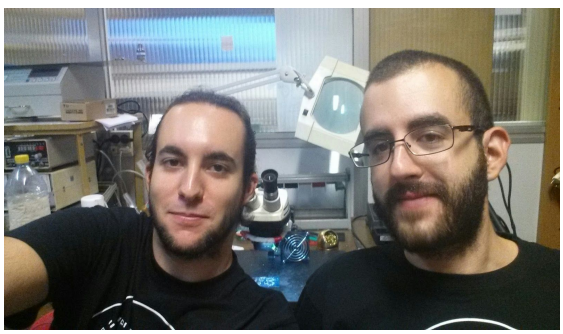
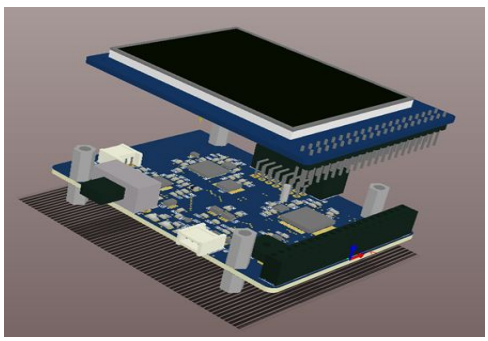
Texas Instruments Innovation
Challenge: Europe Design Contest 2015 Project Report
H2H Pacemaker Secure Access Device

Team Leader:	Samuel López Asunción [samuel.lopez.asuncion@alumnos.upm.es]
Team Members:	Tomás Valencia Noheda [tomas.valencia.noheda@alumnos.upm.es]
Advising Professor:	Alvaro Araujo Pinto [araujo@die.upm.es]
University:	Technical University of Madrid -Spain
Date:	31.07.2015

Qty.	**TI Part Number & URL**	**Qty.**	**TI Part Number & URL**
1	BQ24090	1	CC2560
1	UCC28910	1	LMS33460
1	ADS1291	1	TXB0106
1	BQ27421	1	MSP430FR5972





Project abstract: Following the emerging trend of using biometrical signals as an authentication method for plenty of applications, such as fingerprint or retinal print recognition, we were inspired by the paper [1], which presents H2H (Heart 2 Heart) as a way to securely interact with medical devices, such as pacemakers, in order to access and change its configuration. The system is based on a simple acquisition of a heartbeat signal using an analog front end for ECG applications provided by TI, and the processing of that signal in order to extract 4 high entropy and uncorrelated bits. This is possible because of the inherent randomness that exists in the time between R peaks in the heartbeat signal. This stream of bits is then checked against the signal measured by the pacemaker, which then allows the user to access it if they are near the patient. The project is also focused in implementing a high functionally, low cost system, capable of including new features. We have developed a compact device capable of data acquisition, processing and communication via a wireless connection; it works on a LiPo battery for portable use with an estimated battery autonomy of 300 uses. We have also developed a charging module based on a flyback off-line power supply.

INTRODUCTION AND MOTIVATION

In a world with a growing necessity of better security systems, static or pre-shared passwords are getting quite obsolete due to the inherent risk of relying on something that has to be remember or stored. The increasing amount of stored data that belongs to a regular citizen (such as medical history, bank information and even private conversations) is making this problem increasingly important, as this kind of security systems are in many cases vulnerable, rendering them unable to protect our rights to privacy and security. In order to prevent malicious attacks many approaches are trying to find the optimal point between simplicity, low cost and good performance systems, such as fingerprint scanning or eye recognition. These biometrical security systems rely on something that doesn't have to be remembered or stored, but instead on something that someone 'is'.

Focusing on this project, we found something that may be even more critical than accessing to personal information of somebody. The fact that medical advances are making possible the development of a wide variety of implantable devices to treat chronic diseases (with the peacemaker as the most common and well known among them) are also devices that are prone to security attacks. They feature continuous monitoring or/and drugs administration by non-invasive configuration and charging, but this advantage is also their biggest drawback, since if extremely caution measures are not taken, the malicious manipulation of these devices can result in serious harm to the patient.

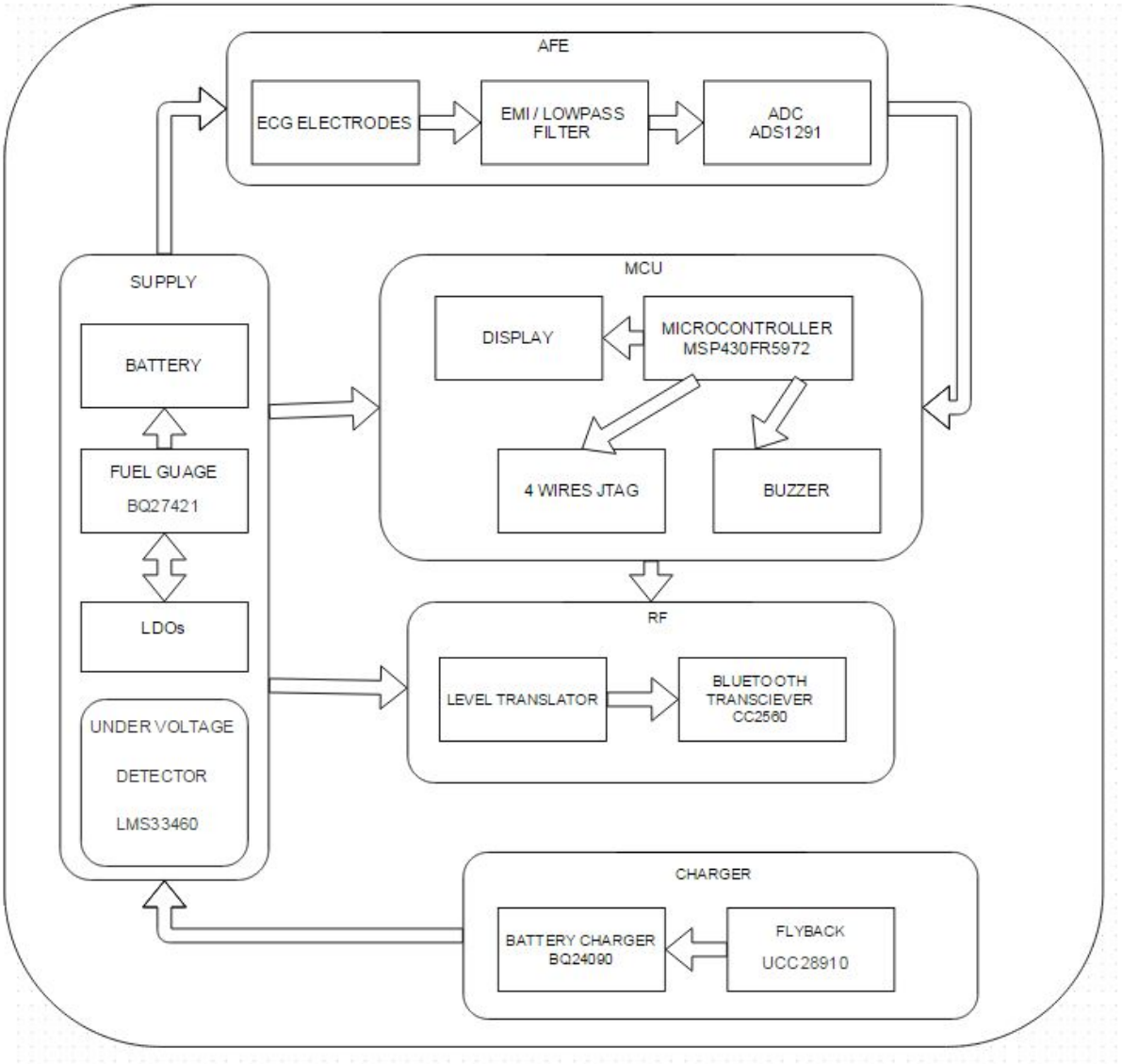
In this context the need of developing security systems that must be extremely hard to hack arises. They must be reliable and must be able to implemented in an environment with very tight design constraints (especially of power consumption and size). Many people are working in order to overcome these challenges, but yet no optimal solution has been found.

This work is aimed to show how with a low cost design and a simple algorithm (in computational terms) we can reach a good performance without requiring a long and costly development process, while offering the possibilities of adding new features.

The two main tools used for developing this project was Altium Designer 14.3 and Code Composer Studio, the free IDE provided by TI.

Implementation

A block-level schematic of the architecture of our heart signal acquisition system is depicted in the following picture:



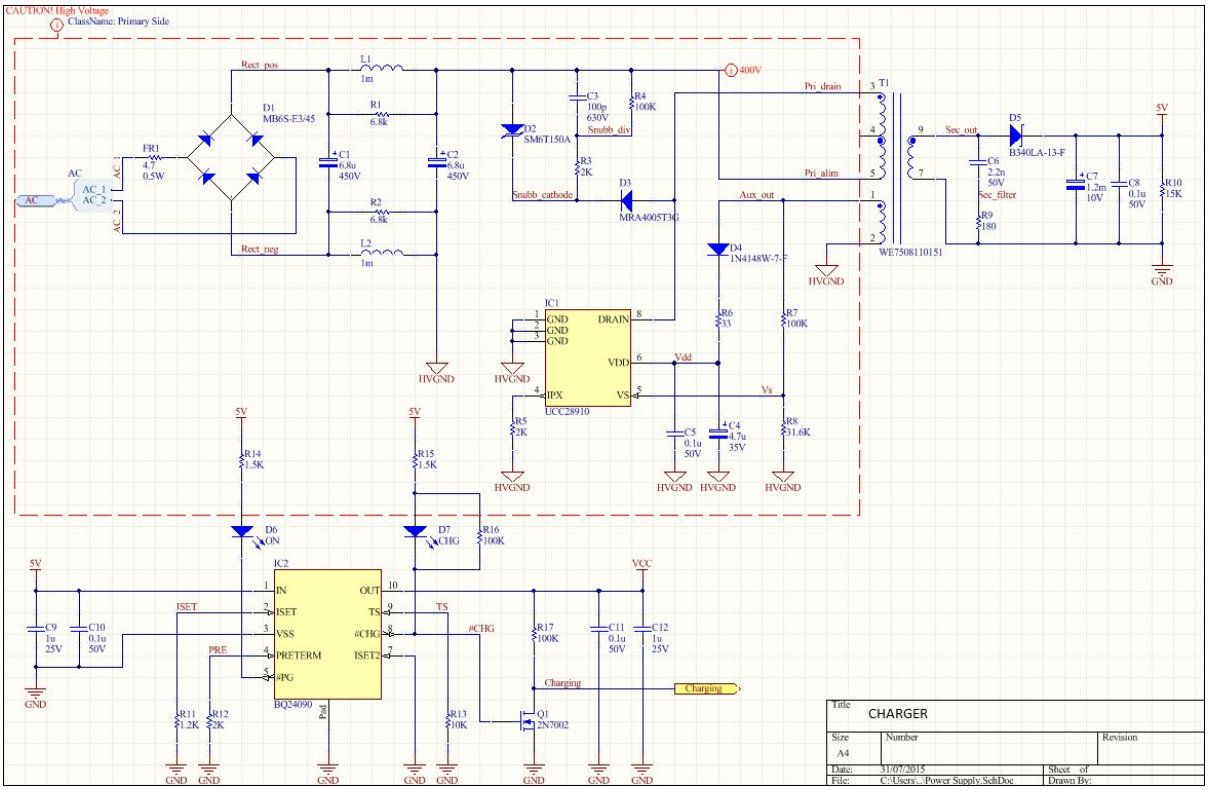
The system can be divided in 5 main parts:

Battery Charger

This module implements a flyback AC/DC converter using the UCC28910 as flyback switcher controller and BQ24090 battery charger.

This provides a 5V, 4W power source capable of 85-285V and 50-60 hz range input, valid for either europe or EEUU. The charging current is limited to 450 mA by hardware .

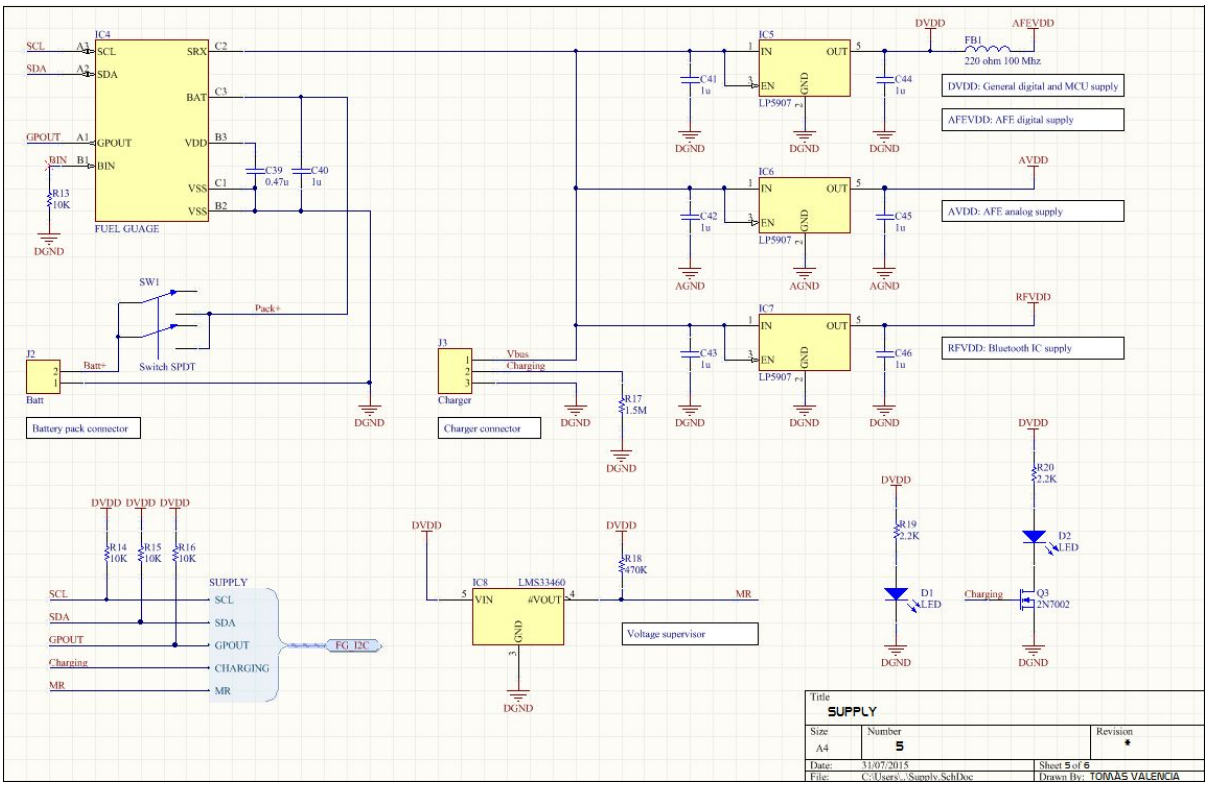
The main reasons of the choice of those IC were the cost-performance ratio and the fact that the UCC28910 has and application note where is explained with high detail how to design the power source, saving us a lot of time.



Supply module

It's responsible to provide the necessary voltages to the rest of the system and also to control the battery charging. It uses the BQ27421 as a fuel gauge for battery level measurements, 2 LP5907 LDOs for the 3.3V analog and digital supplies and a 1.8V LP5907 LDO for the RF interface. The main reasons why we chose the BQ27421 were the small package size (size was a concern since this is intended to be a portable device) and some characteristics suitable for our design (charging current, battery chemistry and communication interface). We also included a 3V LMS33460 voltage supervisor.

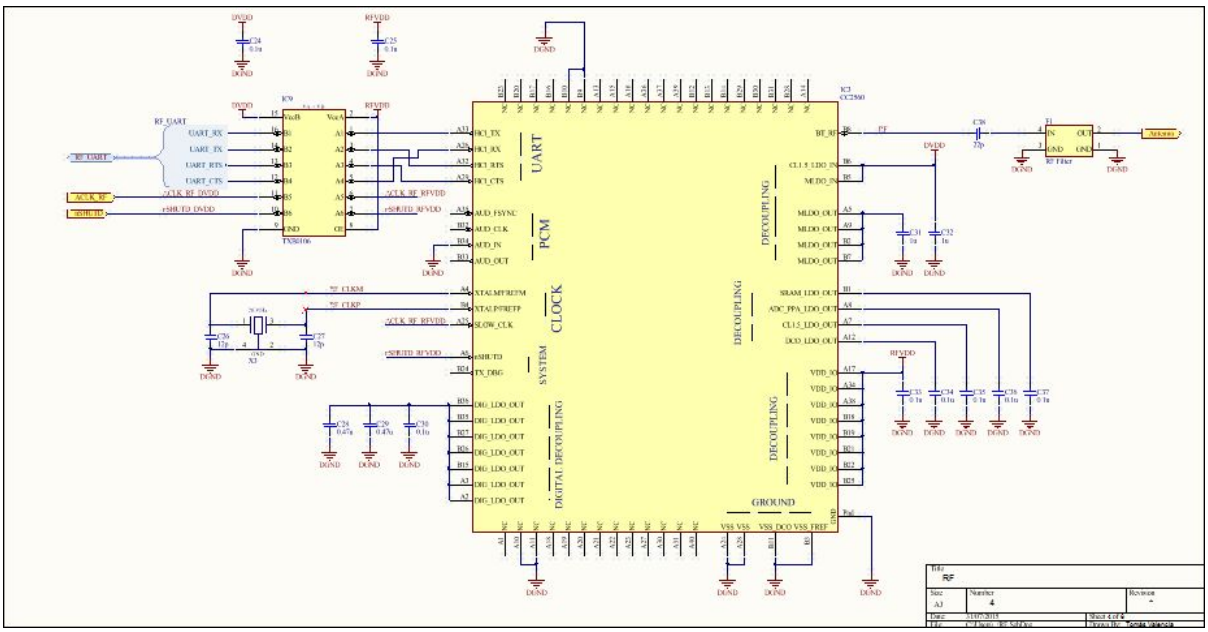
We use a 1150 mAh battery which is capable of giving more than 2 h of full activated mode battery autonomy (the total current consumption of the board is 500 mA). Since this device is thought to be in deep sleep mode most of the time, with 15-20 seconds of active use per access, this allows an average of 350 uses before a recharge is needed, which should be more than enough in a usual case scenario. Finally, this module is directly communicated with the MCU to retrieve information of the remaining battery charge, voltage levels, battery status and many more. This allows to develop further energy planification to reduce power consumption by temporarily disabling non critical parts, such as the display.



RF module

It implements the wireless communication function. It is composed of the CC2560 bluetooth controller and the 2.4 GHz Inverted F Antenna printed on the PCB (Design Note DN0007), as well as the TXB0106 voltage level translator necessary for the 1.8V I/O signal of the CC2560.

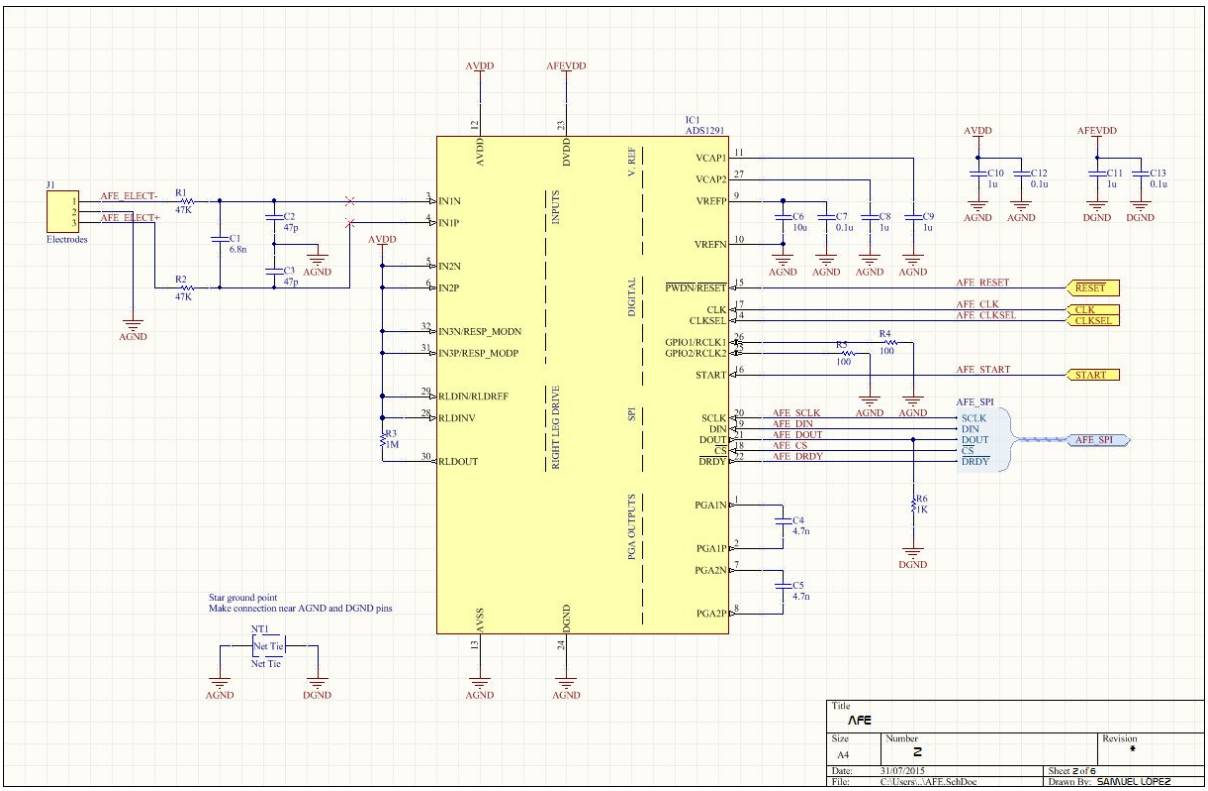
We chose the CC2560 IC to be the Bluetooth controler mostly because it can be used with the TI bluetooth stack without further programming, but also because its power management features (shutdown and sleep modes) are useful to implement low power modes.



AFE module

The data acquisition module. It's implemented using the ADS1291, with input signal and EMI filters and the ECG electrodes. As stated in the datasheet, the PCB layout has been carefully designed to achieve low levels of noise (14 uV peak to peak noise measured without any input).

The choice of the ADC was made taking into account that the data acquisition was one of the most critical points of the system, since noisy or inaccurate measurements could lead to a failure in its main function. This analog front end offers a good performance (>19 noise-free bits at some data acquisition rates), enough to detect heartbeat signal peaks.



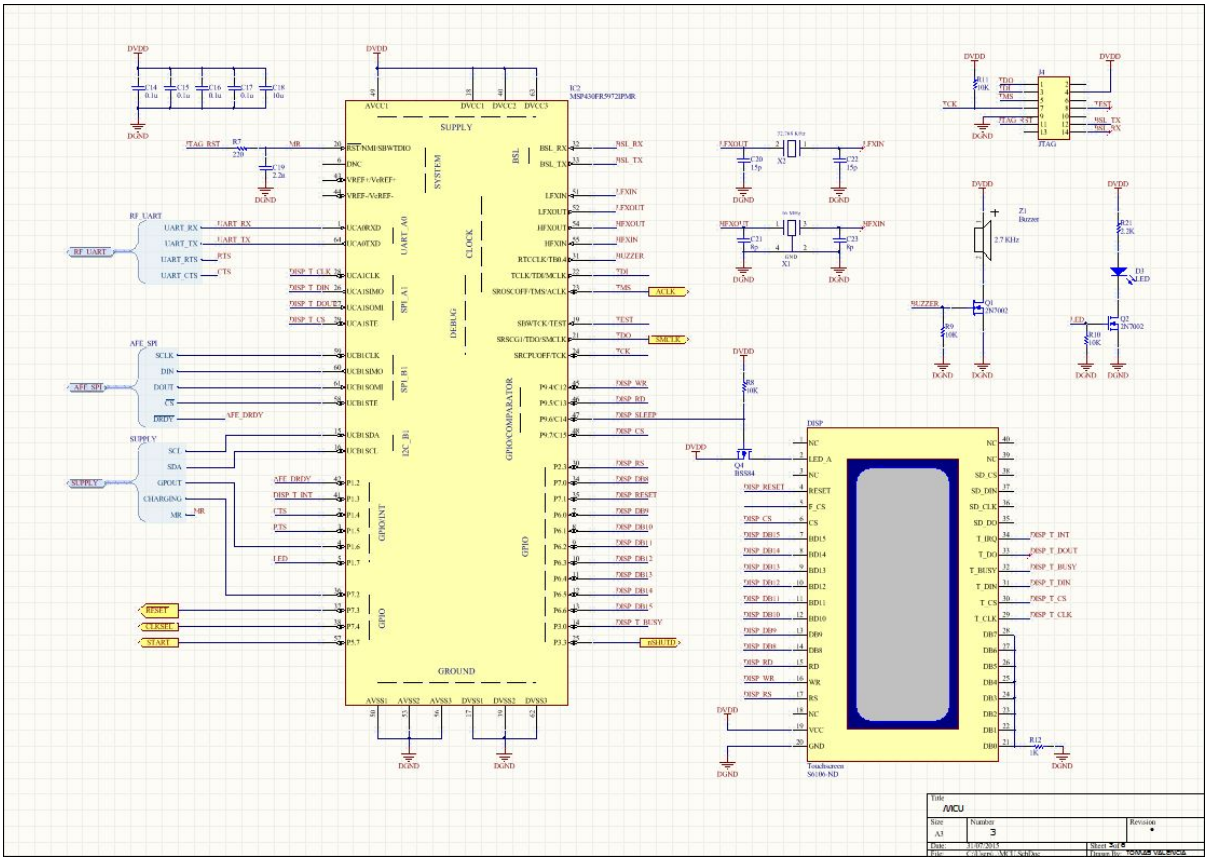
MCU module

This module includes the main processor (MSP430FR5972) and a 2.4” TFT display with resistive touchpad which is intended to give a graphic interface to the board, as well as some LEDs and a buzzer. We also included a JTAG connector to program the microcontroller.

The choice of the MCU was one of the hardest in the design process. On one hand, we wanted to fully cover the requirements of our design (serial interfaces, GPIO, etc) without over dimensioning the system, having in mind the size and power consumption constraints. On the other hand, we needed to provide enough room for adding new functionalities and improving the existing ones (more complex algorithms, a better graphic interface, etc). Also, we need some encryption method for the data generated, so we searched for one microcontroller with an AES256 hardware module. Finally, we chose this MCU as the compromise solution between the two first concerns.

Focusing on the functionality, this module performs 3 main tasks: reads and processes the data from the AFE according to the implemented algorithm, controls the wireless module in

order to communicate with other devices, and generates the graphic interface by reading the touchscreen output and drawing graphics in the LCD.



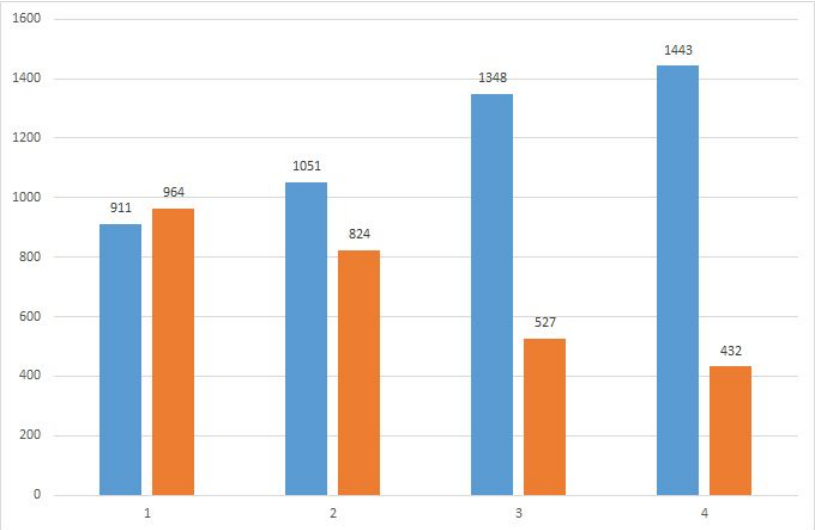
When the tactile switch on the sensor board is pressed, an interrupt is raised and the microcontroller exits from the deep sleep mode. The microcontroller and the peripherals (the ADS1291 via SPI, the display via parallel interface and the CC2560 via USCI) are then initialized. Next, the data readings from the ADC and the calculations necessary for the algorithm are performed. Meanwhile, the ECG is shown in the display. When the calculations are finished and the key is generated, this information is encrypted using the AES256 module and the data is transmitted via Bluetooth through the USCI. After that, the system returns to a deep sleep mode again.

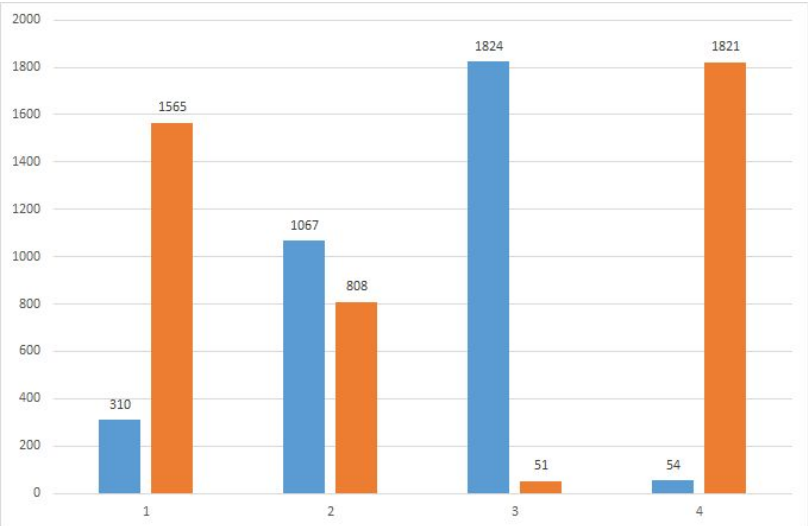
Experimental results

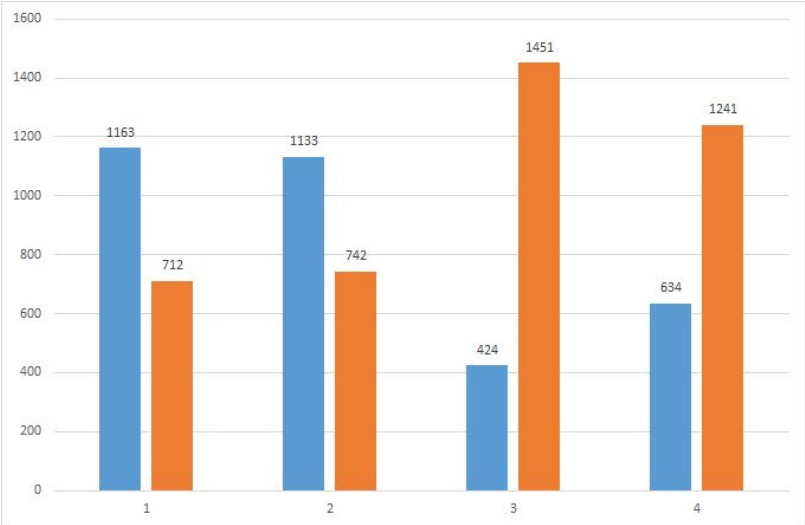
Since the final design could not be properly tested, the result we got are only those in the early stages of development, where we tested the data acquisition and processing to see if the algorithm truly generates 4 uncorrelated bits.

The analysis was pretty basic, as we only check how many times did each bit took the 1 or 0 value in 15 secs windows.

In blue, the number of zeros and in orange the number of ones:







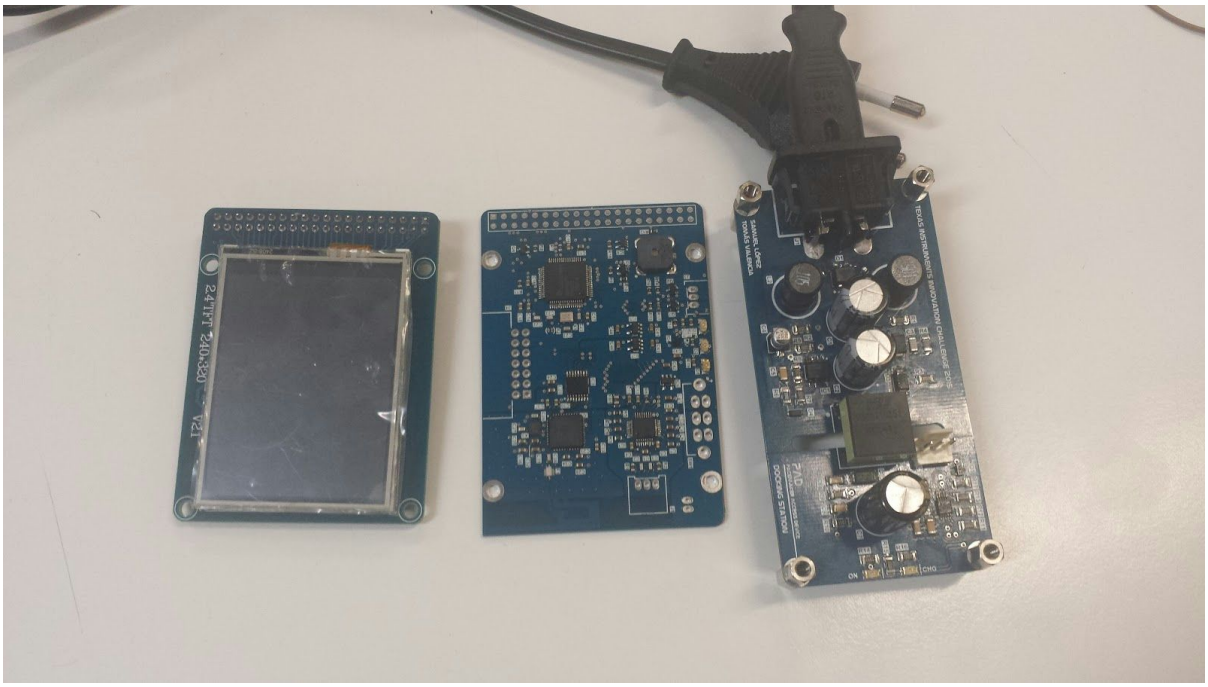
Since this is statistical information, 3 samples aren't really representative, but this is intended to show how form a consecutive 45 seconds of data acquisition. The distribution changes dramatically, which is a good proof for the utility of this authentication method.

Conclusions

This project had two main objectives: first, showing that is possible to generate a high entropy key with a simple algorithm and second, building a portable device capable of implementing this functionality and also to be the base for more complex biosecurity systems in the future. The first one was completely fulfilled with a small experiment. The second one was too ambitious for the time and resources we had and it's not yet being tested properly, but design is complete, only the implementation and testing are left.

Future plans

The future plans for this project are the implementation and testing of the system to check if it offers the functionality that it's designed for. Second, the work should focus on improving the strength of the security algorithm in terms of the key generation and also in making the RF transmission and authentication process more robust and invulnerable to malicious attacks.



In the picture, from left to right:

TFT Display 320x240, partially finished ECG Main Board prototype,
finished and working Battery Charger 5V/4W

Bill of materials

Charger

Comment	LibRef	Designator	Quantity	Supplier 1	Supplier Part Number 1
6.8u	Pol Capacitor	C1, C2	2	Farnell	1831315
100p	Capacitor	C3	1	Farnell	2211011
4.7u	Pol Capacitor	C4	1	Farnell	2069186
0.1u	Capacitor	C5, C8, C10, C11	4	Farnell	2407345
2.2n	Capacitor	C6	1	Farnell	2409062
1.2m	Pol Capacitor	C7	1	Farnell	1848381
1u	Capacitor	C9, C12	2	Farnell	2346954
MB6S-E3/45	MB6S-E3/45	D1	1	Farnell	1815631
SM6T150A	SM6T150A	D2	1	Farnell	9885889
MRA4005T3G	MRA4005T3G	D3	1	Farnell	1459136
1N4148W-7-F	1N4148W-7-F	D4	1	Farnell	1776392
B340LA-13-F	B340LA-13-F	D5	1	Farnell	1843681
ON	LED	D6	1	Farnell	2426228
CHG	LED	D7	1	Farnell	2426227
4.7	Fuse Resistor	FR1	1	Farnell	9474080
Inlet, IEC	Inlet, IEC - Plug	J1	1	Farnell	9248161
1m	Inductor	L1, L2	2	Farnell	2457618
2N7002	2N7002	Q1	1	Digi-key	568-5818-1-ND
6.8k	Resistor	R1, R2	2	Digi-key	CR1206-FX-6801ELFCT-ND
2K	Resistor	R3, R5, R12	3	Digi-key	CR1206-FX-2001ELFCT-ND
100K	Resistor	R4, R7, R16, R17	4	Digi-key	CR1206-FX-1003ELFCT-ND
33	Resistor	R6	1	Digi-key	P33.0FCT-ND
31.6K	Resistor	R8	1	Digi-key	CR1206-FX-3162ELFCT-ND
180	Resistor	R9	1	Digi-key	CR1206-FX-1800ELFCT-ND
15K	Resistor	R10	1	Digi-key	CR1206-FX-1502ELFCT-ND
1.2K	Resistor	R11	1	Digi-key	CR1206-FX-1201ELFCT-ND
10K	Resistor	R13	1	Digi-key	CR1206-FX-1002ELFCT-ND
1.5K	Resistor	R14, R15	2	Digi-key	CR1206-FX-1501ELFCT-ND
WE7508110151	WE7508110151	T1	1	Digi-key	1297-1122-ND

ECG Main Board

Comment	LibRef	Designator	Quantity	Supplier 1	Supplier Part Number 1
6.8n	Capacitor	C1	1	Digi-Key	399-9120-1-ND
47p	Capacitor	C2, C3	2	Digi-Key	399-1056-1-ND
4.7n	Capacitor	C4, C5	2	Digi-Key	399-9091-1-ND
10u	Capacitor	C6, C18	2	Digi-Key	490-10728-1-ND
0.1u	Capacitor	C7, C12, C13, C14, C15, C16, C17, C24	15	Digi-Key	490-1532-1-ND
		C25, C30, C33, C34, C35, C36, C37			
1u	Capacitor	C8, C9, C10, C11, C31, C32, C40	13	Digi-Key	490-3900-1-ND
		C41, C42, C43, C44, C45, C46			
2.2n	Capacitor	C19	1	Digi-Key	399-7881-1-ND
15p	Capacitor	C20, C22	2	Digi-Key	399-9004-1-ND
8p	Capacitor	C21, C23	2	Digi-Key	490-9670-1-ND
12p	Capacitor	C26, C27	2	Digi-Key	490-10704-1-ND
0.47u	Capacitor	C28, C29, C39	3	Digi-Key	490-3295-1-ND
22p	Capacitor	C38	1	Digi-Key	399-9031-1-ND
47K	Resistor	R1, R2	2	Digi-Key	CR0603-FX-4702ELFCT-ND
1M	Resistor	R3	1	Digi-Key	CR0603-FX-1004ELFCT-ND
100	Resistor	R4, R5	2	Digi-Key	CR0603-FX-1000ELFCT-ND
1K	Resistor	R6, R12	2	Digi-Key	CR0603-FX-1001ELFCT-ND
220	Resistor	R7	1	Digi-Key	CR0603-FX-2200ELFCT-ND
10K	Resistor	R8, R9, R10, R11, R13, R14, R15, R16	8	Digi-Key	CR0603-FX-1002ELFCT-ND
1.5M	Resistor	R17	1	Digi-Key	311-1.50MHRCT-ND
470K	Resistor	R18	1	Digi-Key	CR0603-FX-4703ELFCT-ND
2.2K	Resistor	R19, R20, R21	3	Digi-Key	CR0603-FX-2201ELFCT-ND
220 ohm 100 Mhz	Ferrita	FB1	1	Digi-Key	490-1054-1-ND
Header 20x2	Touchscreen	DISP	1	Digi-Key	S6106-ND
RF Filter	LFB212G45SG8A127	F1	1	Digi-Key	490-5021-1-ND
ADS1291	ADS1291	IC1	1	Digi-Key	296-36547-5-ND
BQ27421	BQ27421	IC4	1	Digi-Key	296-38880-1-ND
LP5907	LP5907	IC5, IC6	2	Digi-Key	296-38557-1-ND
LP5907	LP5907	IC7	1	Digi-Key	296-41463-1-ND
LMS33460	LMS33460	IC8	1	Digi-Key	LMS33460MG/NOPBCT-ND
TXB0106	TXB0106	IC9	1	Digi-Key	296-23759-1-ND
Electrodes	JST PH 3 Pin Socket	J1	1	Digi-Key	455-1720-ND
Batt	JST PH 2 Pin Socket	J2	1	Digi-Key	455-1719-ND
Charger	JST PH 3 Pin Socket	J3	1	Digi-Key	455-1720-ND
JTAG	JTAG 14 Pins	J4	1	Digi-Key	ED10534-ND
2N7002	2N7002	Q1, Q2, Q3	3	Digi-Key	568-5818-1-ND
BSS84	BSS84	Q4	1	Digi-Key	BSS84CT-ND
Spacer	Spacer 11mm M3x0.5	SP1, SP2, SP3, SP4	4	Digi-Key	952-2312-ND
Spacer	Spacer 7mm M3x0.5 Screw	SP5, SP6, SP7, SP8	4	Digi-Key	952-1498-ND
Switch SPDT	MFS201N-16-Z	SW1	1	Digi-Key	563-1558-ND
XTAL_32768	XTAL_32768	X2	1	Digi-Key	535-9032-ND
XTAL_26_MHz	XTAL_26_MHz	X3	1	Digi-Key	644-1261-1-ND
XTAL_16MHZ	XTAL_16_MHz	X1	1	Farnell	2467444
CC2560	CC2560	IC3	1	Farnell	2334559
LED	LED	D1	1	Farnell	2426228
LED	LED	D2	1	Farnell	2426227
LED	LED	D3	1	Farnell	2426229
Buzzer	Buzzer	Z1	1	Farnell	2215090