On the Design of Distributed Autonomous Embedded Systems for Biomedical Applications

José Germano[1], Rui Ramalho, Leonel Sousa
INESC-ID / IST, TU Lisbon
R. Alves Redol 9, 1000-029, Lisboa, Portugal
Email: jahg@inesc-id.pt[1]

***Abstract*— Embedded systems assume an increasing importance in several biomedical applications. These applications present dissimilar requirements and characteristics, posing problems at the computing and communication levels. This paper proposes a general network based platform that follows a distributed approach based on a client/server architecture, in order to integrate embedded systems for biomedical applications. This platform makes use of autonomous communication modules, and relies on personal digital assistants to act as Masters, and to interconnect the embedded systems to computer networks. Information is sent to a main server that maintains and provides access to a database. Data security is assured in all systems by using cryptographic algorithms and protocols. Two embedded systems have been developed based on this platform, a simple system for movement monitoring, and another for biomolecular recognition detection. Furthermore, we show that the optimization of the communication module lead to an increase of 70% of the platform's autonomy for the movement monitoring system.**

I. Introduction

In the last few years there has been a growing interest on embedded systems for biomedical applications, increasing the demand on computing and communication, but, at the same time, reinforcing the necessity to keep them portable and autonomous. Applications such as biochemical operations for clinical analysis (e.g, glucose/lactate analysis), DNA analysis and proteomics analysis for clinical diagnostics [1], and real-time pervasive patient monitoring and biomedical digital assistants [2]–[4] are typical examples where portability and computing power are important requirements. However, namely in the latter case, computing and communication requirements lead to the integration of wireless devices on the embedded systems in order to communicate with general purpose computing systems. Therefore, the actual embedded systems for biomedical applications have to be designed with low power communication sub-systems and, on the other hand, have to be easily integrated with more general distributed computing platforms. Reliability and security issues have to be considered on those platforms, both at computation and communication levels [5].

Distributed embedded systems for biological and biomedical applications is one of the most multidisciplinary research areas, which covers fields from micromechanics and microsystems [6], signal acquisition and digital signal processing [7], embedded systems, computer networks, and information systems and databases [5]. The enormous diversity of sensors and medical apparatus demands the development of general computation/communication architectures that can be applied for deploying distributed embedded systems that may cover a wide range of applications and environments. A general platform has to be defined to setup and integrate these embedded systems in general computer networks, which in turn allows the storage and retrieval of the information generated by these remote embedded systems in a distributed way.

This paper proposes a communication architecture for implementing a distributed platform that supports autonomous embedded systems for medical applications. The considered architecture includes both the hardware and software components and allows the development of autonomous but collaborative embedded systems using current technologies.

The paper is organized as follows. In section II it is presented the general architecture of the proposed platform to integrate embedded systems, with both the computing and communicating components. Section III presents the generic architecture of the embedded systems and describes the prototype of the communication module. Two biomedical applications that follow the proposed architecture are presented in IV. Experimental results on the system's autonomy and the developed user interface are presented in section V. Section VI concludes the paper.

II. Proposed Distributed Platform Architecture

As depicted in Fig. 1, a master device can be connected and control a single or multiple portable embedded systems (which contain biosensors) by using wire based or wireless communication protocols. Furthermore, Masters can act themselves as a second communication layer, by directly using the IEEE 802.11 standard for wireless local area networks (LANs) to connect to servers hosted in general purpose computers.

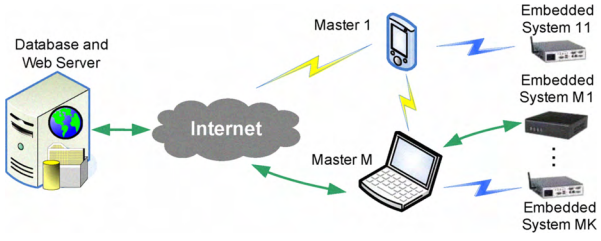


Fig. 1. Block diagram the proposed distributed architecture.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

We propose the usage of the hyper text transfer protocol (HTTP) and WebServices [8] to achieve a distributed environment in which different Masters can be relatively far away and connected by a wide area network (WAN). For security reasons it is advisable to adopt an implementation of the HTTP on the top of secure socket layer (SSL) or transport layer security (TLS) leading to hyper text transfer protocol secure (HTTPS). Using this secure connection, the Master devices can upload or download data from a common database located in a remote server. The servers also implement a web server allowing a secure web based access to the stored information. By implementing different client roles, the access to stored information can be efficiently managed according to the user profile.

Communication between the Masters and the server is accomplished by exchanging simple object access protocol (SOAP) requests and replies via WebServices. WebServices provide a request acceptance and a reply service by using extensible markup language (XML) based files. Figure 2 represents the client-server interactions of a SOAP request, client **A**, and also represents the web access role from a web browser, client **B**.

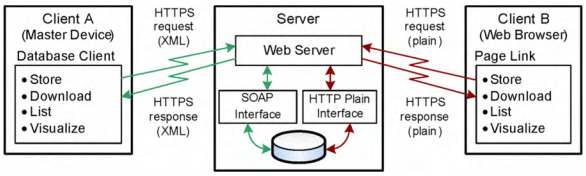


Fig. 2. Client-server data flow.

The usage of SOAP offers some advantages: *i)* the data posting is performed using the HTTPS protocol, which makes the delivery mechanism widely available and does not require additional firewall configuration; *ii)* the usage of the XML allows an easy expansion of the system as well as wide support; and *iii)* since it is based in XML and HTTPS, it exhibits a high interoperability level. SOAP allows the client Master device to wrap a method call in SOAP/XML which is then posted over HTTPS to the server. At the server side, the XML request is parsed to read the method's name and parameters which are passed and delegated to perform a database query. Trough a PHP database interface, the server database supports storage, retrieval and list operations. The XML response is then sent back to the client, containing the return value (or fault data) of the method call. Finally, the client may parse the response XML to make use of the return value. As depicted in Fig. 2, the remote server also supports access to the database through a web browser using HTTPS plain interface. This standard interface enhances information availability and management.

III. Embedded System Architecture and Communication Module Prototype

A common autonomous communication module (ACoM) is proposed to interface any sensing and processing device. These ACoMs are connected to the sensing and processing systems through serial standard interfaces and communicate with Masters, which can be personal digital assistants (PDAs) or laptops, through standard wire or wireless communication systems. Data security is assured by the ACoM by encrypting the acquired data, based on public-key or symmetric cryptosystems.

A. Embedded system architecture

Figure 3 presents the block diagram of the embedded system architecture. The design comprises two fundamental modules: *i)* the autonomous communication module (ACoM); and *ii)* the sensing and processing module (SPM). These two modules

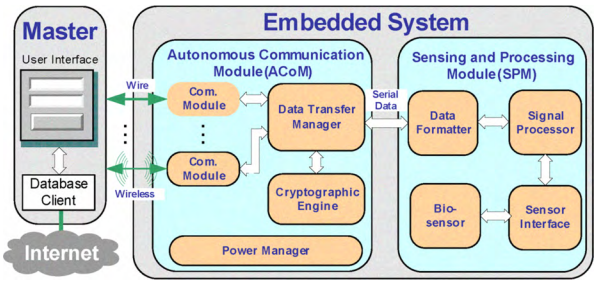


Fig. 3. Architecture of the embedded system.

compose an embedded system able to communicate with more general computing devices, such as laptops or PDAs.

In the core of the ACoM there is a data transfer manager and a set of standard communication interfaces. The transfer manager is responsible for communicating data and commands from and to a local SPM, and also to interface the ACoM with the Master (see Fig. 3). Two additional important blocks are present in the ACoM: the power manager and the cryptographic engine. The power manager is responsible for monitoring the state of the system battery and controlling its recharge. Data security is assured by the ACoM by encrypting the acquired data. Public-key or symmetric cryptosystems can be applied, and the SSL can be adopted at the Master's level.

The SPM architecture is generic, the only strict requirement is that it communicates with the ACoM using a standard serial protocol in order to ease compatibility between the embedded system modules. A required block of this subsystem is a data formatter that serializes the data to transmit. The SPM usually includes a sensor interface block to perform the conditioning of the acquired signals and digital processor.

The Master device has full control over the embedded system. It must provide a user interface that allows the execution of complex preprogrammed tasks at the SPM. Although the interface is customized to fulfil the requirements of the different types of SPMs, a set of common tasks can be identified, namely the ability to: display the received data in real-time, store and retrieve data from a remote database or from a local repository, encrypt and decrypt the transferred data, communicate data and commands to the ACoM by using a serial communication channel.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

B. Communication module prototype

The described architecture of the ACoM was implemented on a conventional two layer board printed circuit board (PCB) with room for the Bluetooth module. The achieved board, depicted in Fig. 4, has a square shape with an area of about 32 cm^2, which is smaller than a credit card.

Fig. 4. Communication module: *1)* microcontroller; *2)* power supply citcuits; *3)* Bluetooth adapter; *4)* USB interface; and *5)* Li-on battery.

At the core of the module, Fig. 4(1), there is an off-the-shelf 16-bit microcontroller (MC), PIC24FJ64GA004, that integrates several communication peripherals and can perform a maximum of 16 MIPS. This MC provides advanced power-saving features that are crucial for an embedded battery powered system. At its maximum clock speed the core power consumption is 50 mW, while in the idle and sleep modes the required power drops to 12 mW and 30 μW, respectively. This device provides universal asynchronous receiver transmitter (UART), serial peripheral interface (SPI) and inter-integrated circuit (I^2C) serial data interfaces. Taking advantage on the peripheral pin select functionality provided by the MC, the same I/O pins can be used for all the communication modules. The MC manages all communications with the SPM using one of the available serial data interfaces. It is the SPM that defines which of these interfaces to use.

This MC also controls the power supply generation circuits, Fig. 4(2). In order to achieve a proper battery management, the battery charge current is defined according to the available external power sources, universal serial bus (USB) bus or DC adapter. The presented prototype of the ACoM includes two low noise power rails that can provide a current up to 500 mA each, and can be adjusted from 1.2 V to 5 V. A fixed high efficiency 3.3 V, 800 mA rail is also available to provide power to digital circuits.

Two communication devices are included in the prototype: a Bluetooth adapter, Fig. 4(3), and a USB serial converter, Fig. 4(4). Both modules are controlled using a peripheral UART of the MC. The selected Bluetooth adapter (Bluegiga Tech WT11) requires a board area of 35x14 mm and works from a 3.3 V power rail. The module implements the Bluetooth 2.0 standard with enhanced data rate (EDR), and can operate with data rates up to 3 Mbps. The adapter is Class 1 compliant achieving a maximum communication range of 300 meters. The module's name and the other pairing parameters can be configured by using the module's control interface.

The adopted USB serial converter (FT232RL) is USB 2.0 full speed compatible, and supports data rates up to 1 Mbaud. This converter provides the standard UART signals and also control signals that allow the MC to monitor the USB connection status. These signals are used to adjust the battery charge current and also to determine which will be the active communication module.

The software of the ACoM was mostly written in C, but some of the critical parts were coded in assembly language. The encryption engine is an optional software module that encrypts messages before sending them to the Master. This is one of the components that can be switched off by the power manager, when it is allowed to relax data security. In order to ease the software development for the ACoM a set of communication libraries was created to provide a common interface to access the different communication peripherals.

C. Techniques applied for lowering power consumption

Two of the four blocks depicted in Fig. 4 have significant power consumption: the MC, Fig. 4(1), and the bluetooth module, Fig. 4(3). The power supply circuits (Fig. 4(2)) are already optimized at the hardware level and no software optimizations are available. The USB interface is powered by USB, having no effect on the system autonomy.

The used Bluetooth module provides several options to lower power consumption, namely the use of low power modes. The module provides several operation modes such as: an active mode (default mode while communicating), idle mode (default mode when no connection is active), sniff mode, park mode and a deep sleep mode. Typical values for the consumption are: 560 mW peak in transmission mode (300 m range); 10 mW when in idle mode and 1.2 mW in sleep mode. The Bluetooth adapter control interface is used to select the operation mode and to adjust some connection parameters that have impact on the module's power consumption. When the device is in sniff mode it only listens to the piconet at certain intervals, thus trading bit rate for power consumption. These intervals can be configured by the user at run time, enabling the user to shape this interval according to the data rate required at that particular time. In the park state the device does not participate in the piconet traffic. This mode requires less power than sniff mode, but is less flexible. Another technique for lowering power consumption is lowering the device's power class. Even though the used module is a class 1 device with a range of up to 300 m, it allows the user to change its class to a less power demanding one. In this prototype the bluetooth module was used as a class 2 device, which should be enough to achieve a 10 m range, deemed suitable for a large number of applications.

At the MC level, some techniques can also be applied for lowering power consumption, namely clock throttling, idle mode and sleep mode. Lowering clock speeds is a well known method of lowering power consumption, however, lowering a processor clock speed does not necessarily increase a portable

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

device's autonomy, as a lower clock speed makes computations last longer. While the MC is in sleep mode its clock source is shutdown, thus powering down the whole processor and all of its peripherals. Idle mode is somewhat similar to sleep mode, only the clock source is not shutdown, but the clock is prevented from reaching both the CPU and a configurable number of peripherals. Even though the idle mode consumes more power than sleep mode, it has far more flexibility.

D. Security

The encryption module is a software module that encrypts or decrypts data using the advanced encryption standard (AES) algorithm. AES is a suitable symmetric key algorithm to protect sensitive electronic information up to SECRET level, if a 128 bit key is used [9], and TOP SECRET information if 192 bit keys or 256 bit keys are adopted. The prototype in this paper uses a 128 bit implementation of AES. In order to prevent the key from being discovered, the master periodically generates a new key randomly, and uses the still secure connection to send this new key to the cryptographic module of the ACoM. This encryption module was built using Microchip's cryptographic libraries, specifically designed for the microcontrollers of this manufacturer. The implementation of the AES algorithm is coded in assembly requiring a total of 2808 instruction cycles [10].

E. Master device

To allow the user to interact with the ACoM, a graphical user interface (GUI) was developed. This interface gives the user the possibility to configure the experience, watch the experience unfold by examining the incoming data in a real-time graphic and send the received data to a remote database through the internet using SOAP. Furthermore, it is also possible to store the data locally on the PDA. As the ACoM is a generic platform for accessing all manner of biomedical SPMs, its interface must be easily extendable in order to accommodate the specific needs of every SPM. However, most of the underlying functionality remains the same for every application. The entire user interface was written in C#, using the .NET compact framework 2.0 for increased portability. For this implementation a MySQL database was set up on a remote machine, and the PDA communicated with the database through a PHP server (also set up on the remote machine). The connection between the master device and the PHP server was done in SOAP.

IV. Embedded Systems for Biomedical Applications

This section presents a detailed description of two prototypes of embedded systems: *i)* one for biological analysis and recognition; and *ii)* other to monitor movement. Although these subsystems use different communication interfaces, the generic design of the ACoM allows the usage of the same board design for both embedded systems. The only differences can be found on the firmware of the MC.

A. System for biomolecular recognition detection

The architecture described in the section III was applied to develop a microsystem for biomolecular recognition assays based on a magneto resistive (MR) biochip. Biochips are biological sensing devices used in lab-on-chip platforms to obtain higher levels of integration and, nowadays, are often used as disposable cartridges. Recently, MR biochips have been used for integrated biorecognition assays, using target biomolecules marked with magnetic particles (MPs) [1], [11], [12]. The recognition assay consists on a biological reaction that allows the detection of a priori unknown biomolecules (e.g. human DNA strand for genetic disease detection or bacteria/cell detection).

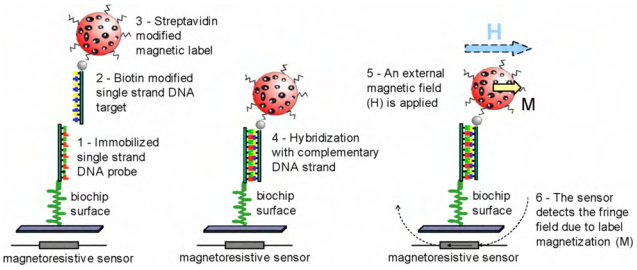


Fig. 5. Detection of complementary single strain DNA.

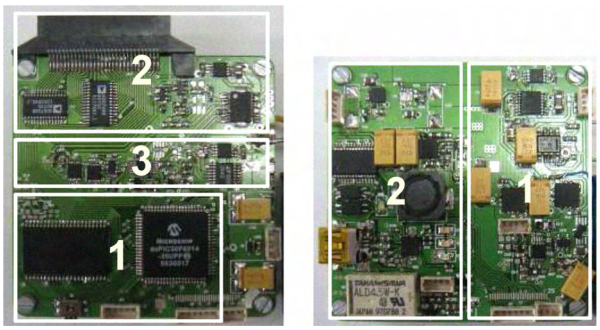
Figure 5 depicts the DNA recognition steps when pre-labeled targets are used [13]. First a DNA strand with a known sequence (probe DNA) is immobilized on the chip surface. The biorecognition assay starts with the introduction of an unknown DNA strand (target DNA) previously labeled with a MP. This target DNA corresponds to the DNA to be analyzed. If the probe and target strands are complementary, a biomolecular reaction (hybridization) occurs binding the two strands. Following, a washing step removes all the target strands which were not recognized. The fringe field created by remaining MPs is then detected by using the MR sensor. The sensor's electrical resistance variation is proportional to the number of biomolecular recognition events.

The main advantage of this type of microsystem is the possibility to directly detect biomolecular recognition (e.g. DNA hybridization) by reading the magnetic field created by the markers using a sensor located below each probe site. The action of taking an electrical measurement, instead of an optical one, offers significative advantages. The complexity is considerably reduced and the system is more compact and less expensive since no laser devices are required [12].

Figure 6 presents the SPM of the microsystem for biological analysis, based on the microarchitecture proposed in [1]. The SPM developed in this work lead to two boards with the same size as the ACoM board (32 cm^2) allowing the boards to be stacked and thereby making the system more compact. Both the SPM boards are powered from the low noise power rails provided by the ACoM.

All electric signals that drive the biochip and that individually address and readout the signals provided by each of the

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966



(a) (b)

Fig. 6. Biological analysis platform; a) main board: *1)* digital signal processor, *2)* addressing and current generation, and *3)* signal acquisition; b) magnetic signal generator: *1)* magnetic drive; and *2)* stand-alone debug interface.

sensors are controlled by a 16-bit microcontroller/digital signal processor (MC/DSP). The selected device, dsPIC30F6014, can perform up to 30 MIPS and includes peripherals that are used to control the on-board electronic components and to communicate with the ACoM, Fig. 6(a)(1). The board also includes a 1 Mbit memory for storing acquired and processed data. This signal processor includes several power saving features like dynamical clock scaling, sleep and idle modes. The operating power of the processor at its maximum clock speed is near 1 W and its idle power consumption is 600 mW. This makes the power management of the MC/DSP critical. The interface with the ACoM is performed using one of the UART peripherals available in the processor. The MC/DSP provides row/column addresses to sensor reading and defines the needed drive current through a digital to analog converter (DAC), Fig. 6(a)(2). The design supports both linear and matrix type biochips with spin-valves (SVs) or magnetic tunnel junctions (MTJs) sensors up to a maximum of 256 elements [13], [14].

To measure sensor resistance variation due to magnetic field variation, an AC excitation is performed using an external magnetic field generated by a coil placed above the biochip. The generation of this magnetic field is digitally controlled. A typical measure with SV sensors requires a 2.38 kA/m DC magnetic field with a 0.8 kA/m AC component superimposed. Since the generation of this magnetic signal is performed using linear amplifiers (Fig. 6(b)(1)) to achieve low harmonic distortion, the power consumption of this circuit is high. A less sensitive alternative reading method only requires a DC magnetic field and an AC drive current making the measure less power consuming. The sensor signals are acquired by using a single instrumentation amplifier and a high resolution analog to digital converter (ADC), Fig. 6(a)(3). The digital signals are processed locally in order to reduce the bandwidth required to transmit the measured data. This process leads to only one or less samples per second per sensor. This allows the ACoM to use a lower bit rate, which further increases the system's autonomy.

B. Movement monitoring system

The SPM for movement monitoring is performed by a 3D accelerometer included in a small electronic module realized with 2 micro machined 2D accelerometers (placed in orthogonal planes) and a MC. The small size (8 cm^2) of this SPM, makes it suitable for movement monitoring.

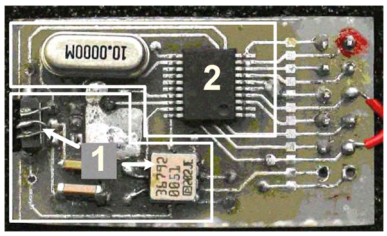


Fig. 7. Movement monitoring prototype: *1)* two 2D accelerometers; and *2)* microcontroller.

Each 2D accelerometer chip (ADXL202) possesses two accelerometers in orthogonal positions, so two chips are required to detect the acceleration along the three axis, Fig. 7(1). The position of both accelerometers is marked in the figure. For the measurements to be correct, the chips must be orthogonal to each other, guarantying that the obtained values are independent. The digital accelerometers can measure accelerations up to $\pm$ 2 G's in each direction. The output of each accelerometer is a duty cycle modulated (DCM) digital signal. The on-board MC reads the data provided by the digital accelerometers and pre-processes it. The selected 8-bit MC, PIC16F84A, (Fig. 7(2)) delivers a performance up to 5 MIPS with a power consumption of 50 mW. The small size and low cost characteristics make this device a good choice for this module. One of the key functions of the MC is to perform the calibration of the sensors. The calibration process reduces the initial measure uncertainty from $\pm$16% to only 2% (noise and calibration errors). The data is transferred to the ACoM using the SPI protocol.

V. Experimental Results

This section provides results on the autonomy of the two considered embedded systems. The graphical user interface and the web interface of the system for biomolecular recognition assays, that is the most complex of the two embedded systems, are also presented.

A. Autonomy of the developed systems

Figure 8 presents the complete prototype of the DNA recognition detection system. In the picture the ACoM and the two SPM boards are identified. The final size of the prototype is 13 cm$\times$15 cm which makes the device portable. Most of the required area is due to the magnetic drive circuits.

The autonomy of the DNA recognition detection system was evaluated in each one of the typical operating modes of the system. The first test, **measure 1**, represents a biological measure using a DC and AC magnetic signal, 1.6 kA/m DC + 0.6 kA/m rms AC, to drive a SV sensor. The sensor

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

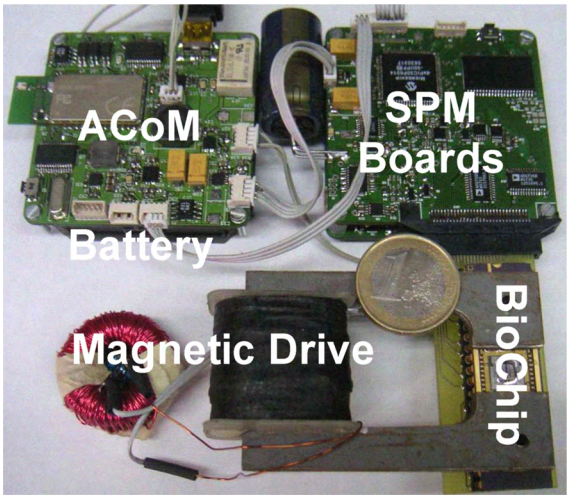


Fig. 8. Prototype of the DNA recognition system.

current was set to 1 mA to obtain a high sensor sensitivity ($(R_{max} - R_{min})/R_{min} \approx 6\%$). This provides a very high measurement sensitivity but also requires more power. In the second test, **measure 2**, the same SV sensor was used. The sensor drive current was set to 1 mA DC with a 20 μA rms component superimposed. In both these tests the data is generated by the SPM at a rate of 1 Hz and the length of each sample is three bytes. The digital signal processor of the SPM was configured to perform 7 MIPS when active. The data is transmitted to the ACoM using an UART peripheral configured to 9600 bps. The ACoM is then responsible for packing the data into 128 bits data blocks, each data block contains five 24 bit sensor samples. Finally, the data is encrypted using the AES algorithm with a 128 bit size key. The ACoM MC is configured to perform 4 MIPS allowing the block to be encrypted in 0.7 ms. The data block is then sent to a PDA using the Bluetooth adapter configured to a data rate of 9600 bps and to the maximum transmission range. This measurement mode provides real-time monitoring of the experience allowing the user to abort the experience if required.

The third test, **idle 1**, is used to evaluate the autonomy of the system in stand-by. In this test no acquisition is being performed, the SPM only replies to commands sent by the Master device. The Master was set to send a data packet with a 10 minutes time interval. Finally, **idle 2**, evaluates the autonomy of the ACoM module with the module configured only to reply to the commands sent by the Master device. In this test the SPM is disconnected and the Master inquires the ACoM every 5 seconds which corresponds to the time interval used in **measure 1** and **measure 2**. The obtained results are summarized in table I, which also contains the autonomy with data encryption disabled at the ACoM. The system was tested with a 3.7 V Li-on battery with a rated capacity of 1300 mA/h.

The results obtained in the **idle 2** test show that the ACoM achieves a good efficiency. These results can also be further improved by using the power saving modes provided by the

TABLE I
DNA RECOGNITION SYSTEM AUTONOMY.

	Encryption	
	on	off
measure 1	7h 40min	7h 50min
measure 2	13h 40min	13h 55min
idle 1	26h 30min	26h 50min
idle 2	45h 40min	46h 05min

Bluetooth adapter. The biological recognition system also does not require the maximum operating range of the adapter, which would also reduce the required power. Using some of the optimization techniques presented in section III-C, the power consumption of the ACoM was significantly reduced. The most favorable configuration was the following: bluetooth configured as a class 2 device (range 10m) and in sniff mode 80; and MC configured to shut down all peripherals when it entered idle mode, except the UART peripheral. This optimization resulted in an improvement in the autonomy of the **measure 1** test with encryption of 11.4% leading to an autonomy of 8h 30min. The obtained results show that the developed system is also a real autonomous system. A typical analysis can take up to one hour, which means that the system can perform up to eight analysis without being recharged. Moreover, it can be observed that the execution of the encryption algorithm, requires less than 2 % of total energy consumed by the system. Nevertheless, the results can be improved by further optimizing the SPM power management or by using a newer digital signal processor. The SPM design is now being refined aiming a 24 hour continuous operation. In the new design, the processor will be replaced by a similar device that only requires 215 mW to operate at 30 MIPS, while achieving a much lower idle power consumption (50 mW). The on-board memory will also be replaced by a newer and less power consuming one. Finally, considering the better results of **measure 2**, an additional effort is being performed to improve the measurement method efficiency by replacing the external magnetic drive circuitry with a solution integrated in the biochip itself.

Regarding the movement monitoring system, two tests were performed to assess autonomy. In both experiments the ACoM MC was configured to perform 4 MIPS. In the first test, **measure 1**, the ACoM was configured to retrieve the accelerometer value 10 times per second. Each packet has 50 bits of valid data. In order to optimize the communication with the Master, a first in first out (FIFO) buffer is implemented in the ACoM. When this FIFO reaches the 128 bits required to perform data encryption, the data is processed and sent to the Master through the Bluetooth adapter. Since the bandwidth required for this acquisition is low, the Bluetooth adapter data rate was set to 9600 bps. The desired sample rate requires that SPM MC must be configured to 2.5 MIPS. The second experience, **idle 1**, evaluates the stand-by time of the movement monitoring system. In this test the Master device requests a reading from the SPM every 10 minutes. The system was tested with the same 3.7 V Li-on battery (1300 mA/h). The test results, with

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

and without data encryption at the ACoM, are summarized in table II.

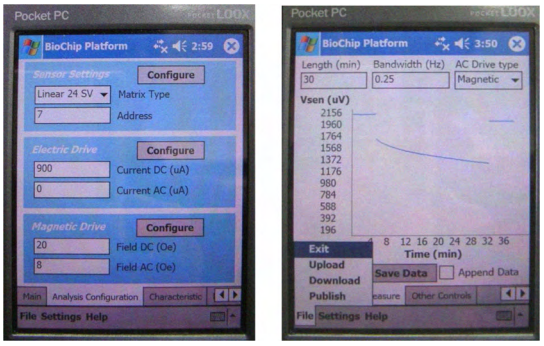
TABLE II
MOVEMENT MONITORING SYSTEM.

	Encryption	
	on	off
measure 1	24h 50min	25h 05min
idle 1	34h 30min	34h 45min

The optimized configuration of the ACoM lead to a significant increase in the autonomy. As in the previous case, the following configurations were also considered: bluetooth configured as a class 2 device (range 10 m) and in sniff mode 80; and MC configured to shut down all peripherals when it entered idle mode, except the UART peripheral. The autonomy for the test **measure 1** with encryption was improved by 71.7% and is now 42h 10m. The results clearly show that this system can be used to effectively perform movement monitoring. However, in situations were a higher autonomy is desirable, it can be improved by replacing the SPM MC by the more expensive low power version of the same MC.

B. Graphical user interface and web interface

The Master device was implemented in a Pocket Loox 720, with an Intel XScale PXA 272 520 MHz processor, 128 MB RAM memory, Bluetooth 1.2 and USB 1.1 host capabilities. The Master may also be hosted in a laptop computer or other mobile devices (PDAs or smartphones) with minimal or no changes on the software. Two of the menus of the GUI provided by the Master are depicted in Fig. 9. The implemented software for the PDA requires 300 kB of static memory and a total memory of 4.5 MB considering data allocated dynamically.



(a) (b)

Fig. 9. PDA interface menus: *a)* experience configuration; *b)* real-time sensor measure.

The first menu, Fig. 9(a), provides control over the experience parameters. It allows the user to define the biochip geometry, and to set the sensor's electric and magnetic drive signal. In the second menu of Fig. 9(b), it is displayed a result of the measurement performed using the parameters set in the configuration menus. The data provided by the SPM is decrypted and displayed in real-time in the graphic. The option to store the acquired data locally in an XML file, that can also contain the configuration parameters of the SPM, and additional information provided by the user about the experience (e.g. identification of the sample) is also provided. This functionality is useful when the Master device has no connection to the internet, such can be the case when the experiments are being performed. The interface with the remote database server is also displayed in this picture (bottom right tool strip). After configuring the database connection parameters, the interface allows the user to **upload** the acquired data, **download** results from previous experiments from the server or to **publish** data that was locally stored. A similar menu, not displayed in the figure, also allows the extraction, display and storage of the sensor's magnetic characteristic.

The acquired data was registered on the PDA and sent to a desktop computer using the SOAP. Taking advantage of the SOAP interoperability, at the server side the SOAP request is received by an Apache 2.0 web server and interpreted by a PHP 5.0 based web application. The information is inserted on a relational database according to the platform type and identifier. The web server also provides access to the information stored in the database through a web page. This web page is generated using a PHP 5.0 application hosted in the server. The stored data can be graphically represented as a web page like the one depicted in Fig. 10. The graphic is drawn through the use of the JpGraph object-oriented graph creating library in order to generate a png file that can be interpreted by a web browser.

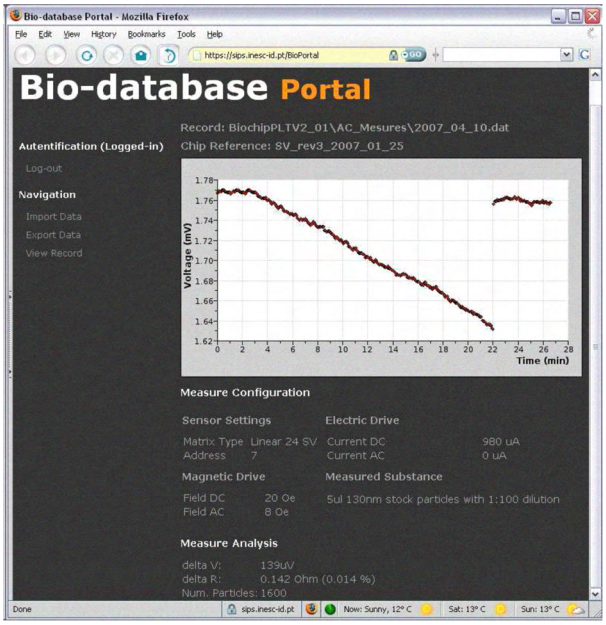


Fig. 10. Snapshot of the web-based data visualization.

In Figure 10 it is shown a test of the DNA recognition detection system using a solution of 30×10^9 particles/ml with

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966

130 nm diameter MPs. The system configuration parameters were similar to the ones used in the autonomy test with magnetic drive. The solution was dropped on the sensor after about 3 minutes and 19 minutes after, the sensor was washed with distilled water. These experimental results clearly show a 140 μV signal component due to the presence of MPs. A resistance variation about 0.014% was detected. The experimental results show that the developed embedded system can be used for particle detection, and therefore to perform biomolecular recognition detection. The web page shows the sensor signal evolution, the most relevant configuration parameters and displays some measure analysis parameters.

VI. Conclusions

This paper proposes a new generic and modular platform for designing distributed autonomous embedded systems for biomedical applications. The architecture of this platform is based on autonomous communication modules that support multiple sensing and processing modules with varied requirements. One or more autonomous communication modules are connected and controlled by a master device, a personal digital assistant or a laptop, through wire or wireless standard communication sub-systems. Public-key or symmetric cryptosystems are applied to assure security when data is communicated with the Master. Masters can act themselves as a second communication layer in order to achieve a distributed environment. Using this secure connection the master devices can upload or download data from a common database located in a remote server.

In order to prove the concept of the proposed platform, we have designed prototypes of autonomous communication modules that support several standard serial peripheral interfaces, universal serial bus and Bluetooth. Moreover, we have designed and implemented embedded systems for biomolecular recognition, based on the detection of paramagnetic nanoparticles attached to target biomolecules, and for monitoring movement, based on 2D accelerometers.

Experimental results show that it is possible to develop autonomous modular embedded systems for biological and biomedical applications with off-the-shelf components and the effectiveness of the proposed architecture to design distributed embedded systems. The scalability of the system was also verified by using several copies of the prototypes of the two types of embedded systems, multiple masters and a server with different databases.

Acknowledgment

José Germano and Rui Ramalho thanks FCT for their PhD grants SFRH/BD/30056/2006 and SFRH/BD/45032/2008 respectively. INESC-Investigação e Desenvolvimento as an Associated Lab acknowledges FCT funding.

References

[1] M. Piedade, L. A. Sousa, T. M. Almeida, J. Germano, B. A. Costa, J. M. Lemos, P. P. Freitas, H. A. Ferreira, and F. A. Cardoso, "A new hand-held microsystem architecture for biological analysis," *IEEE Trans. Circuits Syst. Regul. Pap.*, vol. 53, no. 11, pp. 2384–2395, 2006.

[2] Tae-Soo Lee, Joo-Hyun Hong, and Myeong-Chan Cho, "Biomedical digital assistant for ubiquitous healthcare," *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE*, pp. 1790–1793, 22-26 Aug. 2007.

[3] E. Jovanov, D. Raskovic, J. Price, J. Chapman, A. Moore, and A. Krishnamurthy, "Patient monitoring using personal area networks of wireless intelligent sensors," *Biomed Sci Instrum*, vol. 37, pp. 373–378, 2001.

[4] A. Halteren, R. Bults, K. Wac, D. Konstantas, I. Widya, N. Dokovski, G. Koprinkov, V. Jones, and R. Herzog, "Mobile patient monitoring: The mobihealth system," *The Journal on Information Technology in Healthcare*, vol. 2, no. 5, pp. 365–373, October 2004.

[5] N. Lovell, F. Magrabi, B. Celler, K. Huynh, and H. Garsden, "Web-based acquisition, storage, and retrieval of biomedical signals," *Engineering in Medicine and Biology Magazine, IEEE*, vol. 20, no. 3, pp. 38–44, May/Jun 2001.

[6] P. Dario, M. C. Carrozza, A. Benvenuto, and A. Menciassi, "Micro-systems in biomedical applications," *Journal of Micromechanics and Microengineering*, vol. 10, no. 2, pp. 235–244, 2000.

[7] E. Joseph and D. Bronzino, *The Biomedical Engineering Handbook*, 2nd ed. Boca Raton: CRC Press, 2000, ch. 53.

[8] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi, and S. Weerawarana, "Unraveling the Web services web: an introduction to SOAP, WSDL, and UDDI," *Internet Computing, IEEE*, vol. 6, no. 2, pp. 86–93, Mar/Apr 2002.

[9] "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," Committee on Nat. Security Systems Policy No.15, Fact Sheet No.1, 2003.

[10] Microchip, "Data Encryption Routines for PIC24 and dsPIC Devices," 2006, ref: DS01044A.

[11] S. X. Wang and L. Guanxiong, "Advances in giant magnetoresistance biosensors with magnetic nanoparticle tags: Review and outlook," *IEEE Trans. Magn.*, vol. 44, no. 7, pp. 1687–1702, 2008.

[12] J. Schotter, P. B. Kamp, A. Becker, A. Pühler, G. Reiss, and H. Brückl, "Comparison of a prototype magnetoresistive biosensor to standard fluorescent DNA detection," *Biosens. Bioelectron*, vol. 19, pp. 1149–1156, 2004.

[13] H. A. Ferreira, F. A. Cardoso, R. Ferreira, S. Cardoso, and P. P. Freitas, "Magnetoresistive dna chips based on ac field focusing of magnetic labels," *J. App. Phys.*, vol. 99, p. 08P105, 2006.

[14] F. A. Cardoso, H. A. Ferreira, J. P. Conde, P. P. Freitas, D. Vidal, J. Germano, L. Sousa, M. S. Piedade, B. A. Costa, and J. M. Lemos, "Diode/magnetic tunnel junction cell for fully scalable matrix-based biochip," *J. Appl. Phys.*, vol. 99, p. 08B307, 2006.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5966
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5966