PROYECTO FIN DE CARRERA

TÍTULO: Diseño e implementación de un servicio de acceso inalámbrico a dispositivos médicos mediante H2H

AUTOR**:** Tomás Valencia Noheda

TUTOR**:** Álvaro Araujo Pinto

DEPARTAMENTO**:** Ingeniería electrónica

TRIBUNAL:

Presidente**:** Da. Ma Elena Hernando Perez

Vocal: D. Alvaro Araújo Pinto

Secretario**:** D.Fernando Fernandez Martínez

VocalSuplente**:** D. Octavio Nieto-Taladriz García

FECHA DE LECTURA**:** Madrid, de de 2016

CALIFICACION**:**

Resumen

En este proyecto de fin de carrera se ha desarrollado el software para el servicio de autentificación Heart To Heart. El objetivo es conseguir un método de acceso seguro a dispositivos médicos implantables que utilice claves generadas dinámicamente a partir de la señal biométrica del corazón. El sistema estará compuesto por un dispositivo de acceso que será utilizado por el usuario que quiera conseguir acceso al dispositivo medico implantable, y un dispositivo que simulará dicho dispositivo médico. Ambas plataformas hardware han sido diseñadas e implementadas en el proyecto DER SAMUÉ.

Como referencia se ha utilizado teórica la publicación [1], en la que se detallan y justifican los algoritmos y protocolos utilizados. (…..)

Para llevar a cabo el proyecto, se ha comenzado estableciendo los requisitos que deberá cumplir el software, así como un estudio de la plataforma hardware utilizada para este proyecto.

A continuación, se ha realizado un proceso de diseño de los distintos módulos software que realizaran las funcionalidades necesarias para conseguir la implementación del servicio Heart To Heart tanto en el lado del dispositivo acceso como en el simulador de dispositivo médico.

Por último, se han realizado una serie de pruebas para comprobar el correcto funcionamiento del sistema y su resistencia a ataques maliciosos, además de su posible utilidad como herramienta de ayuda al diagnóstico.

Palabras clave

Dispositivo medico implantable, protocolo H2H, seguridad biométrica (…)

Agradecimientos

Índice

Índice de figuras

Índice de tablas

Acrónimos

H2H *Heart To Heart*

ECG *Electrocardiograma*

# Introducción

## Motivación

El uso de los dispositivos médicos implantables está ampliamente extendido debido a las facilidades que ofrecen a la hora de monitorizar constantemente al paciente y proporcionarle tratamiento que de otra manera seria más complejos o agresivos de aplicar. Los dispositivos médicos activos (marcapasos, bombas de insulina, etc.) normalmente disponen de módulos radio que permiten tanto la extracción de datos del paciente como la reprogramación/reajuste de dichos dispositivos de una manera no invasiva.

En la actualidad, los protocolos de comunicación son poco seguros ya que se prioriza el que el acceso sea rápido y sencillo en casos de riesgo crítico para la salud. Sin embargo, diversos estudios como el realizado en [3] han demostrado que dicho planteamiento es altamente inseguro, ya que con una formación y unos recursos “básicos” se pueden realizar ataques que permitan el acceso a los datos monitorizados e incluso desactivar o alterar el funcionamiento del IMD.

Este proyecto está centrado en mejorar la seguridad en el acceso a estos dispositivos, ya que un acceso no autorizado puedo poner en peligro no solo la privacidad del paciente, sino su propia salud. Para solucionar esta deficiencia de seguridad, se plantea desarrollar un sistema que conserve esa capacidad de acceso rápido para situaciones de peligro, pero a la vez aumente en gran medida la resistencia ante ataques maliciosos. Esta solución consiste en un dispositivo de dimensiones reducidas y uso sencillo que genere una clave de acceso dinámicamente mediante una señal biométrica, la cual será validada por el propio dispositivo médico. El procedimiento de validación consistirá en la monitorización de la frecuencia cardiaca durante unos segundos y a partir de la información recogida, generar una ficha de acceso única que será enviada al dispositivo, que al compararla con la que él mismo ha generado a partir de su información de la señal cardiaca, tomara la decisión de permitir o bloquear la petición.

## Objetivos

El objetivo de este proyecto es el de diseñar e implementar un servicio de acceso inalámbrico a dispositivos médicos mediante H2H. El sistema se encarga de proporcionar un método de acceso sencillo y seguro a dispositivos médicos implantables.

Dentro de este objetivo principal, pueden distinguirse los siguientes subobjetivos:

* Desarrollo de un módulo software que se encargará del tratamiento de la señal recogida por los electrodos y la extracción de la información necesaria para generar la clave.
* Desarrollo de un módulo software que controlará el acceso al dispositivo médico, bien validando la contraseña recibida o bien entrando en modo promiscuo en caso de que situación de riesgo para la salud.
* Desarrollo de un módulo software que gestionará la comunicación inalámbrica, tanto el proceso de descubrimiento de dispositivos como el de emparejamiento de los mismos
* Desarrollo de un módulo software de interfaz de usuario, lo cual permitirá al usuario comenzar el proceso de acceso de una manera sencilla e intuitiva, así como la presentación de otros datos de interés.

El objetivo principal de ambos proyectos en conjunto es desarrollar e implementar un sistema electrónico portátil que permita acceder a la configuración y registros de un marcapasos simulado utilizando una política de acceso “touch-to-access” a través de una conexión inalámbrica.

## Planificación del desarrollo

El desarrollo del proyecto ha seguido las siguientes fases:

* Análisis y definición del sistema, que incluye el estudio de las publicaciones en las que se basa este proyecto y la plataforma hardware en la que se va a desarrollar con el objetivo de poder definir los requisitos que tiene que cumplir la solución propuesta.
* Diseño de la solución propuesta, estableciendo para cada una de las partes los submodulos de los que estará formado y detallando las decisiones que se han tomado para conseguir que se cumplan los requisitos definidos antes.
* Implementación del software del sistema, lo cual implica un análisis de las distintas estrategias posibles para abordar el problema, la decisión de cual seguir y la programación de software necesario para dicha solución.
* Realización una serie de pruebas para comprobar el correcto funcionamiento de todos los módulos del sistema, tanto del hardware como del software desarrollado, y su conformidad con los requisitos planteados.
* Por último, se han extraído una serie de conclusiones sobre la solución final implementada y se sugieren varias líneas futuras a partir del trabajo realizado.

# Análisis de requisitos

## Introducción

En este capítulo se analizarán los requisitos que deben cumplir los distintos módulos software. Este proyecto está basado en el contenido de la publicación [1], por lo que los requisitos han sido definidos acorde con lo necesario para implementar su propuesta.

Adicionalmente, para la detección de la frecuencia cardiaca se ha desarrollado un algoritmo basado en el algoritmo “The Hamilton and Tompkins QRS detector” detallado en [2], por lo que los requisitos de la parte de tratamiento digital de señal han sido definidos teniendo también en cuenta las restricciones necesarias para este algoritmo.

## Servicio

### Tratamiento de la señal cardiaca

Este módulo deberá acondicionar la señal adquirida con el objetivo de extraer la información de la manera más precisa posible. Dado que el sistema hardware no cuenta con un módulo especifico de tratamiento de señal, el diseño de esta parte deberá tener especial cuidado con el tiempo de ejecución, con lo que habrá que llegar a un compromiso entre la exactitud y la duración.

#### Requisitos de resolución y fase de los filtros

El filtrado digital de este sistema se encargará de eliminar la máxima cantidad de ruido proveniente de la adquisición de la señal cardiaca conservando las componentes que contienen la información fundamental para el sistema. Añadiendo esto último, los requisitos pueden resumir en:

* Los filtros elegidos deben ser del menor orden posible para que el tiempo de cálculo sea limitado.
* La fase de dichos filtros deberá ser lo más lineal posible, ya que un retardo de grupo no constante puede distorsionar el cálculo de la frecuencia cardiaca.
* Su respuesta debe estable, insensible a la cuantización de los coeficientes y con un rizado mínimo en la banda de interés.

#### Algoritmos de detección de ritmo cardiaco

##### El algoritmo utilizado para este sistema deberá ser capaz de extraer la información pulso a pulso ya que en la generación de la contraseña se toma la distancia entre los máximos de la onda R del ECG. Adicionalmente, con el objetivo de no acaparar los recursos del microprocesador, se evitará el uso de algoritmos que almacenen gran cantidad de muestras.

### Algoritmo de autenticación

Este módulo será el encargado de llevar a cabo la función principal del sistema. El modulo debe por un lado generar la clave de autentificación y por el otro, gestionar todo el proceso de validación especificado en [1].

### Comunicación inalámbrica

La tecnología radio utilizada vendrá impuesta por el hardware proporcionado, y la tarea será proveer de una pila de protocolos capaz de gestionarlo. Dicha pila deberá proporcionar además de los servicios básicos para poder establecer la comunicación, algún método para la autentificación de dicha comunicación para evitar ataques del tipo “man in the middle”.

### Interfaz de usuario

La interfaz de usuario debe gestionar todo lo relacionado con la interacción usuario-dispositivo y con la presentación de información útil. Esto requisitos pueden resumirse en lo siguiente:

* Controles básicos del sistema electrónico, que permitirán el inicio de adquisición de datos, apagado por software, etc.
* Visualización del ECG
* Conexión con el marcapasos
* Manipulación de los parámetros del marcapasos

# Diseño del sistema

En esta sección se detalla el diseño del software del sistema. En primer lugar, comenzamos con un análisis de la plataforma hardware proporcionada, poniendo especial atención en el alcance de la capa de abstracción hardware, para poder determinar la flexibilidad de la que disponemos a la hora de modificar algún parámetro de un módulo hardware. Tras esto, daremos una vista general de los bloques que componen el sistema y como se relacionan con los distintos módulos hardware previamente analizados. Por último, detallaremos la funcionalidad individual de cada módulo y las decisiones que se han tomado para el diseño.

## Análisis de la plataforma hardware

El primer paso para el diseño del sistema es el determinar los elementos hardware de los que disponemos y poner especial cuidado en aquellos aspectos que nos impongan algún tipo de restricción, ya sea en funcionalidad, resolución o temporización. Dado que también se ofrece una capa de abstracción hardware, en el análisis obviaremos los detalles de control y configuración que cubre dicha capa de abstracción hardware y al final haremos un breve análisis de dicha capa de abstracción.

### Hardware del primer prototipo

#### Microcontrolador

La plataforma cuenta con un MSP430FR5972 con frecuencia máxima de trabajo de 16MHz y una capacidad de memoria de 64Kb de FRAM para código y 2Kb de RAM, y es utilizado para las funciones de control, calculo y comunicación con otros elementos hardware. Dicho microcontrolador cuenta con multiplicador hardware de 32 bits y carece de unidad de coma flotante, lo cual nos impone el que las operaciones aritméticas se hagan en coma fija.

En cuanto a la comunicación con los demás elementos hardware, cada elemento cuenta con su propio puerto salvo el Analog Front End y el fuel gauge que están conectados al mismo puerto (aunque en distintos pines), por lo que habrá que tener cuidado de reconfigurar el pinout del puerto adecuadamente cada vez que accedamos a cada uno. Para las operaciones de acceso directo a memoria, tenemos tres canales de DMA.

Por último, cabe comentar que dispone una unidad de encriptación hardware (AES256) que nos evitará tener que implementar una encriptación por software.

#### Adquisición de datos

Para la digitalización de la señal cardiaca, se utiliza un Analog Front End especializado para aplicaciones de electrocardiograma (ADS1291), con una velocidad máxima de muestreo de 8000 muestras por segundo y 24 bits por muestras, lo cual es más que suficiente para los requisitos de resolución del algoritmo. Este periférico cuenta con una línea de interrupción para indicar cuando los datos están listos (lo cual nos evitar tener que pollear) y transmite los datos por SPI.

#### Comunicación inalámbrica

El dispositivo utilizado para la comunicación inalámbrica es el CC2560B, que es un circuito integrado que soporta bluetooth clásico, lo cual nos impone el uso de la pila de protocolos para esa tecnología y nos ofrece la posibilidad de establecer comunicaciones autenticadas para la transmisión de los datos necesarios entre el dispositivo de acceso y el simulador de marcapasos. Este módulo se comunica por un puerto UART con control hardware de flujo.

#### Interfaz de usuario

Como elementos de interacción con el usuario, cuenta con tres leds de color rojo, verde y azul, y un buzzer para emitir avisos sonoros y visuales básicos, un interruptor para cortar la alimentación. El PWM necesario para el buzzer está generado por uno de los timer del microcontrolador y los leds se controlan con gpios.

También disponemos display LCD que ofrece la posibilidad de mostrar todo tipo de información visual, desde mensajes de texto hasta representación de señales digitales. Dicho display además cuenta con una touchpad resistivo, lo cual nos permite implementar un intérprete de comandos para incrementar la interacción que se tiene con el sistema. El LCD no tiene un puerto serie hardware específico para él, sino que se ha tenido que implementar un puerto paralelo software mediante varios gpios, lo cual limita la tasa de refresco. El touchpad se comunica por SPI y dispone de una línea de interrupción para avisar cuando hay un cambio de presión en la pantalla.

#### Control de consumo

Para este objetivo contamos con dos elementos principalmente: el primero de ellos son los modos de bajo consumo del microcontrolador, y el segundo es la disposición de LDO’s independientes para cada módulo, lo cual nos permite apagar de forma independiente cada elemento hardware, pudiendo así reducir el consumo sin necesidad de apagar completamente el sistema.

### Capa de abstracción hardware del primer prototipo

Esta capa de abstracción hardware está basada en los registros definidos en el header de nuestro micro (msp430fr5972.h) que proporciona el entorno de desarrollo de Texas Instruments Code Composer Studio.

Esta capa cuenta con funciones que permiten la configuración y el uso de los distintos módulos hardware utilizados en el sistema hardware, lo cual permite construir todo el sistema alrededor de dichas funciones.

#### Funciones de configuración

* Relojes del sistema: Se encarga de configurar los registros necesarios para poder trabajar a la frecuencia escogida (8 MHz)
* Analog front end: Configura el puerto SPI para que se adecue a las necesidades del front end (velocidad, flanco de lectura, etc) y también se encarga de enviar la secuencia de comandos necesaria para configurar los registros del analog front end.
* Interfaz inalámbrica: Realiza la configuración de la UART a través de la cual nos comunicaremos con el modulo radio.
* Buzzer: Esta función configura los registros del timer utilizado para generar el pwm y también los del que se utiliza como base de tiempos para la duración del pitido.
* Pantalla táctil: Estas funciones engloban tanto la configuración del SPI para el touchpad como la secuencia de inicialización del display.

#### Funciones de uso de periféricos

* Envío/recepción de datos: Estas funciones gestionan la recepción y transmisión de datos al periférico para el que están implementadas. Todas ellas están diseñadas de manera que bloquean la ejecución hasta que se completa la operación, lo cual debe ser tenido en cuenta a la hora de la temporización. Aunque el uso es el mismo, según el periférico al que se dirijan, deben gestionar además ciertas señales:
  + Analog front end y touchpad: Gestiona la activación del chip select
  + Lcd: Gestiona la generación y temporización de todas las señales necesarias (referencia al datasheet)
* Activación del buzzer: Permiten la emisión de un pitido con el buzzer de una frecuencia y duración determinadas.

### Hardware del segundo prototipo

Dado que el segundo prototipo tiene en común varios elementos, solo detallaremos las diferencias.

#### Microcontrolador

La plataforma cuenta con un STM32L162VD que ofrece mayores prestaciones en diversos aspectos, algunos de los cuales son especialmente interesantes de cara al servicio.

Primero, su frecuencia de trabajo máximo es mayor (32MHz) así como su memoria para código (384 Kb de flash) y RAM (64Kb).

Por otro lado, para el control del lcd disponemos de un puerto paralelo hardware, lo cual nos va a permitir alcanzar velocidades sensiblemente mayores. En cuanto al resto de periféricos, cada uno cuenta con su propio puerto serie y además disponemos de seis canales de DMA, tres más que en el anterior.

(…) cambiar alguna cosa cuando este el micro nuevo

#### Interfaz de usuario

Aunque el esquema es similar (leds + buzzer + lcd con touchpad resistivo) tenemos ciertas diferencias respecto el otro prototipo.

El trio de led ha sido sustituido por un único led rgb, y el interruptor se ha cambiado por un pulsador conectado a una línea del wakeup del microcontrolador, lo que nos permitirá implementar un “apagado” por software y alguna otra funcionalidad básica, como puede ser apagar la luz de retroiluminación de la pantalla, de una manera similar al pulsador que tienen los Smartphone.

### Capa de abstracción hardware del segundo prototipo

En este caso, esta capa está basada en el código de inicialización generado por el programa STM32CubeMX, el cual permite configurar todos los periféricos del microcontrolador y proporciona funciones para el uso de los puertos serie (entre otras muchas cosas).

La funcionalidad que ofrece esta nueva capa es idéntica a la del primer prototipo, salvo que en este caso no bloquean la ejecución del programa principal, ya que utilizan las funciones que ofrece el código de inicialización diseñadas para este propósito, bien mediante el uso de interrupciones o acceso directo a memoria.

## Visión general del sistema

El funcionamiento de este servicio será diferente según se ejecute en el dispositivo de acceso o en el IMD, pero dado que ambas plataformas comparten la gran mayoría de la funcionalidad, se ha decidido diseñar un único sistema, el cual después incluirá o no ciertas partes según se trate del dispositivo de acceso o el simulador de marcapasos.

Debido a que este es un sistema de uso puntual, la mayor parte del tiempo se encontrara en estado de suspensión para reducir el consumo, lo cual es especialmente crítico en un hipotético IMD, donde la recarga de la batería es especialmente problemática.

Durante el acceso, el simulador de marcapasos entrará en modo escucha para poder ser detectado por el dispositivo de acceso, el cual establecerá una comunicación autenticada mediante un proceso que se detallará más adelante. Una vez el simulador de marcapasos nos haya concedido el acceso, el dispositivo ofrece una serie de opciones que simulan la manipulación de parámetros del marcapasos. Finalmente, el dispositivo cierra la conexión enviando un comando que “apaga” el modulo radio del simulador.

## Arquitectura Software del primer prototipo

El software se divide en una serie de niveles en los que podemos distinguir:

* Hardware Abstraction Layer (Hal): Implementada en el proyecto DER SAMUE, consiste en una serie de librerías que permiten la configuración y gestión de los periféricos del microcontrador, así como la configuración inicial del propio microcontrolador.
* Drivers: Son los módulos software que permiten configurar y utilizar los distintos módulos hardware, como puede ser el analog frontend, la pantalla o el medidor de batería.
* Midleware: Este módulo consiste en un sistema operativo de tiempo real(FreeRTOS) que se encarga de sincronizar los distintos módulos software.
* Aplicación:

## Diseño del software del primer prototipo

### Adquisición y tratamiento de la señal

#### Adquisición

#### Filtrado digital

##### Selección del tipo de filtros

#### Detección de ritmo cardiaco

##### Umbrales estáticos

##### Umbrales dinámicos

### Algoritmo de autenticación

#### Uso del ritmo cardiaco como contraseña dinámica

#### Estimación del umbral de validación

### Comunicación inalámbrica

#### Pila de protocolos

Como ya se ha dicho en el análisis del hardware, la tecnología para la comunicación es bluetooth clásico, en concreto la versión 4.1, para el cual Texas Instruments ofrece una pila de protocolos para bluetooth (Bluetopia).

Aprovechando esto, nuestro diseño se va a centrar en hacer los cambios necesarios para portar dicha pila a nuestro microcontrolador. Estos cambios están especificados en la documentación que incluida cuando te descargas la pila.

#### Gestión de la red por el master

#### Conexión segura

### Interfaz de usuario

#### Visualización de la señal ECG

#### Inicio de comunicación con un IMD

### Módulo de gestión de consumo

#### Apagado por software

#### Control de consumo de la pantalla

#### Apagado de elementos hardware

#### Gestión de consumo en RF

## Arquitectura Software del segundo prototipo

El software se divide en una serie de niveles en los que podemos distinguir:

* Hardware Abstraction Layer (Hal): Implementada en el proyecto DER SAMUE, consiste en una serie de librerías que permiten la configuración y gestión de los periféricos del microcontrador, así como la configuración inicial del propio microcontrolador.
* Drivers: Son los módulos software que permiten configurar y utilizar los distintos módulos hardware, como puede ser el analog frontend, la pantalla o el medidor de batería.
* Midleware: Este módulo consiste en un sistema operativo de tiempo real(FreeRTOS) que se encarga de sincronizar los distintos módulos software.
* Aplicación:

## Diseño del software del segundo prototipo

### Adquisición y tratamiento de la señal

En diseño de este módulo software

#### Filtrado digital

##### Selección del tipo de filtros

#### Detección de ritmo cardiaco

##### Umbrales estáticos

##### Umbrales dinámicos

### Algoritmo de autenticación

#### Uso del ritmo cardiaco como contraseña dinámica

#### Estimación del umbral de validación

### Comunicación inalámbrica

#### Pila de protocolos

Como ya se ha dicho en el análisis del hardware, la tecnología para la comunicación es bluetooth clásico, en concreto la versión 4.1, para el cual Texas Instruments ofrece una pila de protocolos para bluetooth (Bluetopia).

Aprovechando esto, nuestro diseño se va a centrar en hacer los cambios necesarios para portar dicha pila a nuestro microcontrolador, ya que esta se está diseñada para la serie L4. Estos cambios están especificados en la documentación que incluida cuando te descargas la pila.

#### Gestión de la red por el master

#### Conexión segura

### Interfaz de usuario

#### Visualización de la señal ECG

#### Inicio de comunicación con un IMD

### Módulo de gestión de consumo

#### Apagado por software

#### Control de consumo de la pantalla

#### Apagado de elementos hardware

#### Gestión de consumo en RF

# Implementación de los prototipos software

## Primera versión

### Implementación de las etapas de tratamiento de la señal

### Filtro paso banda FIR

### Diferenciador

### Elevar al cuadrado punto por punto

### Integrador

### Interfaz de usuario

#### Presentación de la señal ECG

#### Problemas encontrados

### Segunda versión (persimmon)

#### Filtrado digital

##### Optimización en los filtros

### Algoritmo de autentificación

#### Extracción de los bits de alta entropía

#### Calculo de distancia hamming y umbral de validación

#### Etapas de emparejamiento master-slave

#### Modo promiscuo

### Interfaz de usuario

#### Pantalla táctil

#### Menú

#### Indicador de batería

### RF

#### Pila de protocolos

#### Gestión de la red por el master

#### Conexión segura

### Gestión de consumo

#### Apagado por software

#### Control de consumo de la pantalla

#### Apagado de elementos hardware

#### Gestión de consumo en RF

# Pruebas y caracterización

## Pruebas con un generador de señal cardiaca

## Pruebas con un individuo real

## Respuesta del modo promiscuo

## Respuesta a un ataque

# Manual de uso

# Conclusiones y líneas futuras

## Seguridad

## Mejora sobre otros sistemas actuales

## Mejoras/Otros posibles usos

### Detección automática de segmentos del ECG

### Cálculo del eje eléctrico

### Ayuda al diagnóstico

### Detección de marcapasos

# Apéndices

# Referencias

[1] “Heart-to-Heart (H2H):Authentication for Implanted Medical Devices”

[2] “Signal Processing Methods for Heart Rate Variability”

[3] Compromising a Medical Mannequin