Real time human body temperature monitor in context of medical data protection

Wojciech Wodo[1], Lucjan Hanzlik[1] and Konrad Zawada[2]
[1]*Wroclaw Univeristy of Technology, Faculty of Fundamental Problems of Technology, Wrolcaw, Poland*
[2]*Faculty of Electronics, Wroclaw University of Technology, Wrolcaw, Poland*
{*f_author, s_author*}*@pwr.edu.pl*

Keywords: measurement, sensor, temperature, wireless, medical data protection, privacy

Abstract: In our paper we present newly developed electronic unit for human body temperature monitoring. The main goals of research were designing as small as possible device with functionality of precise temperature measurement for human body, implementing secure wireless communication between device and workstation (e.g. personal computer or smartphone) and reducing power consumption. Thanks to its tiny physical size, device is really mobile and could be easily equipped by patient (e.g. in a watch-like style on a wrist). Electronic circuit is designed in such a way that it is mostly in stand-by mode and wake up only if it is necessary, thanks to that it could work over 40 days without charging the battery (only of 120mA capacity). The crucial part of the project was providing protection for medical data, which is transferred between device and end-point station. We use blue-tooth technology to establish the connection and develop our communication protocol, which assures secure data transfer.

1 INTRODUCTION

According to the golden rule - it is better to prevent than cure, we decided to investigate the subject of human body factors monitoring devices. There are professional and complex devices in clinics and hospitals, which are multifunctional and thus very expensive. We do not often need all of these features, but only one of them may be useful in our case. Our motivation was to facilitate the process of preventing and eventually curing diseases, especially when time interval in reaction is essential. We would like to help medical personnel or even parents to identify that something is wrong. That is the way we consider developing cheap mobile sensors with wireless communication and secure transmission channel. We focused in this paper on temperature monitoring as a factor of heat or hypothermia. Our main goal is to investigate few fields like power supply, mobility (casing and fastening), accuracy of measurement, bluetooth communication, protection of biomedical data and make results applicable in case of other sensors.

1.1 Paper structure and our contribution

The paper is structured in the following way, in Section 2 we describe our deep analysis of unit desired functionalities. We show our conceptions on casing and fastening unit as well as power supply. We present our idea of data transmission and comparison of few temperature measuring methods. Section 3 describes final results of our research, there are the scheme of electronic measuring unit and constructed prototype. We show there particular modules of unit and give a description of their functionalities. There is a part related to the microprocessor algorithms and designed transmission protocol. At the end of that section we present an example of end-point client implementation. In Section 4 we discuss problem of medical data security and show how we meet needs for protection it. Conclusion 5 includes remarks on possible applications of our system and defines challenges for future works.

Our main contributions to this paper are following:

- minimizing physical size of complex microprocessor temperature measuring unit equipped with wireless communication (bluetooth)
- radical reducing power consumption by the unit, giving a possibility of a real mobility (up to 40 days without necessity of charging battery)
- providing medical data security in hardware-based device by design

2 THEORETHICAL PART

In this section we present analysis of unit functionalities and user model as well as assumed work conditions. Some recommendations related to used materials and solutions are posted.

2.1 Analysis of functionalities

The subject of this research is monitoring system for temperature of human body, especially infants. Such a system should be able to transmit data via wireless channel and alarm in emergency cases. Due to special working conditions - infants, a set of factors should be taken into consideration while designing the solution.

Case of measuring device should be made of material which is non-allergic and elastic in order not to injure or bruise skin. Simultaneously case must be resistant to bites or impacts. Fastening of device should ensure close contact with human body without causing too much pressure on arteries or veins. If possible, the device should be embedded in a compact form so that it is not possible to disconnect some fragments of the housing that could be swallowed by an infant.

Measuring temperature should be processed in such a way, that it is possible in any moment to take a sample. It means, sensor should be in constant contact with the body of infant. Such an approach excludes measurement performed with term vision camera or laser thermometer.

Communication between measuring unit and end-point station (*e.g. smartphone or laptop*) should be performed in a way that generating electromagnetic waves is limited as much as it is possible. Additionally, it should be cost-effective in terms of energy consumption. Thus, device should work in stand-by mode for most of the time until critical moment, when the communication is necessary - alarm case. In case of low energy level, unit should inform user.

Critical situation means a rise of body temperature by defined gradient in time or exceeding defined threshold value - threat of health and life. It is similar in case of decreasing body temperature.

Due to the sampling frequency and changing outside conditions, measuring algorithms should be resistant to incorrect data and temporary hesitation of measured value.

During measurements one should consider that infant moves, changes environment of measurement (hides sensor beneath clothes or quilt), bumps device with other items or tries to remove measuring unit.

2.2 Conceptions of casing and fastening

In consultations with physiotherapists and doctors we worked out two types of casing and fastening for the measuring unit.

First solution is based on watch-like case, made of elastic synthetic material, equipped with Velcro strip. One can properly align unit to the arm of infant without causing too much pressure. Measuring unit is placed inside the case and is in contact with the skin via metal or ceramic plate, which is isolated from the housing. Fastening on the infant arm causes necessity of using correction coefficient, because it is not stable point for temperature reference.

Second solution uses silicone electrode, on which measuring unit is placed in a form of thickening covered with elastic synthetic material. Bottom of the electrode is covered with easy cleaning silicone, which sticks to the skin when contacting with it, providing good adhesion. Additionally one can attach the electrode with hypoallergenic plaster that prevents infant from removing the sensor.

Functional requirement for the casing is microswitch allowing to turn on/off or reset the unit. It should be placed inside the case accessible only from outside when using pencil or thin stick via hole in the case. Signaling of turning on/off should take one and two beeps respectively.

2.3 Power supply

Depending on the energy demand for the device we consider two conceptions of power supply: lithium battery 3V (*e.g. CR2016 capacity of 80mAh, exchanged like in watches*) or lithium-ion accumulator (charged via micro-USB). We consider following solutions available on the market:

- LIR2450, 3.6V, 120mAh, Li-ion, Φ 24.5x5.0mm, weight: 5.2g, prize: 5 USD, (our choice)
- ACCU-E45/2.4V-600, 2.4V 0.6Ah, NI-MH, 35 x 33 x 6.2mm (large), weight: 0.02kg
- ACCU-VL2020-1VC, 3V 0,02Ah, Li, Φ 20 x 2.7mm (small), weight: 3.11g
- Panasonic VL-3032/VCN, 3V, 0.1Ah Li, Φ 30 x 3.9mm (small), weight: 15g (barely accessible)

2.4 Data transmission

We designed two models for data transmission between measuring unit and end-point device.

In the first conception measuring unit is equipped with blue-tooth module (*e.g. BTM112 of 10m range*),

which communicates directly with blue-tooth modules embedded in smartphones or laptops. In that case blue-tooth in end-point device must be turned on all the time and in measuring unit it works in stand-by mode. We considered following modules:

- BTM-331 is not equipped with *Serial Port Profile - SPP (SIG, 2012b)* (requires much work on emulating SPP (COM port), includes only *Host Controller Interface - HCI (SIG, 2012a)*, very low power consumption - 34mA
- BTM-162 is equipped with SPP, power consumption at the level of 40mA, (includes HCI as well)

Second solution assumes existing middle station, which is connected to electricity and transmits/receives data based on own protocol on frequency of 2,4 GHz and passes them via USB or bluetooth. Such a solution allows saving energy on the measuring unit side thanks to waking it up only if it is necessary. We consider using radio module RFM73, which consumes about 22mA energy.

2.5 Temperature measurement

Valid measurement of temperature is fundamental functionality of the unit. Due to special work conditions - human body, it requires precision of 0.1°C. In order to gain accurate measurement we use sequence of samples separated one each other by time interval. Values of samples are analyzed (removing outliers), and the rest of measurements are averaged. We assume such a measurement is correct, but additionally it is compared with previous measurements in order to calculate change gradient and check reality of it. We define that one complete measurement of temperature should be performed no more than once per minute, and no less than once per three minutes, what corresponds to human body.

We consider using following sensors available on market:

- TSYS01 (from 0 do 50°C, precision +/-0.1°C), factory calibrated, 24bit
- LM92 (+/- 0.33°C) (in our range +/-0.5°C), too low precision
- LM35CAH (+/-0.5°C), analog sensor, requires 12bit converter, too low precision
- PT-100 (necessity of A/C converter designing), too much complex solution

3 EXPERIMENTAL PART

In this section we present solutions for stated problem in a form of electronic measuring unit and designed software. A prototype implementation of the measuring device with the monitoring application has also been prepared.

3.1 Measuring unit

3.1.1 Used components

- Bluetooth module - BTM-162 (with SPP), power consumption about 40mA,
- Temperature sensor - TYS01 (range: from 0 to 50°C, precision +/-0.1°C), factory calibrated, 24bit,
- Microprocessor - ATXMEGA32E5, low power consumption including enabled RTC - about 0.7uA,
- Battery - LIR2450, 3.6V, 120mAh, Li-ion, Φ24.5x5.0mm, weight: 5.2g,
- Charging unit - MCP73831, appropriate charging current - from 50mA, signaling of charging,
- Converter 3.3V - LT1615 *Single-Ended Primary-Inductor Converter - SEPIC*, power consumption about 20uA, efficiency 75-80%, small size,
- Acoustic signaling - beeper Φ27mm
- Visual signaling - two double LEDs

3.1.2 Modules functions

Bluetooth module - performs communication between computer (or other host) and measuring unit via SPP profile. Module communicates with microprocessor via serial *Universal Asynchronous Receiver and Transmitter - UART* interface with a speed of 19200 bods/sec, 1 bit stop and 8 bits of data.

Temperature sensor - measures temperature with a resolution of 24 bits and precision of 0.1°C. The result of measurement is calculated according to the polynomial from documentation and individual calibration data stored by manufacturer in memory of unit. Communication with temperature sensor is performing via *Inter-Integrated Circuit - I2C (Academy, 2014)* interface.

Charging unit - responsible for charging the li-ion battery 3.7V with current about 68mA. In order to charge the unit, one should connect charger (5V 100mA) via micro-USB port.

Battery - one cell rechargeable li-ion 3.7 V with a capacity of 120 mAh. Estimated operating time is around 40 days.

Converter 3.3V - works in SEPIC mode and stabilizes voltage of li-ion battery at the level of 3.3V, needed for other elements of unit. It is

a high-efficiency converter with low power self-consumption.

Microprocessor - the main unit managing the device. Microcontroller is responsible for processing temperature measurement by appropriate algorithms, checking thresholds and gradients defined by user with current measured temperature. Additionally microprocessor checks the battery voltage determining the state of charge and supports real time clock regardless of a measuring unit. Configuration of device is performed via BT module.

3.1.3 Prototype and minimizing the unit

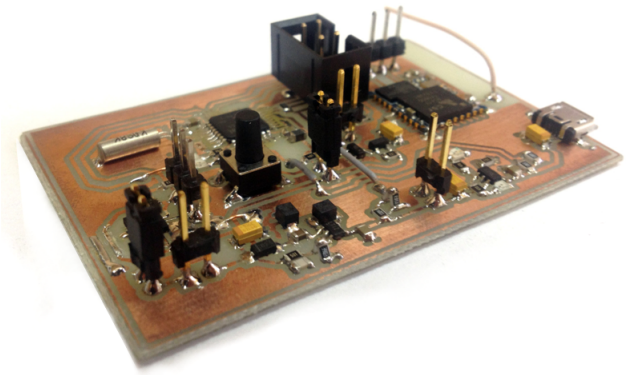

Figure 1: Prototype of the device (100mm x 70mm)

Prototype was realized in *Surface Mount Technology - SMT*, to facilitate the measurements gold pins and 10-pins socket (for programing and additional power supply) were embedded - see Fig. 1.

After many tests we redesigned the whole unit in order to minimize it to the size of 34mm x 34mm - see Fig. 2. Thanks to that it suits to the 3D printed watch-like case.

Figure 2: Minimized device (34mm x 34mm)

3.2 Microprocessor software

3.2.1 Algorithms

As part of the developed software for microprocessor we designed algorithms for communication between Bluetooth module and microprocessor, communication between temperature sensor and microprocessor, logic for calculating appropriate temperature values and analyzing archival measurement data. We created data structure for storing measurements and communication frames - alarm, configuration and informational. Thanks to the measurement of the battery voltage, processor via analog-to-digital converter controls the condition of its discharge and informs user in the appropriate moment about the necessity to connect the power supply. We developed also built-in-test - some sort of self-controlling mechanism, if microprocessor hangs, unit will reset. In that case we use solution similar to watchdog. It is similar in case when one of the modules stops responding correctly, then device signalizes the error.

We designed two work modes: regular and configuration. In the first mode, unit acts like an independent device, BT module is in stand-by mode and only in critical case wakes up to send the alarm message. After that it turns again into stand-by mode. In the latter mode device turns into slave mode, turns BT module on and waits for connection with end-point device (*e.g. computer or smartphone - master*). Then it is possible to send/receive configuration data. In order to trigger configuration mode one should keep pressed switch for 4 seconds.

Temperature measurement is based on conception of multi sampling and removing outliers. Using the documentation of sensor TYS01, of which every single piece is factory calibrated, we calculate correction coefficient and final value of the measurement. Additionally it is possible to add correction coefficient manually, using software. It could be useful in case of different fastening places on the human body.

3.2.2 Example of application

In order to test our device we developed client application on personal computer. Software was implemented in Java using class Swing for GUI. First step in connecting application and measuring unit is pairing BT modules. It is possible in configuration mode, PIN is generated from serial number of unit (unique for each device). Since then, virtual port COM is available in a computer. To establish the connection between application and this serial port we use project java-simple-serial-connector (on GNU Lesser

GPL (Foundation, 2007)) allowing easy access to serial ports from Java. Software detects appropriate port automatically and starts monitoring the unit, in case of exceeding defined thresholds or rapid temperature growth, unit sends warning message and application alarms, see Fig. 3. It is also possible to watch history of measurements on a chart.

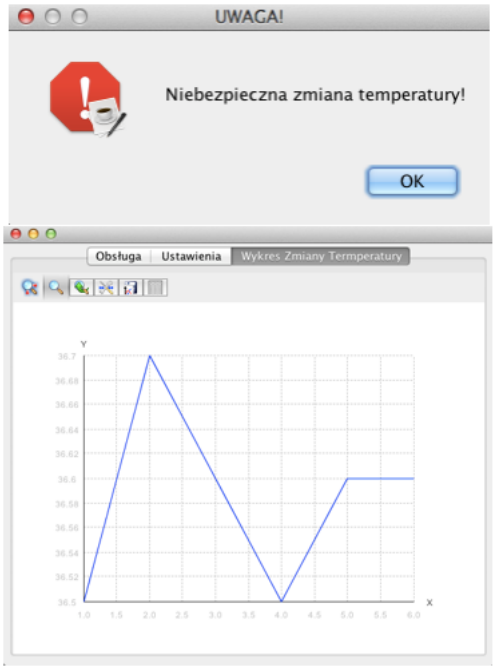

Figure 3: Example application - alarm message and history of measurements chart

4 MEDICAL DATA PROTECTION

All medical information protection is guaranteed by law. For this purpose, the device is equipped with a number of safeguards against unauthorized access.

4.0.3 Data transmission

Transmitted data is organized in frames with headers including information about content and length. An example frame - setting clock is presented in Table 1.

0x01	0x00	0x00	0x00	0x3c

Table 1: Example frame of setting the clock

Next, for each frame control sum CRC16 is calculated and attached to the frame. Sum is calculated by using divisor 0x1021 and starting value CRC 0xffff.

0x01	0x00	0x00	0x00	0x3c	$0xXX^1$	$0xXX^2$

Table 2: Previous frame with added CRC. (1) High byte CRC, (2) low byte CRC.

Before frame is sent special bytes must be added, at the beginning and at the end of the frame as well as an escaping byte - in case when one of the data frame bytes was special char. Such an approach guarantees receiver easy and quick possibility of splitting incoming data in separate frames and detect errors. These method is commonly used in serial data transmission.

0x12	0x01	0x00	0x00	0x00	0x3c	0xXX
0xXX	0x13					

Table 3: Data frame with added special chars.

Frame from Table 3 is ready to send, but data included is in plain text, thus the final stage is encryption by AES algorithm with secret key and send data. Receiver works analogically to the sender, decrypts data and checks CRC, in case of inconsistency in CRC, current frame is dropped.

4.0.4 Data encryption

Security mechanisms are based on four-digits PIN and on a secret key for encryption of transmission. Thanks to the bluetooth pairing protocol and the PIN, we prevent the pairing of our device with unauthorized units. After the connection is established, data is encrypted with *Advance Encryption Scheme - AES (Daemen et al., 1998)* using a secret key *sk*. In order to assure semantic security we implemented the *Counter Mode of operation - CTR (Dworkin et al., 2001)*. This way an adversary cannot recognize if the same frame was send twice (which would mean the same temperature). At start both devices share a common initial vector, which is incremented each new frame is send. Note that if a frame is lost, then this would imply that the decryption would fail on the side of the unit (counters would desynchronize). Thus, we also use the CTR mode to assure coherence of the data send through the secure channel.

We also consider the threat of *Replay attacks (Adams, 2011)* and that is why we decided to embed timestamp for each message:

$$m = "data\ frame||timestamp"$$

Thanks to the *Real Time Clock - RTC*, the microprocessor can easily generate this value and concatenate it to the data frame. The end-point device decrypts the ciphertext and splits the data into frame and timestamp. Next, the received timestamp is checked with

previous ones. In case of equality of timestamps, there is a suspicion of replay attack and the frame is dropped with an entry to the log.

PIN and secret key *sk* are generated for each device independently and are correlated with the serial number. The user is able to change the secret key only knowing the old one. The PIN is permanently assigned to the unit. In case of losing the secret key, there is a possibility of resetting the unit to defaults settings. Although, this erases all data in the units memory.

5 CONCLUSIONS

During the research we tried to develop some sort of standard for human factors measurement sensors. Thanks to that approach, our solution is applicable for other sensors and systems - by assigning individual identifiers to each unit it is possible to build network of sensors and have preview of all results in one place. Such networks could be implemented in clinics or hospitals.

Thanks to significant effort put in minimizing unit power consumption, it is suitable for critical work conditions - like military field hospitals, where possibility of connection to electricity is very limited.

It is possible to exchange the sensor to the other one and rest of the system remains the same, it is achieved by developed universal power supply section and communication protocol.

ACKNOWLEDGEMENTS

This project was partially supported by European Union as part of the European Social Fund 8.2.1 - Low Silesian Bon for Innovation.

REFERENCES

Academy, E. S. (2014). I2c (inter-integrated circuit) bus technical overview and frequently asked questions. www.esacademy.com/en/library/technical-articles-and-documents/miscellaneous/i2c-bus.html.

Adams, C. (2011). Replay attack. In van Tilborg, H. C. A. and Jajodia, S., editors, *Encyclopedia of Cryptography and Security (2nd Ed.)*, page 1042. Springer.

Daemen, J., Daemen, J., Daemen, J., Rijmen, V., and Rijmen, V. (1998). Aes proposal: Rijndael.

Dworkin, M., Dworkin, M., Gallagher, P. D., and f, D. N. S. P. (2001). Recommendation for block cipher modes of operation: Methods and techniques.

Foundation, F. S. (2007). Gnu lesser general public license. https://www.gnu.org/licenses/lgpl.html.

SIG, B. (2012a). Host controller interface (hci) architecture. https://developer.bluetooth.org/TechnologyOverview/Pages/HCI.aspx.

SIG, B. (2012b). Serial port profile (spp). https://developer.bluetooth.org/TechnologyOverview/Pages/SPP.aspx.