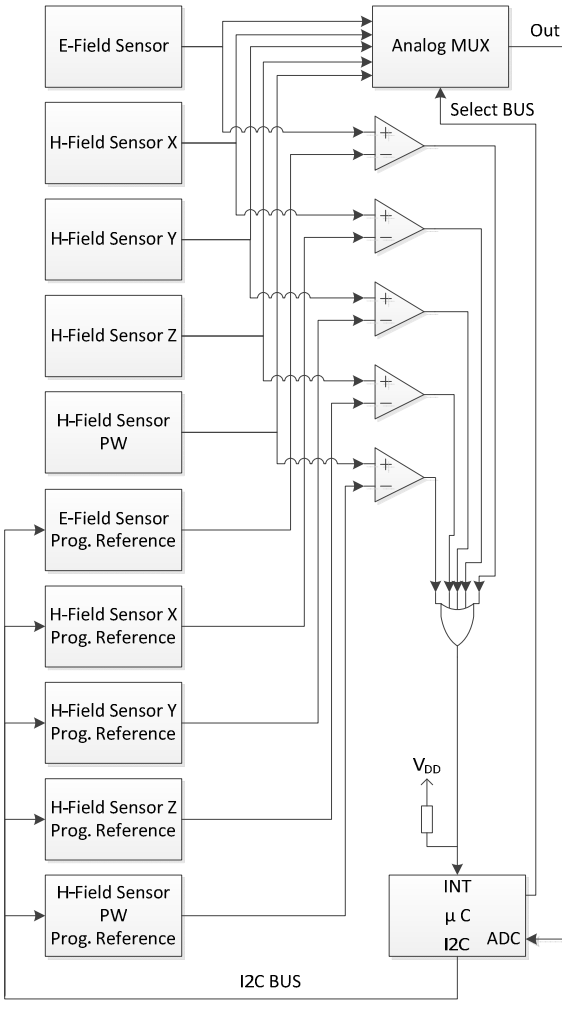

Figure 3. The block diagram of the sensing system

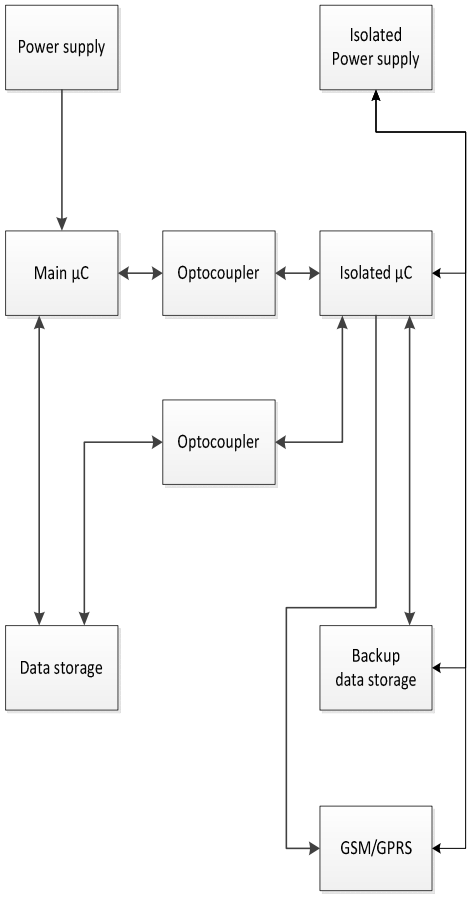

Figure 4. Block diagram of the system architecture

to the system, it should been controlled by the embedded system, which is embedded beyond the main embedded system. The data archiving and EMF sensing microcontroller can send directly a notification or an alert for the central supervisor system, if it is measuring or experiencing an out of place or abnormal operation. The architecture of the system is shown on Fig. 4.

IV. SOFTWARE REALIZATION

A. The Independent Supervisor

The data backup supervisor embedded system may work independently from the main embedded system [14]. The only connection is need because, it need to decide when which microcontroller can use the common data storage. The data backup supervisor microcontroller most of the time is in sleep mode, to save battery life time. It can be wake up for some external interrupt, or some internal timer interrupt. After the communication, or logging, or archiving, it goes back to sleep mode [15].

The flowchart of the data backup supervisor embedded system main software is shown on Fig. 5., and the flowchart of the data archiving method is shown on Fig. 6.

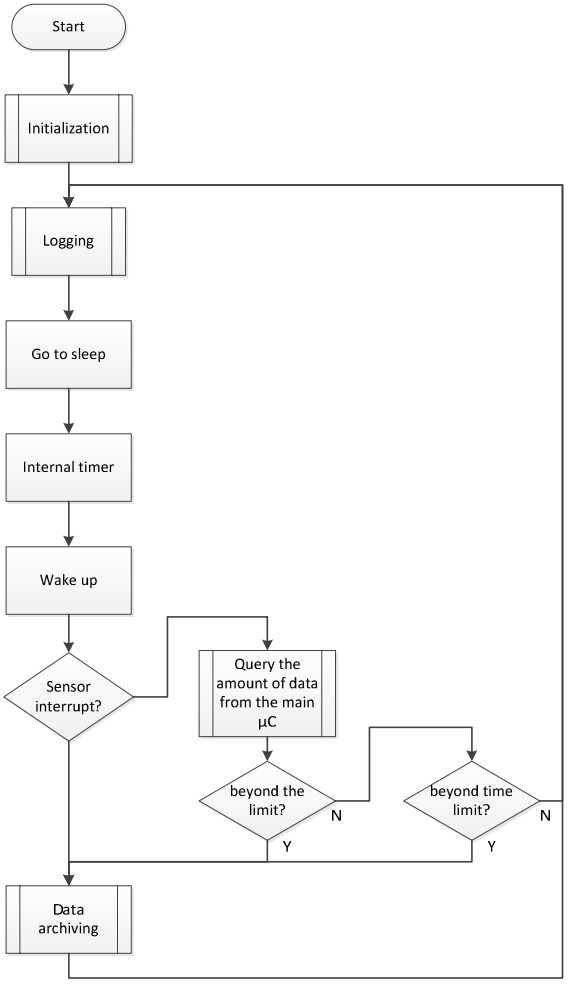

Figure 5. Flowchart of the main loop of the supplementary microcontroller

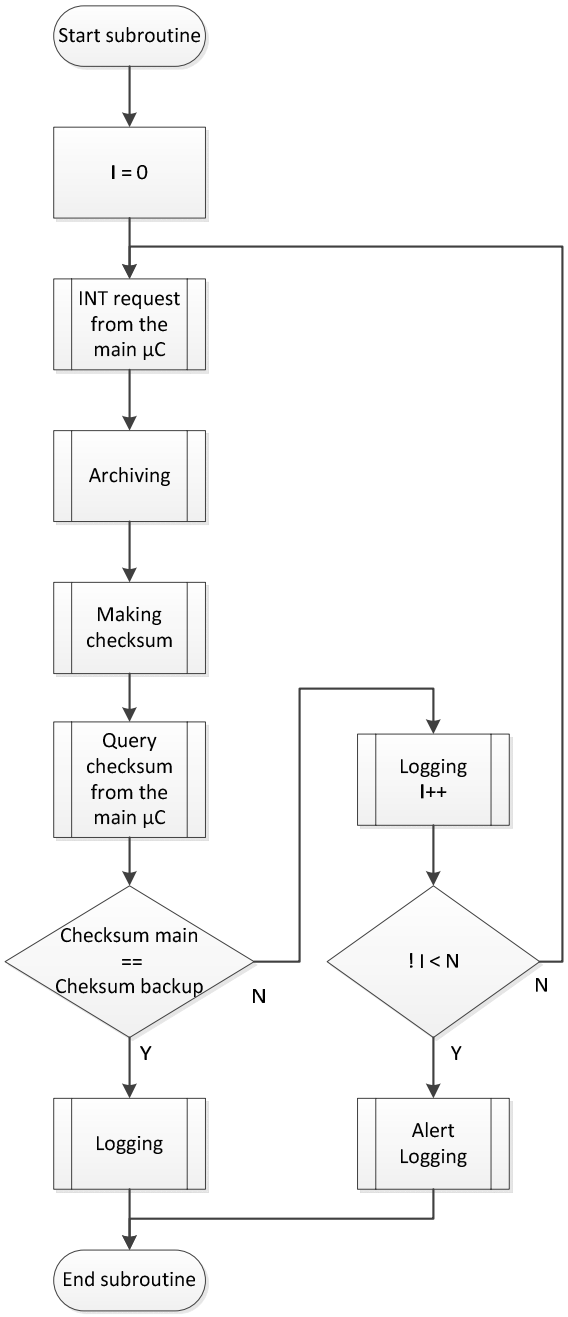

Figure 6. Flowchart of the data archiving subroutine

CONCLUSION

With this method it is easy to tell that the data – measured by the embedded system, which have a backup data storage – is trustable, or there is a possibility that it is contains errors caused by some external electromagnetic interference. It is also can be tell that which part of the data can contains failures, depending the archiving frequency. This solution needs some extra hardware and software redundancy, but it is still feasible at low cost. We believe, that this method can be useful for some civil and industrial applications, where reliability is highly required.

REFERENCES

[1] Gy. Györök. A-class amplifier with FPAA as a predictive supply voltage control. Proc. 9th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics (CINTI2008), pages 361–368, November 2008.

[2] T. Orosz. Analysis of sap development tools and methods. 15th IEEE International Conference on Intelligent Engineering Systems (INES), pages pp. 439–443, 2011.

[3] György Györök, Bertalan Beszédes. Fault-tolerant Software Solutions in Microcontroller Based Systems. In: Orosz Gábor Tamás. AIS 2017 - 12th International Symposium on Applied Informatics and Related Areas: Proceedings. Székesfehérvár, Magyarország, 2017.11.09. Székesfehérvár: Óbudai Egyetem. 2017. pp. 7-12. ISBN:978-963-449-032-6

[4] H. Whiteside, R. W. P. King."The loop antenna as a probe". IEEE Trans. On Antennas and Propagation, Vol. AP12, May 1964, pp. 291-297.

[5] Györök György, Bertalan Beszedes. Fault tolerant power supply systems. In: Orosz Gábor Tamás, 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország, 2016.11.17. Budapest: Óbudai Egyetem, 2016. pp. 68-73.

[6] G. S. Smith. "Loop antennas". R. C. Johnson & H. Jasik (Editors). Antenna Engineering Handbook, Chapter 5. McGraw-Hill, NY, 2nd Ed, 1984. ISBN 0-07-032291-0.

[7] Chris Hall, Thomas Kuehl. EMI Rejection Ratio of Operational Amplifiers. SBOA128A. 2011.

[8] Alexander Baklanov, Svetlana Grigoryeva, György Györök. Control of LED Lighting Equipment with Robustness Elements. Acta Polytechnica Hungarica 15:(3) pp. 105-119. (2016)

[9] Györök György. Számítógép perifériák. óbudai Egyetem, OE AREK 8003 ISBN 978 615 5018 57 2, Budapest, 2013.

[10] Györök György. Programozható analóg áramkörök mikrovezérlő környezetben. Óbudai Egyetem, ISBN 978 615 5018 97 8, Budapest, 2013.

[11] Berek Lajos, Berek Tamás, Berek László. Személy- és vagyonbiztonság: ÓE-BGK 3071. Budapest: Óbudai Egyetem, 2016. 173 p. ISBN:978-615-5460-94-4

[12] Vass Attila, Berek Lajos. Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei. HADMÉRNÖK 24:(2) pp. 41-57. (2015)

[13] Györök György, Tihomir Trifonov, Alexander E. Baklanov, Bertalan Beszédes, Svetlana V. Grigoryeva, Aizhan Zhaparova. A Special Robust Solution for Battery Based Power Supply. In: Orosz Gábor Tamás. 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország, 2016.11.17. Budapest: Óbudai Egyetem, 2016. pp. 32-35.

[14] Györök György, Beszédes Bertalan. Duplicated Control Unit Based Embedded Fault-masking Systems. In: Szakál Anikó. IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017. Szabadka, Szerbia, 2017.09.14-2017.09.16. New York: IEEE, 2017. pp. 283-288. ISBN:978-1-5386-3855-2

[15] Dr. Györök György. Mikrokontrollerek hardver-hatékony alkalmazása. In: Nagy Rezső, Hajnal Éva. Garai Géza Szabadegyetem II. Székesfehérvár: Óbudai Egyetem, 2015. pp. 5-15. ISBN:978-615-5460-62-3