
# Sistema de intrusión y control de accesos

**Daniel Gómez García**
Grado de Tecnologías de la Telecomunicación
Sistemas Empotrados

**Consultor**
Jordi Becarés Ferrés

**Profesor responsable de la asignatura**
Pere Tuset Peiró

15 de Enero de 2017

## FICHA DEL TRABAJO FINAL

| | |
|---|---|
| **Título del trabajo:** | *Sistema de intrusión y control de accesos* |
| **Nombre del autor:** | *Daniel Gómez García* |
| **Nombre del consultor:** | *Jordi Bécares Ferrés* |
| **Nombre del PRA:** | *Pere Tuset Peiró* |
| **Fecha de entrega (mm/aaaa):** | *01/2017* |
| **Titulación o programa:** | *Grado de Tecnologías de la Telecomunicación* |
| **Área del Trabajo Final:** | *Sistemas Empotrados* |
| **Idioma del trebajo:** | *Castellano* |
| **Palabras clave** | *Wifly, Mifare, Alarma* |

**Resumen del Trabajo:**

En el contexto de la seguridad física en edificios e infraestructuras, los principales sistemas que se deben disponer para velar por la integridad de los espacios a supervisar son los sistemas de intrusión, sistemas de circuito cerrado de televisión y control de accesos.

Este proyecto surge de la voluntad de integrar en un mismo dispositivo las principales necesidades de la seguridad. Cuando ambos sistemas trabajan conjuntamente y se complementan se obtiene información adicional en cuanto al acceso de personas a la hora de investigar una posible intrusión.

La idea principal del proyecto se basa en el diseño e implementación de un sistema de intrusión con elementos básicos para poder simular el funcionamiento de un sistema de intrusión real. La central de intrusión diseñada dispone de entradas que indican la presencia ficticia de una intrusión y unas salidas o respuestas del sistema. Adicionalmente, cuando se produce una intromisión de personal no deseado, se envía un correo electrónico de aviso al responsable.

Paralelamente se ha dotado al sistema de intrusión de un lector mifare que permite el control de acceso mediante identificación por tarjeta. La central de intrusión y control de accesos comprueba en la base de datos si la tarjeta está aceptada, y facilita la conexión y desconexión del sistema y además permite la apertura de una puerta mediante un cerradero electrónico. Cuando se accede a la instalación mediante tarjeta mifare, también se envía un correo electrónico a la persona encargada de la instalación.

**Abstract:**

In the context of physical security in buildings and infrastructures, the main systems that must be available to ensure the integrity of the spaces to be supervised are intrusion systems, closed-circuit television systems and access control.

This project arises from the will to integrate in the same device the main needs of security. When both systems work together and complement each other, additional information is obtained regarding the access of people when investigating a possible intrusion.

The main idea of the project is based on the design and implementation of an intrusion system with basic elements to be able to simulate the operation of a real intrusion system. The designed intrusion control unit has inputs that indicate the fictitious presence of an intrusion and outputs or responses from the system. In addition, when an intrusion of unwanted personnel occurs, a warning email is sent to the responsible person.

At the same time, the intrusion system has been equipped with a mifare reader that allows access control through card identification. The intrusion control unit and access control checks in the database if the card is accepted, and facilitates the connection and disconnection of the system and also allows the opening of a door by means of an electronic lock. When accessing the installation via a mifare card, an email is also sent to the person in charge of the installation.

# Índice de contenidos

# Lista de figuras

# Lista de tablas

# 1. Introducción

La idea principal del proyecto se basa en el diseño e implementación de un sistema de intrusión con elementos básicos para poder simular el funcionamiento de un sistema de intrusión real. La central de intrusión diseñada dispone de entradas que indican la presencia ficticia de una intrusión y unas salidas o respuestas del sistema.

Como objetivo secundario se ha dotado al sistema de intrusión de un lector Mifare que permite el control de acceso mediante identificación por tarjeta. Este control de accesos facilita la conexión y desconexión del sistema de intrusión y además permite la apertura de una puerta mediante un cerradero electrónico.

## 1.1. Contexto y justificación del trabajo

En el contexto de la seguridad física en edificios e infraestructuras, los principales métodos que se utilizan para velar por la integridad de los espacios a supervisar son los sistemas de intrusión, sistemas de circuito cerrado de televisión (CCTV) y control de accesos (CCAA).

Este proyecto surge de la necesidad de integrar en un mismo dispositivo las principales necesidades de la seguridad en edificios e infraestructuras: intrusión y control de accesos. De esta manera se puede obtener información adicional para saber quién ha accedido a una estancia y controlar las intrusiones.

## 1.2. Descripción del trabajo

En cuanto a los elementos físicos o hardware del proyecto, se utilizan varios periféricos que, conectados a la controladora, nos permita procesar señales de entrada y de salida. Estos elementos serán:

- Detector volumétrico
- Contacto magnético
- Lector de tarjetas MIFARE
- Sirena acústica
- Foco disuasorio
- Cerradero eléctrico de puerta
- Elementos lumínicos visuales (LED’s)

El control de accesos está realizado mediante un lector de tarjetas MIFARE, a través del cual la centralita comprobará la identificación de la tarjeta en su base de datos para saber si debe permitir el acceso o armado/desarmado del sistema y permitiendo la apertura del cerradero de puerta.

El sistema tiene como señales de entrada un detector volumétrico y un contacto magnético, que se monitorizaran desde la central mediante la tensión recibida a los pines configurados para tal efecto en la placa LPC1769. Como respuesta a las entradas, el sistema tendrá una alarma y un foco disuasorio como salidas, accionados por la central en caso de intrusión.

Son tres los estados del sistema: armado, desarmado y alarma. En el modo armado, el sistema de intrusión se encuentra monitorizando las entradas para que, en caso de activación de alguna de ellas, se pase al estado de alarma. En el modo desarmado, el sistema no realiza monitorización de las entradas y por tanto no tiene actuaciones previstas. En el estado de alarma se activan las salidas de alarma y foco para notificar que se ha producido una intrusión. Además se envía un correo electrónico informando a la persona encargada del sistema de que se ha producido dicha intrusión.

## 1.3. Objetivos del TFG.

Para la realización del proyecto de sistema de intrusión y control de accesos se han especificado los siguientes objetivos básicos y secundarios:

**Objetivos básicos**

- Detectar la presencia de movimiento mediante detector volumétrico, lo que indicaría que una persona ha accedido a la instalación con el sistema armado
- Detectar apertura de puerta mediante contacto magnético, para saber si alguien ha abierto la puerta con el sistema conectado
- Dotar al sistema de un led de estado para notificar si el sistema está armado o desarmado
- Permitir el armado/desarmado del sistema mediante llavín
- Activar las salidas de sirena y foco disuasorio en caso de intrusión
- Enviar un e-mail de notificación en caso de intrusión para avisar al responsable

**Objetivos secundarios**

- Leer la codificación de una tarjeta mifare que se pase por el lector
- Permitir el acceso si la lectura de la tarjeta es aceptada
- Armar o desarmar el sistema mediante reconocimiento de tarjeta y lector Mifare
- Enviar un e-mail para informar de la identificación de la tarjeta que se ha pasado por el lector

## 1.4. Enfoque y método seguido.

Para llevar a cabo la realización de este proyecto, se ha requerido inicialmente de un proceso de documentación y aprendizaje sobre el hardware a utilizar: la placa LPC 1769, que es el principal elemento del proyecto; el módulo Wifly, que permite la conexión a internet del sistema; y el módulo CP2102, que permite realizar un log para ver por pantalla información proporcionada por el sistema.

También ha sido imprescindible alcanzar unos conocimientos básicos de software y configuración para utilizar los tres elementos descritos anteriormente, así como para utilizar el "Integrated Development Environment" (IDE), que es el aplicativo que permite implementar el código para hacer funcionar los diferentes dispositivos.

Adicionalmente se ha realizado una división y planificación de tareas del proyecto para llevar un control y supervisión con el objetivo de cumplir con los plazos principales de entregas establecidos.

## 1.5. Planificación del trabajo.

Como principal pauta para la realización de todo el proyecto como conjunto, se ha dividido en diferentes fases y tareas el trabajo a realizar coincidiendo con las fechas de entrega parciales durante el semestre. Con la ayuda de los objetivos básicos y secundarios expuestos en la propuesta inicial del proyecto, se han definido una serie de tareas y subtareas a completar para alcanzar dichos objetivos.

Se ha indicado una temporización estimada para cada tarea con la verificación y ayuda del consultor y una vez distribuida la carga de trabajo y los recursos disponibles, se han asignado unas determinadas tareas a cada fase de entrega indicada en el calendario de la asignatura.

Para cada fase de entrega realizada se ha valorado y modificado la planificación inicial según la situación real del momento, haciendo constar los problemas que han podido surgir durante el transcurso del tiempo previsto y los riesgos y acciones a realizar en futuras entregas para alcanzar con éxito la entrega final de proyecto.

Las fases en las que se divide el proyecto según las entregas parciales, y las tareas asignadas se describen en la siguiente tabla:

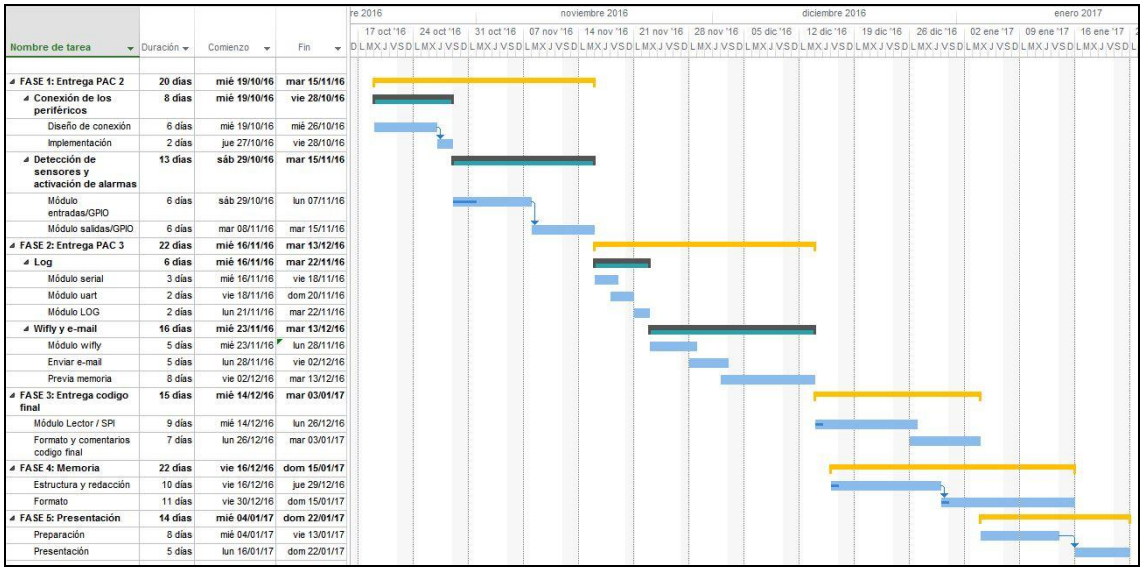
| | |
|---|---|
| FASE 1 | Conexión de periféricos |
| | Diseño conexión |
| | Implementación |
| | Detección de sensores y activación de alarmas |
| | Módulo GPIO |
| FASE 2 | Implementación del LOG |
| | Módulo Serial |
| | Módulo UART |
| | Módulo LOG |
| | Wifly y e-mail |
| | Módulo wifly |
| | Enviar e-mail |
| | Previa memoria |
| FASE 3 | Objetivos secundarios |
| | Módulo Mifare |
| | Módulo alarmas |
| FASE 4 | Memoria |
| | Estructura y redacción |
| | Formato |
| FASE 5 | Presentación |
| | Preparación |
| | Presentación |

**Tabla 1:** Fases y tareas del proyecto

Tal y como se puede observar en las figuras 1 y 2, inicialmente se realizó una planificación irreal en cuanto al tiempo necesario para resolver algunas de las tareas, como por ejemplo para la realización del LOG, con los 3 módulos LOG, serial y UART. Esto condicionó a las siguientes tareas y sobre todo a la realización de las Fases 4 y 5, reduciendo el tiempo disponible considerablemente en 9 días para la memoria y 7 para la presentación.

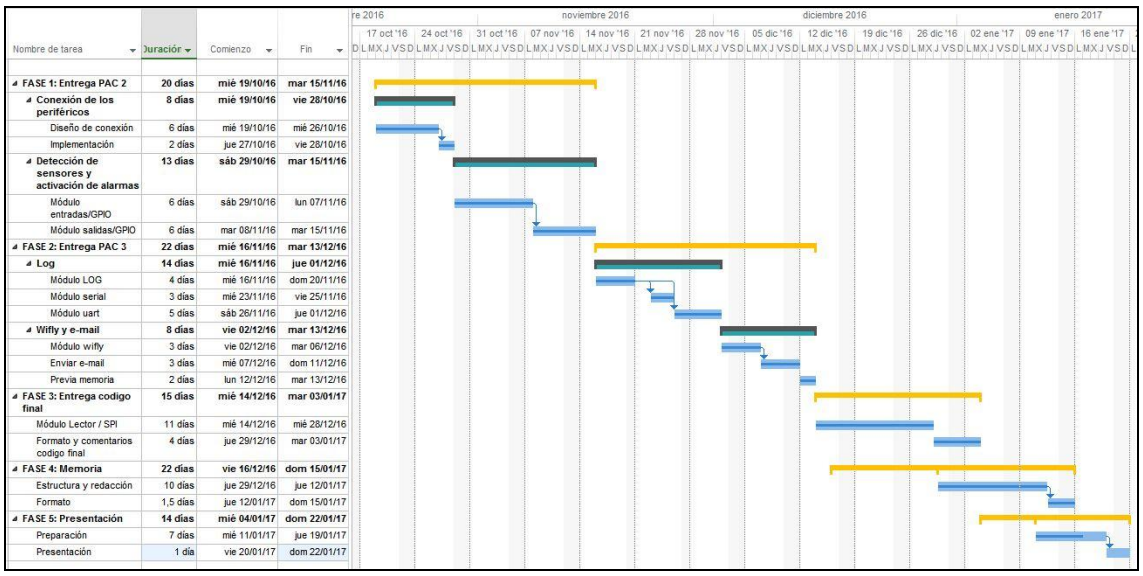
En general se han cumplido los plazos para las entregas excepto en la fase 2, en la que se entregó sin que llegara a funcionar el envío de correo electrónico mediante wifly y con una entrega previa de la memoria poco trabajada. La fase 3 se entregó a tiempo con todas las tareas realizadas, a pesar de que se hubiera podido mejorar la arquitectura del código creando un módulo e-mail independiente de wifly. Para las fases 4 y 5 se estima que se realizarán dentro del margen de tiempo previsto.

En las siguientes figuras se indica la planificación temporal inicial y final de las tareas englobadas dentro de las fases, estas últimas con fecha de finalización conocida e inamovible:



| Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|
| **FASE 1: Entrega PAC 2** | **20 días** | **mié 19/10/16** | **mar 15/11/16** |
| **Conexión de los periféricos** | **8 días** | **mié 19/10/16** | **vie 28/10/16** |
| Diseño de conexión | 6 días | mié 19/10/16 | mié 26/10/16 |
| Implementación | 2 días | jue 27/10/16 | vie 28/10/16 |
| **Detección de sensores y activación de alarmas** | **13 días** | **sáb 29/10/16** | **mar 15/11/16** |
| Módulo entradas/GPIO | 6 días | sáb 29/10/16 | lun 07/11/16 |
| Módulo salidas/GPIO | 6 días | mar 08/11/16 | mar 15/11/16 |
| **FASE 2: Entrega PAC 3** | **22 días** | **mié 16/11/16** | **mar 13/12/16** |
| **Log** | **6 días** | **mié 16/11/16** | **mar 22/11/16** |
| Módulo serial | 3 días | mié 16/11/16 | vie 18/11/16 |
| Módulo uart | 2 días | vie 18/11/16 | dom 20/11/16 |
| Módulo LOG | 2 días | lun 21/11/16 | mar 22/11/16 |
| **Wifly y e-mail** | **16 días** | **mié 23/11/16** | **mar 13/12/16** |
| Módulo wifly | 5 días | mié 23/11/16 | lun 28/11/16 |
| Enviar e-mail | 5 días | lun 28/11/16 | vie 02/12/16 |
| Previa memoria | 8 días | vie 02/12/16 | mar 13/12/16 |
| **FASE 3: Entrega codigo final** | **15 días** | **mié 14/12/16** | **mar 03/01/17** |
| Módulo Lector / SPI | 9 días | mié 14/12/16 | lun 26/12/16 |
| Formato y comentarios codigo final | 7 días | lun 26/12/16 | mar 03/01/17 |
| **FASE 4: Memoria** | **22 días** | **vie 16/12/16** | **dom 15/01/17** |
| Estructura y redacción | 10 días | vie 16/12/16 | jue 29/12/16 |
| Formato | 11 días | vie 30/12/16 | dom 15/01/17 |
| **FASE 5: Presentación** | **14 días** | **mié 04/01/17** | **dom 22/01/17** |
| Preparación | 8 días | mié 04/01/17 | vie 13/01/17 |
| Presentación | 5 días | lun 16/01/17 | dom 22/01/17 |

**Figura 1:** Planificación inicial del proyecto



| Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|
| **FASE 1: Entrega PAC 2** | **20 días** | **mié 19/10/16** | **mar 15/11/16** |
| **Conexión de los periféricos** | **8 días** | **mié 19/10/16** | **vie 28/10/16** |
| Diseño de conexión | 6 días | mié 19/10/16 | mié 26/10/16 |
| Implementación | 2 días | jue 27/10/16 | vie 28/10/16 |
| **Detección de sensores y activación de alarmas** | **13 días** | **sáb 29/10/16** | **mar 15/11/16** |
| Módulo entradas/GPIO | 6 días | sáb 29/10/16 | lun 07/11/16 |
| Módulo salidas/GPIO | 6 días | mar 08/11/16 | mar 15/11/16 |
| **FASE 2: Entrega PAC 3** | **22 días** | **mié 16/11/16** | **mar 13/12/16** |
| **Log** | **14 días** | **mié 16/11/16** | **jue 01/12/16** |
| Módulo LOG | 4 días | mié 16/11/16 | dom 20/11/16 |
| Módulo serial | 3 días | mié 23/11/16 | vie 25/11/16 |
| Módulo uart | 5 días | sáb 26/11/16 | jue 01/12/16 |
| **Wifly y e-mail** | **8 días** | **vie 02/12/16** | **mar 13/12/16** |
| Módulo wifly | 3 días | vie 02/12/16 | mar 06/12/16 |
| Enviar e-mail | 3 días | mié 07/12/16 | dom 11/12/16 |
| Previa memoria | 2 días | lun 12/12/16 | mar 13/12/16 |
| **FASE 3: Entrega codigo final** | **15 días** | **mié 14/12/16** | **mar 03/01/17** |
| Módulo Lector / SPI | 11 días | mié 14/12/16 | mié 28/12/16 |
| Formato y comentarios codigo final | 4 días | jue 29/12/16 | mar 03/01/17 |
| **FASE 4: Memoria** | **22 días** | **vie 16/12/16** | **dom 15/01/17** |
| Estructura y redacción | 10 días | jue 29/12/16 | jue 12/01/17 |
| Formato | 1,5 días | jue 12/01/17 | dom 15/01/17 |
| **FASE 5: Presentación** | **14 días** | **mié 04/01/17** | **dom 22/01/17** |
| Preparación | 7 días | mié 11/01/17 | jue 19/01/17 |
| Presentación | 1 día | vie 20/01/17 | dom 22/01/17 |

**Figura 2:** Planificación final del proyecto

## 1.6. Recursos empleados

Se ha requerido tener conocimientos en el lenguaje de programación C que es compatible con el IDE de LPCXpresso y con la placa LPC1769, además de el estudio de las principales funcionalidades de FreeRTOS en cuanto a tareas, semáforos y en general en todo lo que respecta a la ejecución de tareas.

Se ha utilizado el material suministrado por la UOC para la asignatura (Figura 3):

- placa LPC1769 con microcontrolador ARM Cortex-M3 de NXP

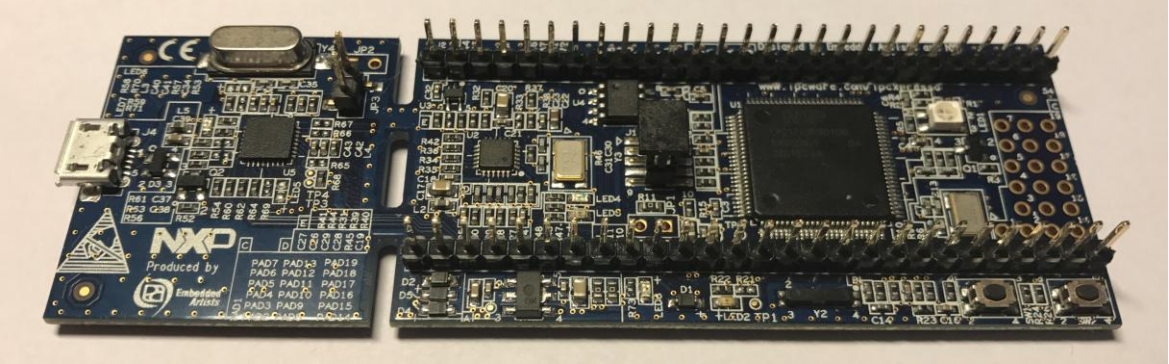



**Figura 3:** LPC1769

- CP2102 convertidor USB a UART

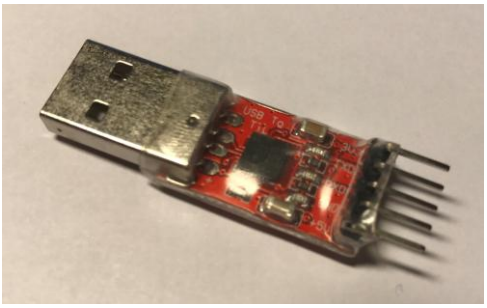


**Figura 4:** CP2102 Convertidor USB-UART

- módulo wifly RN-XV conectividad Wi-Fi 802.11b/g

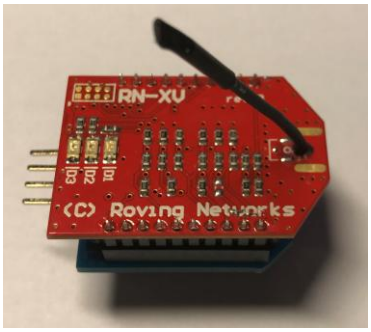



**Figura 5:** Dispositivo Wifly

Los periféricos usados para el funcionamiento del sistema se muestran en las siguientes figuras:

- Detector volumétrico

**Figura 6:** Detector Volumétrico

- Contacto magnético

**Figura 7:** Contacto magnético

- Lector de tarjetas MIFARE

**Figura 8:** Lector MIFARE

- Tarjetas MIFARE

**Figura 9:** Tarjetas MIFARE

- Sirena acústica (zumbador)

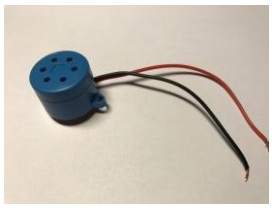


**Figura 10:** Zumbador

- Foco disuasorio (LED)

**Figura 11:** Diodo LED

- Cerradero de puerta

**Figura 12:** Cerradero electrónico

- Llavín

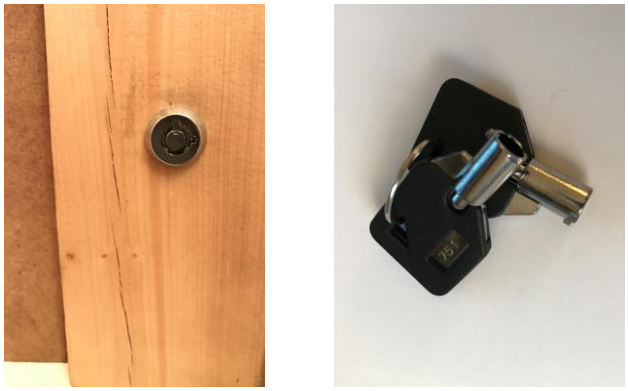


**Figura 13:** Llavín

- Puerta en miniatura para implementar los diferentes elementos

**Figura 14:** Prototipo de puerta

Como fuente de alimentación de 12V y protoboard se ha utilizado la placa proporcionada por la UOC para la asignatura Tecnología Electrónica del Grado Tecnologías de Telecomunicación (Figura 5):

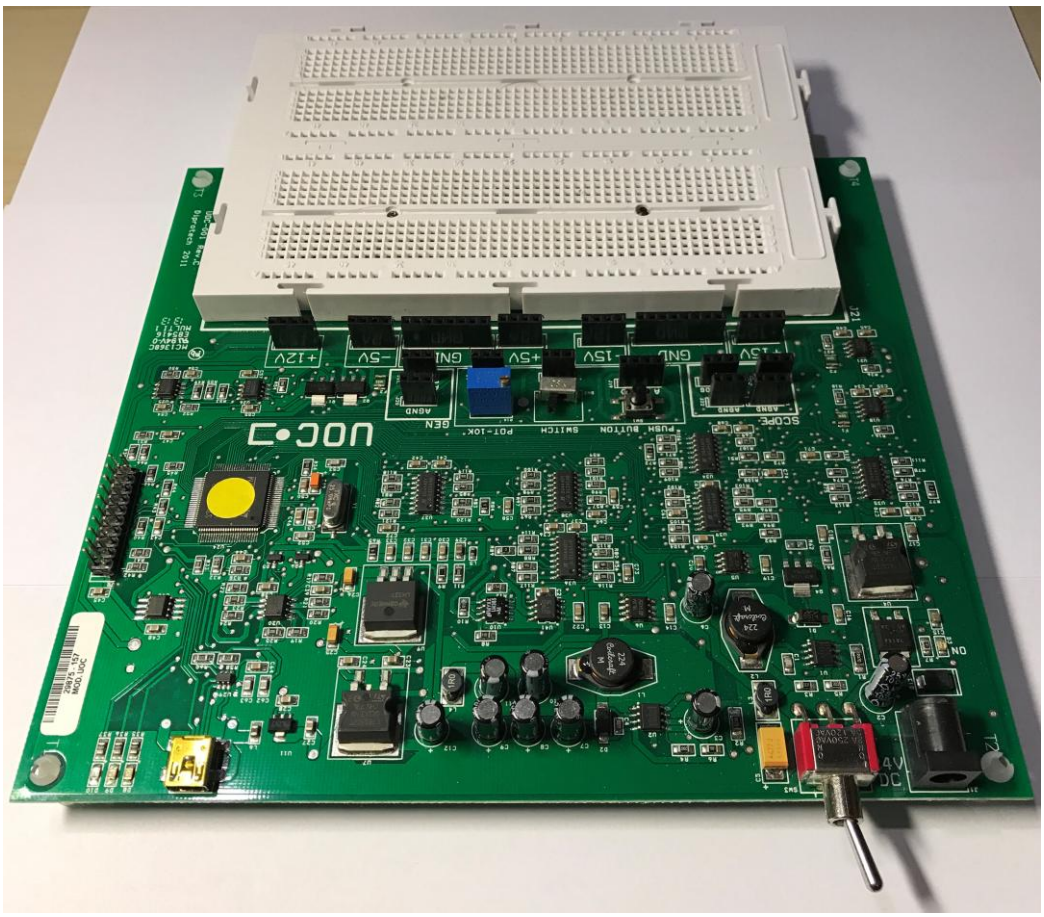


**Figura 15:** Fuente de alimentación y protoboard

## 1.7. Productos obtenidos

El prototipo obtenido para el desarrollo del proyecto consiste en la simulación a pequeña escala de un sistema de intrusión y control de accesos real, tal y como se ha indicado en apartados anteriores.

Para ello el principal elemento es la placa LPC1769 y los periféricos indicados en el apartado anterior. Con el objetivo de que la simulación sea lo más real posible, se han dispuesto los elementos externos a la placa en una puerta a escala, con la misma operativa que tendrían en un acceso o instalación real.

En la siguiente figura se muestra el prototipo de simulación creado a tal efecto. Se puede observar la puerta por la parte exterior de la estancia con el lector MIFARE y el llavín de armado desarmado:

**Figura 16:** Prototipo de sistema de intrusión y control de accesos (parte exterior)

En la siguiente figura se muestra el prototipo por la parte interior, donde se puede observar el detector volumétrico, el contacto magnético empotrado en la puerta y marco y el cerradero electrónico:

**Figura 17:** Prototipo de sistema de intrusión y control de accesos (parte interior)

De esta manera, la funcionalidad del sistema se acerca al uso para el que ha sido diseñado, pudiendo asimilar y visualizar de una manera más fácil el diseño final del sistema.

En la siguiente figura se muestra el prototipo del sistema junto a la central de intrusión:

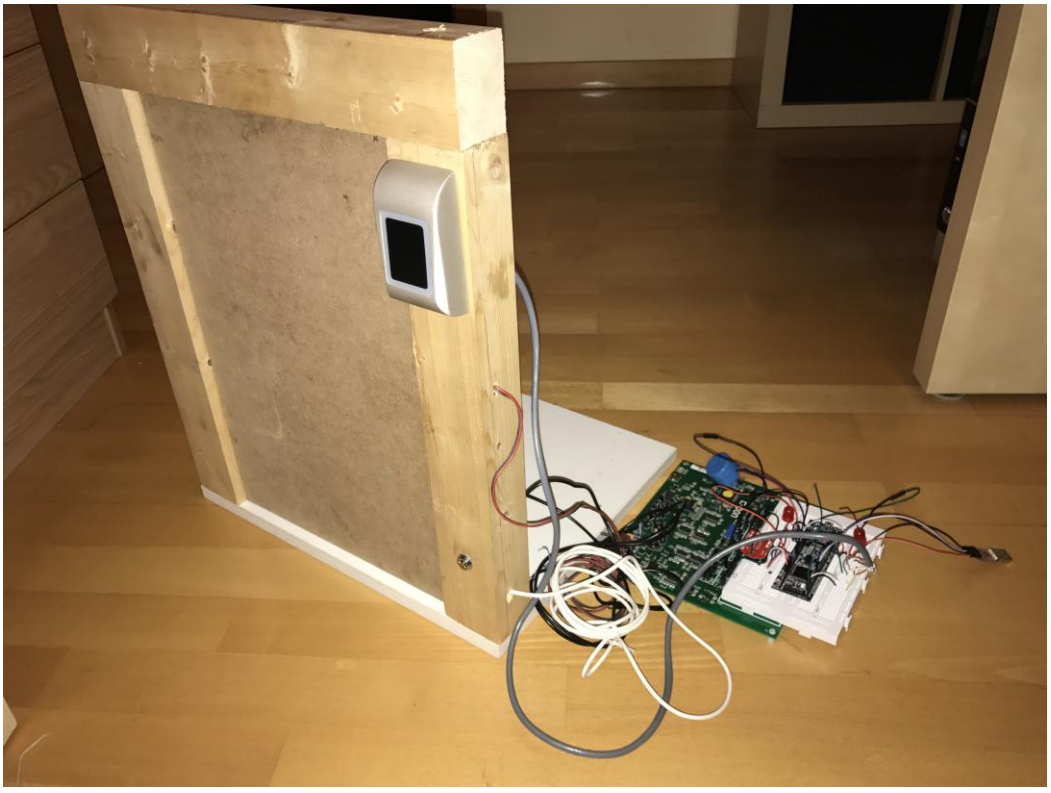


**Figura 18:** Prototipo de sistema de intrusión y control de accesos

## 1.8. Breve descripción de los otros capítulos de la memoria.

En el siguiente capítulo se indican los antecedentes y se analizan los diferentes tipos de tecnologías disponibles en el mercado para la realización del proyecto diseñado.

En el capítulo 3 se muestra la funcionalidad específica del sistema, como se ha diseñado la funcionalidad de los periféricos para su interacción con la central junto con su diagrama, y cómo se realiza la comunicación con wifly y la lectura de tarjetas mediante lector MIFARE. Seguidamente se muestra el diagrama del diseño de la aplicación que controlará el sistema.

En el capítulo 4 se realiza una explicación detallada y técnica del diseño de la aplicación, sus librerías y sus módulos y el esquema de conexionado.

En el capítulo 5 se realiza un pequeño manual de usuario para explicar cómo se debe interactuar con el sistema.

En el capítulo 6 se realiza un estudio de la viabilidad técnica del producto obtenido.

En el capítulo 7 se expone la valoración económica del producto y se estudia cuáles deberían ser los precios de venta del producto para que sea rentable y asequible para un posible cliente.

# 2. Antecedentes

Un sistema empotrado o embebido, es un dispositivo electrónico diseñado para cubrir unas necesidades de actuación o control sobre otros elementos, con el objetivo de obtener un producto que sea capaz de funcionar de una manera lógica en respuesta a unos acontecimientos determinados.

La lógica del sistema empotrado viene dada por la programación del mismo en consonancia con las funcionalidades que se deseen obtener. Señales de entrada provenientes de sensores provocan respuestas requeridas o esperadas para un determinado diseño. La mayoría de aparatos electrónicos que existen en los hogares necesitan un sistema empotrado o micro controlador para funcionar. También son utilizados para la industria y manejo de maquinaria, procesamiento de datos, etc.

El principal componente de un sistema empotrado es la CPU, que es la encargada de procesar y controlar cada una de las tareas que tiene asignadas, como por ejemplo la monitorización de periféricos o sensores de que disponga el sistema.

## 2.1. Estado del arte

Actualmente existen en el mercado una amplia variedad de dispositivos destinados al desarrollo de un sistema empotrado. Los más utilizados en cuanto a desarrollo a nivel de aprendizaje son Beagle Bone, Raspberry Pi y Arduino.

En este apartado compararemos las principales características de uno de los modelos de cada marca de micro controladores, con el utilizado en la realización de este proyecto, que es la placa LPC1769 de NXP Semiconductors.

**Figura 19:** Beagle Bone Black

Beagle Bone Black

Dispone de una gran compatibilidad con la gran mayoría de elementos diseñados para micro controladores y sistemas operativos como Debian, Android y Ubuntu. Tiene un procesador ARM Cortex-A8 AM3358 de 1GHz, 4GB 8-bit eMMC de memoria flash, 512 MB DDR3 RAM. Dispone de conexión USB, Ethernet, HDMI y 2x46 pins.

Raspberry Pi 3 Model B

Tiene una CPU ARMv8 quad-core de 64 bits a 1,2 GHz, 1GB de LPDDR2 RAM, 40 GPIO Pins, 4 puertos USB, Interfície de cámara (CSI), Interfaz de display (DSI), HDMI port, ranura para SD.

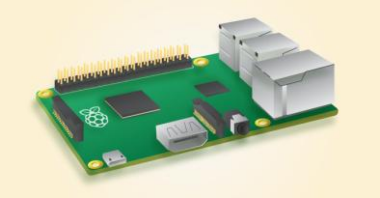


***Figura 20:*** *Raspberry Pi 2 Model B*

**Figura 21:** Arduino Mega 2560

Arduino Mega 2560

Es una de la marcas de micro controladores de 8-bit más conocidas. Tiene un procesador de AVR ATMEGA2560 a 16MHz, 256k de memoria flash y dispone de 54 GPIO, 4 puertos UART.

LPC1769

ARM Cortex-M3 100 MHz de 32 bits, con 64 KB de SRAM, 512KB de memoria flash. Como interfaces tiene 4 puertos UART, 3 I2C, 2 SSP, 2 CAN, USB 2.0, Ethernet.

A continuación se analizan estos datos en una tabla comparativa:

| | Beagle Bone Black | Raspberry Pi 3 Model B | Arduino Mega 2560 | LPC1769 |
|---|---|---|---|---|
| **Procesador** | ARM Cortex-A8 1GHz | ARMv8 64b 1,2GHz | AVR ATMEGA2560 16MHz | ARM Cortex-M3 100MHz |
| **Flash** | 4GB | 1GB | 256 KB | 512 KB |
| **RAM** | 512 MB | SD | 8 KB | 64 KB |
| **Interfaces** | USB<br>Ethernet<br>HDMI<br>2x46 pins | 40 GPIO pins<br>4 puertos USB<br>Cámara (CSI)<br>Display (DSI)<br>HDMI | 54 GPIO pins<br>4 puertos UART | 52 GPIO pins<br>4 puertos UART<br>3 I2C<br>2 SSP<br>2 CAN<br>USB 2.0<br>Ethernet |

**Tabla 2:** Comparativa micro controladores

Si se analizan los datos de las dos primeras columnas, se puede observar que son controladores con una capacidad de procesado mucho mayor que las otras dos, además de tener unas interfaces de salida de vídeo que en nuestro caso, para el proyecto que nos ocupa, no son necesarias.

Entre el micro controlador Arduino Mega 2560 y LPC1769, este último dispone de una memoria flash y RAM superior, así como la velocidad del procesador, que también es mayor. En cuanto

a nivel de programación, la placa Arduino utiliza para su utilización un lenguaje de alto nivel propio. Por el contrario, con la placa de NXP Semiconductors el lenguaje de programación utilizado está basado en el lenguaje C.

Por los motivos indicados en este apartado, se considera que la placa LPC1769 suministrada en la asignatura es apropiada para la realización del presente proyecto.

## 2.2. Estudio de mercado

El producto que se desarrolla en este documento existe actualmente en el mercado y además de manera muy extensa y experimentada. Obviamente existen productos mucho más avanzados y con muchas más funcionalidades que facilitan sustancialmente la complicada tarea de velar por la seguridad de un emplazamiento de forma remota.

Honeywell, por ejemplo, es uno de los fabricantes más conocidos con productos para la seguridad como centrales de incendio, intrusión, control de accesos, video vigilancia, etc. Además de ofrecer estos productos independientemente, el avance en las tecnologías para la seguridad viene dada por la integridad de todos los productos en uno solo, con el consecuente ahorro en mantenimiento con diferentes fabricantes, facilidad de manejo con un único software de gestión y sobre todo la gestión de los datos en una misma base de datos que permite contrastar de manera rápida y eficaz la información disponible ante una intrusión.

El modelo que se muestra en la siguiente figura de Honeywell que implemente un sistema de intrusión y control de accesos en un mismo producto:

**Figura 22:** Sistema de intrusión y control de accesos de Honeywell

Por el contrario también existen productos que o bien están indicados únicamente para la detección de intrusiones, o bien para control de accesos. En el campo de la seguridad física la tecnología a utilizar depende no solamente de los productos disponibles en el mercado, sino de la inversión que se desee realizar en ella.

El sistema básico planteado en este proyecto presenta la ventaja de que además de funcionar como sistema estático de intrusión, también es capaz de enviar información sobre lo que ha ocurrido durante una intrusión y además actúa como sistema de control de accesos. Es decir, es capaz de detectar una intrusión y generar una salida para que el posible intruso o personal de las inmediaciones se percate de que se está produciendo una alarma, pero también envía información a la persona responsable para que pueda gestionar la seguridad de la instalación a proteger.

# 3. Descripción funcional

En el tercer capítulo de este Trabajo Final de Grado se entra en detalle en el diseño del sistema planteado y se describe la funcionalidad del mismo.

## 3.1. Sistema de intrusión y control de accesos

Tal y como se ha indicado anteriormente, el sistema que se estudia y se pone en práctica en este proyecto es la realización de un sistema de intrusión y control de accesos. Este sistema tiene las funcionalidades básicas de un sistema de intrusión, que son: detección de intrusión, respuesta ante una intrusión y envío de información para su gestión.

En lo que a control de accesos se refiere, el sistema determina si la persona poseedora de una tarjeta de identificación tiene permitido el acceso o por el contrario no se le debe dar acceso. Además de permitir o no el acceso, cuando una tarjeta es leída por el sistema, es capaz de enviar información acerca de la identificación de la tarjeta y de esta manera controlar quién ha accedido.

En la Figura 10 se muestra gráficamente el funcionamiento del sistema diseñado. Cuando la estancia detecta que se produce una intrusión, activa sus respuestas locales ante este acontecimiento, y además informa a su propietario a través de la red mediante un e-mail. De igual modo, cuando se produce un acceso mediante tarjeta, se informa a través de la red.

**Figura 23:** Gráfico ilustrativo de funcionamiento del sistema

### 3.1.1 Diagrama general de los periféricos del sistema

En la Figura 11 se muestra el diagrama general de los periféricos del sistema, donde se indican los diferentes elementos que interactúan con la central de intrusión y control de accesos, el funcionamiento básico de los cuales ya han sido introducidos en apartados anteriores:

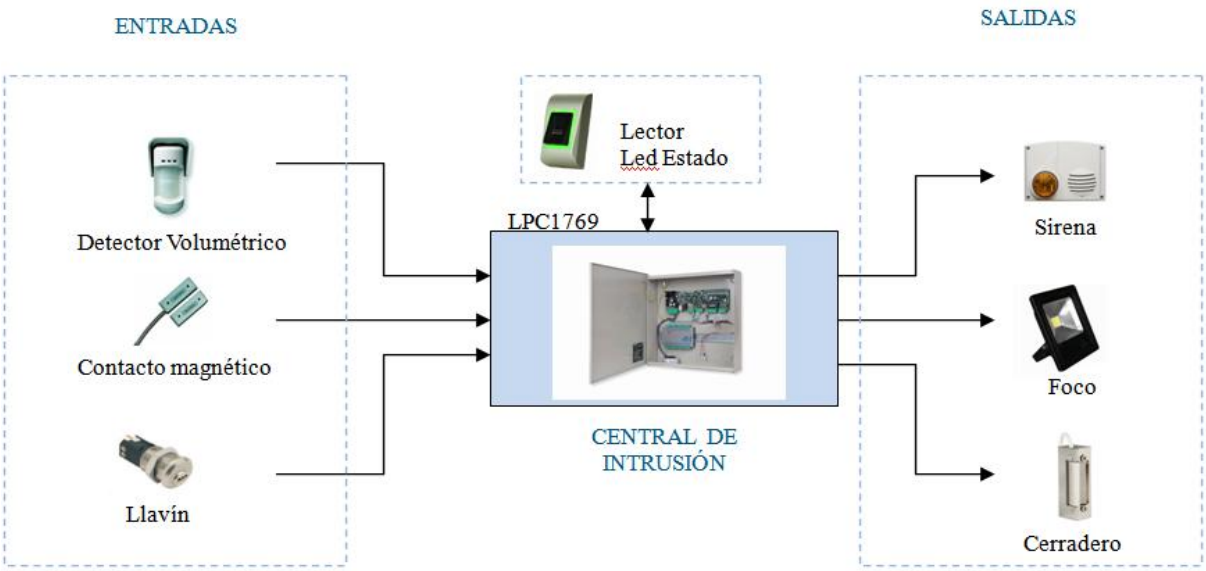



**Figura 24:** Diagrama general de los periféricos del sistema

### 3.1.2 Diagrama de la central de intrusión

La central de intrusión es la parte principal de todo el sistema, ya que es la parte que recibe las entradas, decide qué hacer en función de su estado, y como actuar en cada caso. Está formada por el micro controlador LPC1769, donde se conectan los periféricos a sus pines GPIO y además, para permitir la comunicación con el servidor de correo que posteriormente enviará las notificaciones, se conecta el módulo wifly RN-XV indicado en el apartado 1.6.

El módulo wifly se comunica con la placa LPC1769 mediante uno de los puertos UART. A través de la información que se le pasa desde la aplicación diseñada, el módulo wifly se conecta a la red mediante conexión inalámbrica. Una vez conectado, el módulo estará a la espera de que se le de instrucción de abrir conexión a través de TCP con el servidor SMTP y de esta manera poder enviar el correo electrónico con la notificación correspondiente.

Por otra parte, la central de intrusión también está dotada de un sistema de LOG que permite al mantenedor de la aplicación o incluso al propietario, disponer de un registro de acontecimientos sucedidos mientras el sistema está en funcionamiento. Esta información se transmite a través de la pantalla de un PC mediante USB gracias al convertidor CP2102 de USB a UART y viceversa. Este convertidor permite que a través del módulo log creado en la aplicación y a

través de un aplicativo que permita la comunicación por puerto COM (como Putty por ejemplo para Windows), se pueda visualizar los mensajes que desde la aplicación se envíen a través del puerto UART de la placa.

En la siguiente Figura se muestran los elementos de que está compuesta la central de intrusión:

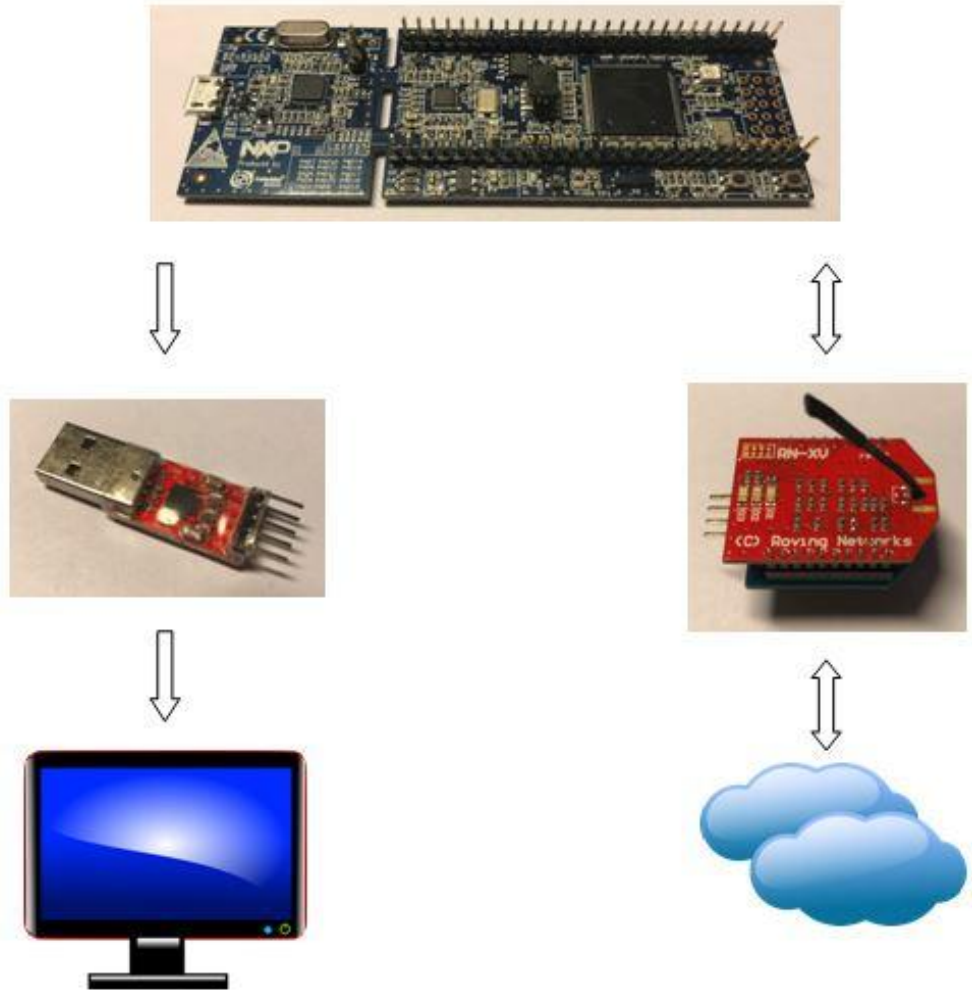



**Figura 25:** Diagrama de funcionamiento de la central de intrusión

### 3.1.3 Diagrama de bloques funcional del sistema

Para entender el funcionamiento general del sistema, cómo interactuar con los diferentes elementos y los procedimientos a seguir para su utilización, se ha realizado el siguiente diagrama de bloques mostrado en la Figura 12. Tal y como se muestra en dicha figura, son 3 los estados del sistema:

- MODO DESARMADO: Para cambiar al modo armado, se realiza un pase de tarjeta por el lector, o mediante el llavín. Cualquier acción realizada mediante el pase de tarjeta se envía un e-mail indicando el ID de la persona que ha realizado la acción.

- MODO ARMADO: Para cambiar de modo armado a modo desarmado, se realizan un pase de tarjeta por el lector, o mediante el llavín. Estando en modo armado, si se produce detección en el Detector Volumétrico o en el Contacto Magnético, se pasa automáticamente al MODO ALARMA.

- MODO ALARMA: Se envía un e-mail indicando el elemento de entrada que se ha activado. Para desactivar el modo alarma y pasar al modo desarmado, se realiza mediante un pase de tarjeta por el lector o mediante el llavín.

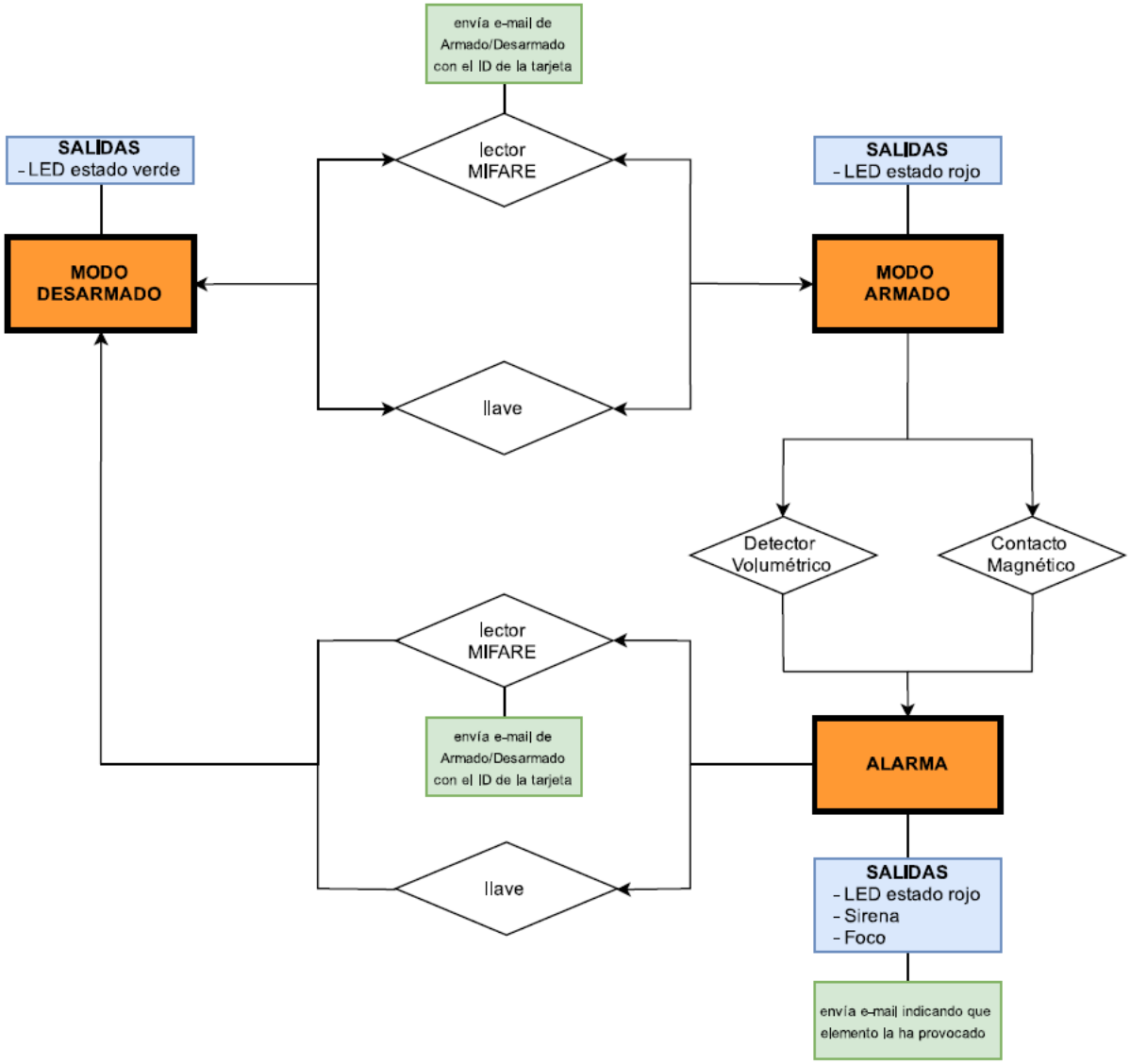



**Figura 26:** Diagrama de bloques funcional del sistema

### 3.1.4 Comunicación a través de la red: Wifly

El módulo Wifly es un dispositivo que incluye un procesador de 32 bit con conexión inalámbrica bajo el estándar 802.11b/g y permite comunicar mediante diferentes tipos de protocolos configurables mediante comandos enviados a través de una consola de comandos como putty. En este caso utilizaremos la configuración para realizar una conexión TCP a un socket del servidor de correo. También se pueden realizar conexiones http, para enviar peticiones a un servidor para requerir datos o para enviar datos y que queden registrados en un gráfico, tal y como se hizo en la PAC correspondiente al dispositivo wifly.

La comunicación de la central de intrusión con el servidor SMTP para el envío de correo electrónico se realiza a través del dispositivo wifly mediante una conexión TCP a un socket del servidor. Inicialmente el wifly debe estar conectado a la red a través de una conexión inalámbrica con un SSID. En el módulo wifly de la librería LibUOC existen los métodos para dicha conexión, para la configuración de la comunicación mediante protocolo SMTP, y para abrir la conexión cada vez que se desee enviar un correo.

Una vez establecida la conexión con el servidor de correo, mediante el método que se utiliza para enviar el e-mail, se le pasan los comandos necesarios para la autenticación, el asunto del correo en función de si lo que se envía es una alarma o un acceso, el destinatario y el cuerpo del mensaje.

A través del dispositivo de comunicación wifly también leemos las respuestas que nos da el servidor a nuestras peticiones, pasando a través del LOG algunas de las respuestas para comprobar que realmente se ha enviado el correo electrónico.

### 3.1.5 Tecnología MIFARE

La tecnología MIFARE se usa en tarjetas de memoria para la lectura sin contacto a través de un lector. Utiliza un protocolo de alto nivel y distancias de lectura de unos 10 cm entre tarjeta y lector y que funciona a una frecuencia de 13,56 MHz.

Cada tarjeta está dividida en sectores, y cada sector se divide en 4 bloques. 3 de ellos pueden contener información del identificador de la tarjeta llamado Card Serial Number (en adelante CSN) o Unique IDentifier (en adelante UID) y contiene mecanismos simples de seguridad. Estos sectores usan claves de acceso llamadas A y B que se almacenan en un cuarto bloque junto a los permisos de acceso para lectura, escritura, descuento o incremento a cada uno de los restantes 3 bloques.

En el momento que se posiciona la tarjeta delante de un lector, recibe alimentación por parte del mismo y se comienza a realizar una comunicación cifrada para proteger la escucha del canal.

Una vez se ha establecido el canal cifrado, el código de identificación de conexión es enviado por la tarjeta y con este número el lector puede acceder a los diferentes sectores de la tarjeta para realizar las acciones para las que tenga permiso: lectura, escritura, descuento o incremento.

### 3.1.6 Protocolo Wiegand y Lector MIFARE

Para el sistema de control de accesos mediante tarjetas MIFARE se requiere de un dispositivo que sea capaz de leer la codificación interna de las tarjetas y que comunique con la central de intrusión y control de accesos. Para este objetivo se ha seleccionado un lector MIFARE que utiliza el protocolo Wiegand, explicado a continuación.

El protocolo Wiegand utiliza la numeración que el lector obtiene de la tarjeta y la envía a través de dos conexiones cableadas que entregan 5 o 0V. Estas conexiones se llaman D0, que transmite la información de los bits ‘0’, y D1, que transmite los bits ‘1’. Por defecto, cuando el lector está en reposo, es decir, sin que lea una tarjeta, siempre entrega un 1 lógico (5V) tanto por el cable D0 como por el cable D1. Cuando se tiene que transmitir un bit ‘0’, la tensión que entrega el lector por el cableado D0 baja a 0V durante 200 micro segundos. Cuando se desea transmitir un ‘1’, realiza el mismo procedimiento con la conexión D1, baja el voltaje a 0V durante 200 microsegundos.

De esta manera, mediante interrupciones creadas en la placa LPC1769 configuradas para detectar los flancos decrecientes en el cableado procedente del lector para D0 y D1, se puede obtener la codificación que el dispositivo transmite de la lectura de una tarjeta.

El protocolo de comunicación Wiegand dispone de diversas modalidades que consisten en el número de bits que se envían al leer una tarjeta, incluyendo bits de paridad, bits de identificación del dispositivo de lectura. En este trabajo se ha optado por la codificación wiegand 26, que lee la codificación de la tarjeta y la envía en 26 bits sin tener en cuenta la codificación del lector.

El modelo de lector utilizado es un MTPX-MF del fabricante XPR. Se ha escogido este modelo debido a que además de proporcionar la posibilidad de selección de varios tipos de transmisión de bits, dispone de una franja que se ilumina mediante led en colores verde, rojo y naranja. Las conexiones disponibles del lector son la alimentación a 12V, led verde, led rojo, D0 y D1. Dichas conexiones se pueden observar en la siguiente figura:

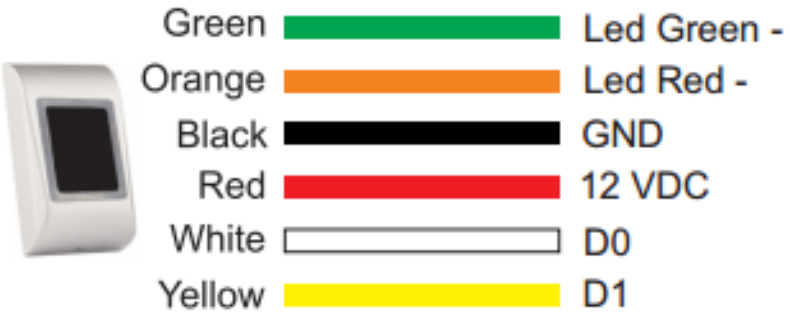



**Figura 27:** Conexiones del lector

Para que se encienda el led verde, es necesario conectar a GND el cable verde indicado en la figura anterior. Para encender el led rojo, será el cable naranja el que se deberá conectar a GND. Si se conecta tanto el cable verde como el naranja a GND, el led quedará de color naranja.

El lector dispone de 6 dips interruptores que, como se ha dicho anteriormente, permite la selección de la variante del protocolo wiegand que se desea utilizar mediante 3 de esos dips. El primer dip se utiliza para activar o desactivar el led. El segundo habilita o inhabilita el sonido al pasar una tarjeta, y el tercero sirve para la conversión del UID de tarjetas de 7 bytes a 4.


**Figura 28:** Dips interruptores del lector

En el caso que aplica a este proyecto, se ponen los dips 1, 2 y 3 en ON para poder disponer de estas funciones, y los dips 4, 5, y 6 a OFF, para usar el protocolo Wiegand 26 de entre los disponibles en la siguiente tabla:

| Jumper | | W 26bit | W 34bit | W 42bit | W 58bit | W 24bit | W 32bit | W 40bit | W 56bit |
|---|---|---|---|---|---|---|---|---|---|
| 4 | Wiegand 1 | OFF | ON | OFF | ON | OFF | ON | OFF | ON |
| 5 | Wiegand 2 | OFF | OFF | ON | ON | OFF | OFF | ON | ON |
| 6 | No Parity | OFF | OFF | OFF | OFF | ON | ON | ON | ON |

**Tabla 3:** Selección wiegand para el lector

A continuación se puede observar el lector con el led rojo, que indica que el sistema está en modo armado, y el led verde, que indica que el sistema está desarmado:

**Figura 29:** Led de estado armado y desarmado

## 3.2. Diseño de la aplicación del sistema

Todo el diseño funcional del sistema no tiene cabida sin que el cerebro de todo el proyecto cobre vida. La aplicación es la que toma decisiones, la que supervisa, la que decide qué hacer, cuándo hacerlo y porqué hacerlo. En este apartado se describe el diseño de la aplicación desarrollada.

### 3.2.1 Diagrama de bloques de la aplicación

Nuestro sistema empotrado deberá funcionar con una aplicación y librerías desarrolladas bajo el sistema operativo en tiempo real FreeRTOS.

En el diseño de la aplicación se ha tenido en cuenta la modularidad en cuanto a que cada módulo realiza las funciones correspondientes para las que ha sido diseñado. El diseño también se ha realizado de manera encapsulada para que cada módulo tenga públicas las funciones necesarias.

En la siguiente Figura se indica el diagrama de bloques de la aplicación del sistema:

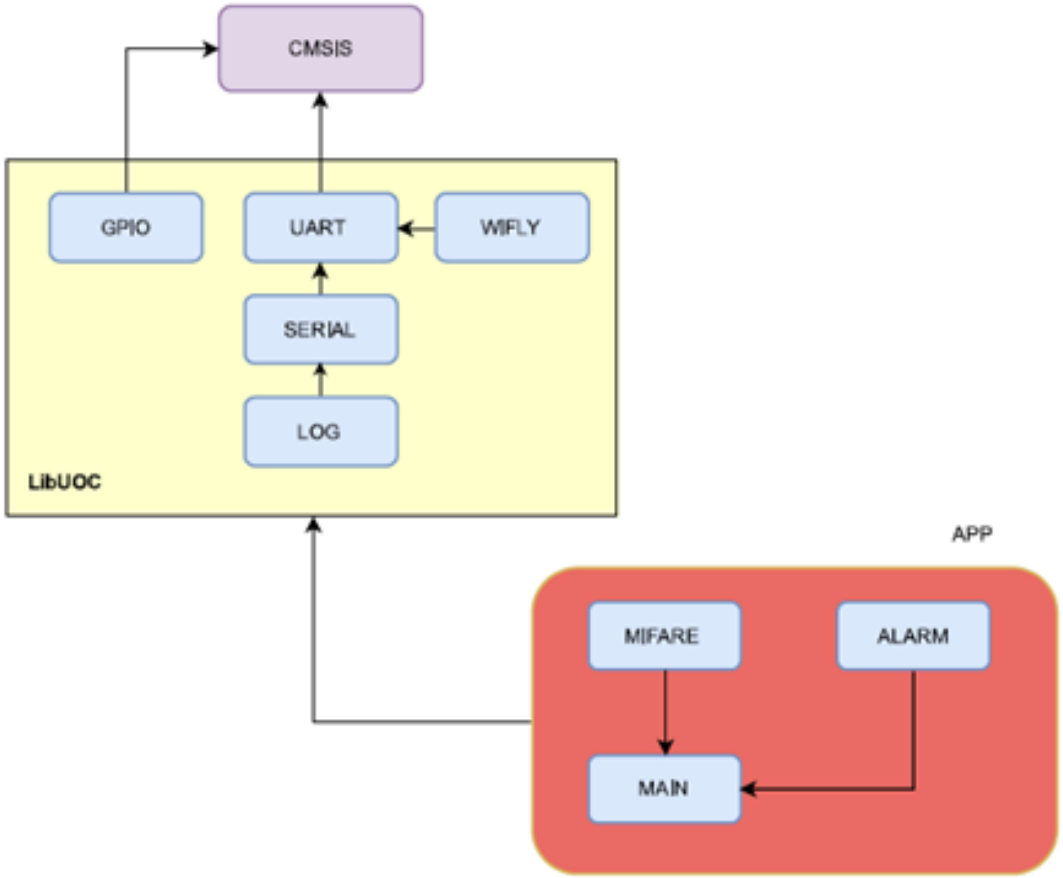



**Figura 30:** Diagrama de bloques de la aplicación

El programa necesario para que el dispositivo funcione está basado en 3 capas principales tal y como se puede observar en la figura anterior: la librería CMSIS, la librería LibUOC y la aplicación:

- CMSIS: Es la librería que nos permite interactuar con la placa LPC1769 y la proporciona NXP Semiconductors, el fabricante de la placa. Gracias a esta librería se permite un desarrollo más rápido y fácil de aplicaciones con los procesadores Cortex de ARM. Ofrece una capa de abstracción de hardware que habilita unas interfaces de software más sencillas, simplificando la reutilización de software.

- LibUOC: Es la librería que posibilita la interacción entre las diferentes interfaces de la placa como son GPIO, para la configuración de pines; UART, para enviar y recibir información a través de los pines correspondientes; contiene los módulos LOG y SERIAL, que permite la visualización de eventos por pantalla; el módulo WIFLY, que permite la interacción entre placa y dispositivo Wifly, como por ejemplo para conectarse a la red inalámbrica, enviar un e-mail o configurar el servidor SMTP.

- Aplicación: es el programa principal que se ejecuta cuando ponemos en marcha el sistema. En el MAIN se inicializan todas las funcionalidades, se definen las tareas que

el procesador debe realizar periódicamente, las funciones y métodos a llamar de las librerías o de la propia aplicación. El módulo ALARM se encarga de gestionar las salidas que se deben activar si se produce una intrusión y el envío de correo electrónico. El módulo MIFARE gestiona el lector y procesa los datos recibidos de este obteniendo una numeración para cada tarjeta. Decide si la tarjeta es aceptada o rechazada.

El funcionamiento conjunto de estas 3 capas principales y la interacción entre ellas, gracias al diseño de la aplicación, posibilita que de cara al usuario sea visualizada como un único elemento.

# 4. Descripción detallada

En este apartado se procede a especificar con detalles técnicos el funcionamiento del sistema de intrusión y control de accesos. Primeramente se muestran la aplicación, su arquitectura, el diseño de módulos realizado, las diferentes tareas creadas para monitorizar el sistema.

Posteriormente se detalla el procedimiento seguido para la comunicación con el servidor SMTP, la configuración del dispositivo wifly, así como las funciones implementadas, semáforos y funcionamiento específico para cada caso.

A continuación se describe el protocolo Wiegand utilizado para la comunicación con el lector de tarjetas MIFARE, el funcionamiento del propio lector y el modo en que se diseña el módulo mifare de la aplicación para que se detecte cada vez que se presenta una tarjeta frente al lector.

Finalmente se detalla el conexionado del sistema con los periféricos, dispositivos de comunicación y la alimentación de la central.

## 4.1. Aplicación desarrollada en la central de intrusión y control de accesos

La aplicación, tal y como ya se ha mostrado en la figura 14, consta de 3 módulos principales que son los que realizan las funciones básicas del sistema. No obstante, la aplicación no podría funcionar sin los módulos incluidos en la librería LibUOC y la librería CMSIS, que son los que permiten gestionar la información que se desplaza interiormente en la aplicación y la que se exterioriza o se recibe del exterior.

Comenzaremos explicando la librería LibUOC para comprender el funcionamiento de configuración de la placa LPC1769, para posteriormente poder entender de una manera más clara el funcionamiento de la aplicación.

### 4.1.1 Librería LibUOC

La finalidad de este trabajo se describe en los objetivos del proyecto, donde se indica que el sistema debe constar de unos elementos de entrada, el detector volumétrico y el contacto magnético principalmente, que en activarse debe generar una alarma, las salidas del sistema, en función de si la intrusión está conectada o no. Estos elementos de entrada y salida se gestionan a través del módulo GPIO.

Módulo GPIO

La placa LPC1769 dispone de 52 pines de entrada y salida denominados “General Purpose In/Out” (GPIO). Dichos pines se pueden configurar como entrada o como salida, se pueden habilitar resistencias “pull-up” o “pull-down” en cada pin para facilitar que la entrada se detecte o bien como un 1 lógico, o bien como un 0 lógico. También se pueden configurar como “open drain mode” que lo que hace es poner a GND el pin especificado.

En nuestro caso se han configurado dos entradas en los pines P0.1 y P0.2 para el contacto magnético y detector volumétrico respectivamente. En reposo estos pines deben recibir un 1 lógico, es decir, siempre reciben tensión. Cuando o bien el detector volumétrico o el contacto magnético se abren por intrusión, entregan al pin un 0 lógico. Por este motivo se ha habilitado el modo pull down en ambos.

Para las salidas se han utilizado los pines P0.7 (zumbador), P0.8 (foco o led) y P0.9 (cerradero electrónico). El funcionamiento es una salida flotante cuando no están activados y un 1 lógico (3,2V) cuando deben activar las salidas. Se ha habilitado el modo pull up resistor en cada uno de ellos.

Mediante las funciones Gpio_config, Gpio_getValue y Gpio_set del módulo GPIO podemos configurar un determinado pin, obtener el valor actual del pin (1 o 0 lógico) y poner el pin a un determinado valor de salida (1 o 0 lógico).

Una vez configuradas las entradas y salidas del sistema, el módulo LOG ayuda a externalizar cómo está funcionando el código, permitiendo añadir un texto de salida por pantalla cuando sea necesario. De este modo, a la hora de desarrollar la aplicación se ha hecho un uso intensivo de esta función para visualizar por ejemplo cuando se ejecuta una función determinada o cerciorarse de que el programa no ha dejado de correr. A nivel de usuario en la aplicación diseñada, el módulo LOG nos da información sobre el estado de las entradas, si se ha producido una alarma, se ha enviado un e-mail o se ha restablecido la alarma entre otros. El módulo LOG requiere del módulo SERIAL y el módulo UART para poder enviar bits a través del puerto UART correspondiente.

Módulo SERIAL

Este módulo realiza la tarea de intermediario entre LOG y UART, con funciones implementadas para leer y escribir a través del puerto UART. Antes de usar el puerto UART es necesario inicializarlo para configurar las interrupciones y semáforos necesarios para el envío y recepción de datos sin interrupciones.

Las funciones que dispone este módulo son Serial_start, que crea un semáforo y llama a la función UART_init del módulo UART; la función Serial_vsend, que coge el semáforo para que la función no sea interrumpida mientras envía la información al puerto UART indicado mediante un buffer; y la función Serial_send, que envía los datos a través del puerto serie.

### Módulo UART

"Universal Asynchronous Receiver/Transmiter", cuyo acrónimo es UART, es el circuito del micro controlador que permite transmitir y recibir datos serie. Su misión principal es convertir los datos recibidos del bus de la placa en formato paralelo al formato serie que es el que se envía a través del puerto UART, es decir, se envía un único bit a la vez y de forma secuencial hacia el exterior. Del mismo modo, cuando se reciben datos serie del exterior, se transforman los datos serie en formato paralelo.

Por lo tanto, este módulo de la librería se encarga de enviar y recibir físicamente datos en codificación de cambios de voltaje de forma asíncrona, por paquetes y con bits de paridad, inicio y final del paquete. Otra de las características que nos permite configurar el módulo UART es la tasa de transferencia de bits o "baudrate" que se envía a través del puerto.

Las funciones que incluye este módulo de la librería son: UART_init, que en función de los parámetros pasados configuran los pines para su función UART e inicializar las interrupciones; las propias interrupciones, que detectan cuando se reciben datos a través del puerto UART; UART_Send, para enviar datos, UART_Scanf, que escanea el pin receptor de información y a través de las interrupciones pasa las cadenas en un buffer; UART_clear y buffer clear, que conjuntament ponen los buffers a cero.

### Módulo LOG

Para imprimir por pantalla a través del convertidor CP2102 de USB a serie y viceversa, se ha utilizado el puerto UART 1 de la placa LPC1769 configurando los pines P2.0 y P2.1 para tal efecto. Antes de comenzar a enviar datos a través del puerto es necesario inicializarlo mediante la función Log_start indicando puerto y baudrate para la comunicación. El módulo Log llama a la función Serial_start del módulo SERIAL, creando el semáforo e inicializando el puerto UART mediante la función UART_init del módulo UART, que configura los pines indicados anteriormente de la placa.

Las dos funciones para que el módulo log pueda enviar datos a través del puerto UART para la visualización de la información por pantalla a través de putty por ejemplo, son: Serial_start, que llama a la función Serial_start e inicializa los puertos correspondientes y las funcionalidades explicadas en los dos módulos anteriores; la otra función del módulo log es Log_print, que envía la información pasada por parámetro al módulo serie para que la gestione.

El sistema de intrusión y control de accesos dispone de una conexión inalámbrica con la red de internet para permitir el envío de notificaciones, tal y como se ha especificado en la descripción del trabajo. La central de intrusión, es decir, la placa LPC1769 hace uso del dispositivo wifly para este fin, por lo tanto se necesita de un modulo en la librería para la comunicación con este dispositivo, el módulo wifly.

### Módulo WIFLY

El dispositivo wifly requiere de un puerto UART para comunicar con la placa micro controladora. En este caso se han utilizado los pines P0.25 y P0.26, que corresponden con el puerto UART 3 de la LPC1769 que se conectan a los pines del dispositivo DIN y DOUT respectivamente. Además, el dispositivo requiere de una señal de salida de la placa para realizar un reinicio al wifly, usándose para ello el pin P1.30 que se conecta al dispositivo wifly en el pin RESET. Además, necesita alimentación a 3,3V y conexión con el punto de referencia GND.

Para las funciones que se desean desempeñar mediante conexión a internet, es necesario realizar unas tareas básicas, como son la conexión y autenticación en una red wifi, configuración de parámetros básicos del dispositivo, configuración del servidor SMTP y envío de la información que se desea pasar por correo electrónico. Todas estas acciones se deben realizar mediante el paso de comandos especificados en el manual del propio dispositivo. Por tanto, es necesario crear unas funciones que permitan escribir en modo consola contra wifly y recibir las respuestas de confirmación.

También es imprescindible la creación de un semáforo para evitar que cuando la aplicación interactúe con wifly pueda ser interrumpida por otro proceso. En este caso se utilizará un semáforo recursivo debido a que cuando se envían comandos a wifly, no es suficiente con que se envíe un solo comando, sino que se requiere enviar y recibir varios comandos sin interrupción.

Es el caso de la conexión con el servidor SMTP mediante TCP para enviar un correo electrónico, en el momento de establecer conexión, autenticar el usuario y pasarle las peticiones, deben hacerse en un tiempo determinado sin que otra tarea pueda interrumpir el proceso, en caso contrario el servidor dará por cerrada la conexión. Por ello la función

wiflyEmail incluida en el módulo wifly toma un primer semáforo recursivo para toda la función, pero dentro de la función, llama a la función WiflyComand cada vez que se le tiene que pasar un parámetro. WiflyComand cogerá el semáforo de wiflyEmail y se lo devolverá cuando acabe. Se realizará el mismo proceso con los siguientes WiflyComand que contenga la función wiflyEmail y tras el último, wiflyEmail soltará el semáforo para que se puedan continuar con las siguientes tareas.

El servidor SMTP utilizado es SMTP2GO, que es un servidor gratuito fácil de configurar donde además, accediendo a su página web y accediendo a la cuenta de usuario, se puede visualizar el detalle de los e-mails enviados. También permiten la creación de varios usuarios con la misma cuenta, para poder configurar en varios dispositivos.

A continuación se detallan las funciones de este módulo:

- WiflyCleanBuffers: pone a cero los buffers de entrada y salida
- _resetWifly: reinicia el dispositivo wifly mediante el pin P1.30 de la placa, con conexión directa al pin de reinicio de wifly
- Wifly_init: crea el semáforo recursivo y llama a la función UART_init del módulo UART, además de indicar por log que se está iniciando wifly
- WiflyComandLog: envía un comando al dispositivo wifly a través del puerto UART 3 y envía la respuesta a través del log por el puerto UART 1
- WiflyComand: envía un comando al dispositivo wifly, pero sin imprimir la respuesta por el log
- WiflyConsola: pone el dispositivo wifly en modo consola enviando los caracteres $$$
- WiflyConect: con el nombre de la red y contraseña pasados como parámetro, envía los comandos necesarios a wifly para que se conecte a la red indicada
- WiflyResponse: escanea los datos de entrada del puerto UART 3 del wifly y los pasa por el puerto UART 1 como log
- wiflyEmail: el objetivo del módulo wifly es esta función, que permite el envío de un correo electrónico. Como parámetros se indican el receptor, asunto y contenido del mensaje y la función envía la configuración TCP de wifly para la conexión con el servidor SMTP, abre la conexión, se autentica y realiza las peticiones necesarias para el envío.
- wiflySetTCPConfig: envía lso comandos a wifly para configurar el protocolo a utilizar, el nombre del servidor y puerto para abrir el socket.

Además de los módulos principales explicados hasta ahora, la librería LibUOC contiene también otros módulos que se utilizan para el manejo de funciones básicas como son los módulos utils y type.

### 4.1.2 Librería CMSIS

Esta librería está proporcionada por el propio fabricante de la placa LPC1769, NXP Semiconductors. “Cortex Microcontroller Software Interface Standard” (CMSIS) es una interfaz que permite la programación de las diferentes funcionalidades de la placa y crea una interfaz estándar para procesadores de la serie M.

También proporciona la “Application Software Interface” (API) para RTOS, el sistema operativo en tiempo real, y con el estándar de programación que facilita la creación de código con comandos definidos en su librería para una amplia cantidad de productos.

A continuación se muestra la Figura 15 donde se puede observar la estructura de la librería que realiza ARM en su página web:

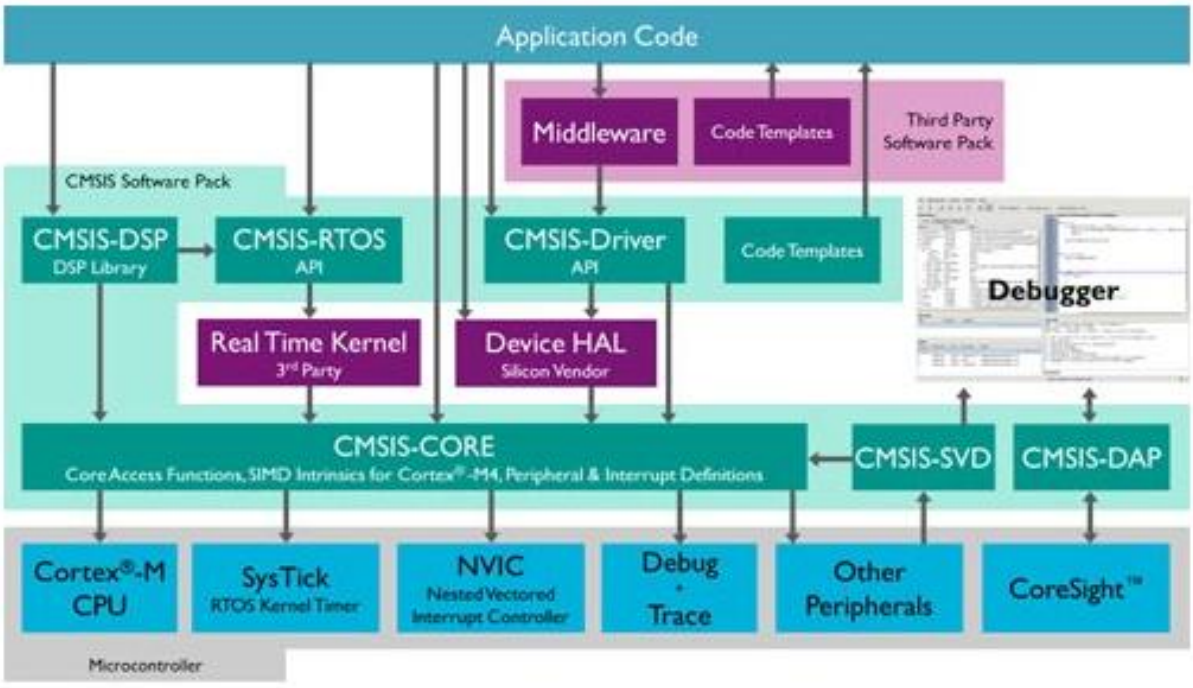



**Figura 31:** Estructura de CMSIS

### 4.1.3 Módulos de la aplicación

La aplicación del sistema de intrusión y control de accesos dispone de 3 módulos principales. El main o programa principal, el módulo alarma y el módulo mifare. En el MAIN se inicializan

todas las funcionalidades, se definen las tareas que el procesador debe realizar periódicamente, las funciones y métodos a llamar de las librerías o de la propia aplicación. El módulo ALARM se encarga de gestionar las salidas que se deben activar si se produce una intrusión y el envío de correo electrónico. El módulo MIFARE gestiona el lector y procesa los datos recibidos de este obteniendo una numeración para cada tarjeta. Decide si la tarjeta es aceptada o rechazada.

MAIN

El main es la pieza inicial de toda la aplicación, la que gobierna a las demás, donde se inicializan los puertos necesarios para las comunicaciones con los demás dispositivos, donde se inicializan los pines de entrada y salida y es donde se definen y ejecutan las tareas de la aplicación que el procesador ejecutará.

Las primeras funciones que se llaman desde el main son en este orden:

- Log_start: que permitirá crear un log de lo que vaya sucediendo en la aplicación
- Wifly_init: inicializa el puerto UART 3 para la comunicación bidireccional con el dispositivo wifly
- alarmInit: esta función del módulo alarm inicializa todos los pines que son necesarios para la conexión con los periféricos
- mifareInit: esta función del módulo mifare, configura y habilita las interrupciones en los pines correspondientes para recibir la codificación de una lectura de tarjeta
- wiflyConect: conecta el dispositivo wifly con la red wifi indicada

Seguidamente se crean las dos tareas necesarias para la aplicación, que son “checkPeripherals” y “accessControl”:

- “checkPeripherals”: se encarga de comprobar tras cada ejecución de la tarea si el sistema está armado o no. Si está desarmado, simplemente se pasa a la siguiente tarea; si está armado, se verifica que los dos periféricos de entrada, contacto magnético y detector volumétrico, tengan el pin correspondiente de entrada a uno lógico (elementos en reposo). Si por el contrario no están a uno lógico, significa que los periféricos de entrada han sido activados por una intrusión y se llama a la función alarmOn del módulo alarm para que actúe.

- “accessControl”: a cada ejecución de la tarea llama a la función cardReader del módulo mifare, para comprobar si se ha recibido algún bit del lector y,

seguidamente, se le pregunta al módulo mifare si hay una ID de tarjeta aceptada. En ese caso, si el sistema estaba armado, pasará a estado desarmado y al contrario, si el sistema estaba desarmado, pasará a modo armado. Por último, en caso de cambio de estado, se envía un correo electrónico notificando a la persona indicada de la identificación de la tarjeta que ha realizado la acción.

El tiempo de retardo para cada tarea es de 100 micro segundos. Este tiempo viene dado por el tiempo que tarda el lector mifare en enviar cada bit de datos cuando se realiza una lectura de tarjeta, que es cada 200 micro segundos. De esta manera, a la tarea “accessControl” le dará tiempo de hacer las acciones correspondientes cuando se active la interrupción de los pines del lector.

Además de las dos tareas indicadas, el main controla las interrupciones externas para los pines P2.10 (EINT0), P2.11 (EINT1) y P2.12 (EINT2), que serán activadas cuando se produzca un flanco descendiente en dichos pines. Las dos primeras interrupciones se utilizan para las entradas de los bits ‘0’ y ‘1’ del lector, y la tercera interrupción se utiliza para el armado/desarmado del sistema mediante el llavín pulsador. A cada interrupción provocada por el llavín, se cambia al estado armado si estaba desarmado, y al estado desarmado si estaba armado.

Módulo ALARM

Este módulo dispone de 4 funciones que gestionan el estado de alarma cuando se activa desde el main por un dispositivo de entrada:

- alarmInit inicializa todos los pines de entrada y salida que intervienen en el sistema de intrusión: entradas, led de estado verde, led de estado rojo, zumbador, led o foco, cerradero eléctrico y también configura la interrupción por flanco descendiente para el llavín de armado en el pin P2.12.
- alarmOn: cuando desde el main se llama a esta función, pasándole por parámetro el elemento que ha causado la alarma, se imprime por log que se ha activado la alarma y el elemento que la ha provocado, se activan las salidas correspondientes, zumbador y foco y se envía el correo electrónico de aviso.
- alarmOff: esta función es llamada cuando estando en el estado de alarma, se desarma el sistema por tarjeta o por llavín. Se envía un correo electrónico indicando que la alarma ha sido restablecida y se apagan las salidas de zumbador y foco

- alarm_getStatus: esta función devuelve el estado actual de la alarma

El siguiente y último módulo de la aplicación es el módulo MIFARE que se encarga de la lectura de las tarjetas y de decidir si la tarjeta es aceptada o rechazada.

Módulo MIFARE

Este módulo gestiona los bits recibidos del lector usando el protocolo Wiegand explicado en el apartado 3.1.5, donde se explica que este protocolo usa dos conexiones, D0 y D1 para enviar los bits con la información de la tarjeta. Estas conexiones están cableadas a los pines de interrupción para tal efecto. En el caso de este proyecto se usa el protocolo Wiegand 26, que envía 26 bits para identificar cada tarjeta. A continuación se describen las funciones creadas:

- mifareInit: inicializa los pines P2.10 y P2.11 para que funcionen en el modo interrupción (EINT0 y EINT1 respectivamente) por flanco decreciente y los habilita.
- data0: esta función es llamada desde el main cuando se produce una interrupción por flanco decreciente en el P2.10, lo que indica que el lector nos está enviando un ‘0’
- data1: esta función es llamada desde el main cuando se produce una interrupción por flanco decreciente en el P2.11, lo que indica que el lector nos está enviando un ‘1’
- Armed: esta función cambia el valor de la variable intrusionArmed a 1 para que el módulo mifare sepa que el sistema está armado
- Disarmed: esta función cambia el valor de la variable intrusionArmed a 0 para que el módulo mifare sepa que el sistema está desarmado
- cardReader: esta función es llamada desde la tarea accessControl a cada iteración. Comprueba si se ha recibido algún bit del lector. Cuando se recibe el primer bit, empieza a contar el número de bits recibidos hasta llegar a 26. En ese momento ya se dispone en el sistema del número de identificación de la tarjeta pasada por el lector y seguidamente se llama a la función checkID del mismo módulo
- checkID: comprueba si la ID de la ultima tarjeta pasada por el lector está entre las permitidas del sistema o no y lo imprime por log
- acceptedID: función llamada desde la tarea accessControl para comprobar si la tarjeta ha sido aceptada o no

- getCardCode: función llamada desde la tarea accessControl para obtener el número de codificación de la tarjeta
- resetCardCode: pone el registro del número de tarjeta cardCode y la variable bitCount a cero

Llegados a este punto, se han explicado con detalle el funcionamiento de la aplicación diseñada para gestionar el sistema de intrusión y control de accesos, cumpliendo los objetivos básicos y secundarios indicados en el apartado 1.3.

### 4.1.4 Esquema de conexionado

Hasta ahora se ha explicado el funcionamiento del sistema a nivel de usuario y a nivel de software. En este apartado se define el procedimiento seguido para llevar a cabo la implementación física de los elementos que intervienen en el sistema.

LPC1769

La alimentación de la placa se realiza mediante la conexión mini USB que utiliza para la carga del programa a la memoria flash del micro controlador. No obstante, también podría alimentarse directamente con una fuente de alimentación de 5V en el pin destinado a dicha función, el J6-2 según el esquema de la placa proporcionado por el fabricante. Se indican en la siguiente figura las conexiones:

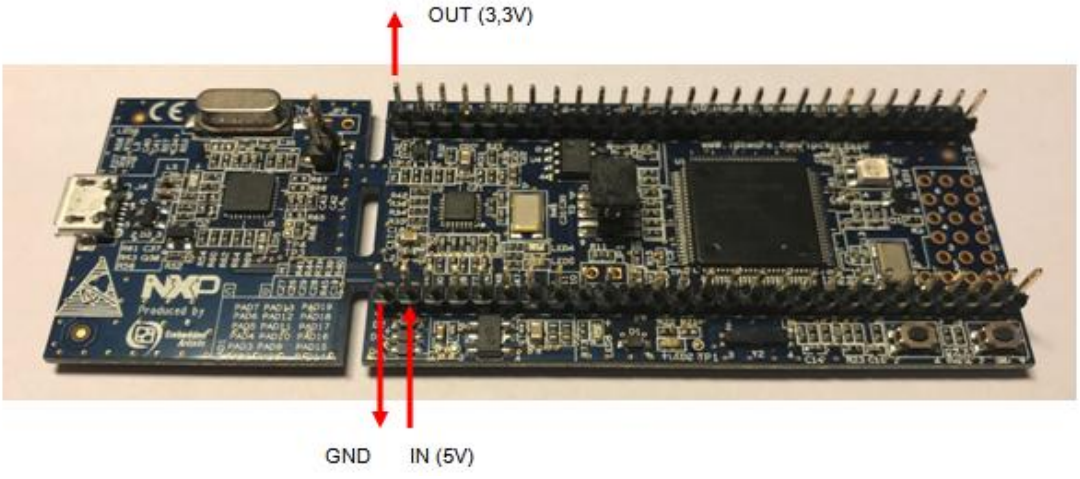



**Figura 32:** Alimentación de la placa LPC1769

Wifly

Wifly funciona a 3,3V, por lo que se alimenta directamente de la tensión que entrega la placa en su pin de salida de 3,3V y su conexión a GND. Este dispositivo dispone de un pin que se debe conectar a la placa para poder realizar un reinicio mediante un pin de

salida a 3,3V. Se debe conectar también los pines DOUT y DIN del dispositivo wifly a un puerto UART de la placa para el envío y recepción de datos.

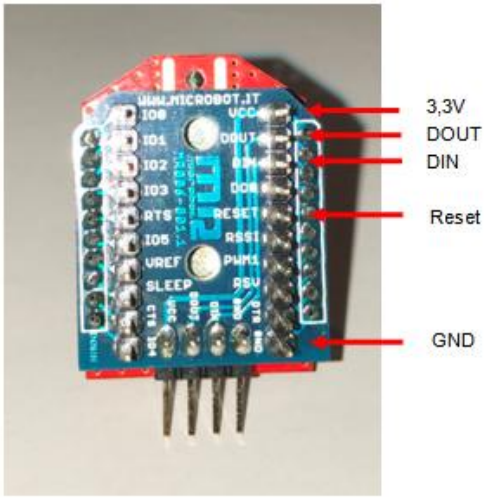



**Figura 33:** Conexión módulo Wifly

CP2102

De igual modo que el dispositivo wifly, este dispositivo convertidor de USB a UART necesita de la conexión a 3,3V y a GND para funcionar además de la conexión a otro puerto UART de la placa para el envío y recepción de información.

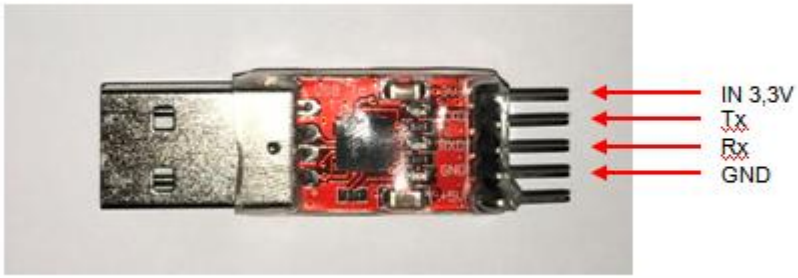



**Figura 34:** Coenxión convertidor CP2102

Detector Volumétrico

El detector volumétrico necesita de una fuente de alimentación de 12V para funcionar. Cuando detecta la presencia de movimiento, abre un contacto normalmente abierto libre de tensión por el que pasamos la señal de 3,3V provenientes de la placa LPC1769. De este modo siempre que el pin de entrada de la central reciba tensión,

significará que está en reposo, y cuando deje de recibir, estará en modo detección. Se muestran la conexiones con el dispositivo en la siguiente figura:


**Figura 35:** Conexión Detector volumétrico

Contacto magnético

Este elemento es un interruptor magnético situado en el marco de la puerta que no necesita alimentación para funcionar. Este contaco cierra por la presencia de un imán situado en la puerta. Cuando la puerta está cerrada, cierra el contacto y permite que al pin de entrada de la placa le llegue 3,3V, indicando que al puerta está cerrada. La conexión se realiza a la salida de tensión de la placa, y al pin de entrada correspondiente de la placa.

LED/Foco

El diodo led que simula el foco disuasorio que se debe activar cuando se activa el modo alarma funciona con los 3,3V que entrega la placa en la activación del pin correspondiente como salida de la placa. En la realidad debería realizarse la activación del foco con un relé en función de la tensión de alimentación necesaria.

Zumbador

Al igual que el led, el zumbador funciona con 3,3V proporcionados por la placa. En el caso de una sirena real, esta irá alimentada a 220V con un contacto a 12V para activar y desactivar la sirena y el flash, por lo que también sería necesario un relé.

Cerradero eléctrico

El cerradero eléctrico necesita de 12V para funcionar, cuando se le aplica dicha tensión en sus bornas, permite la apertura de la puerta. Es necesario un relé con tensión de alimentación de la bobina a 3V para activarlo cuando sea necesario desde la central.

La alimentación a 12V se pasa por la cámara del relé conectándola en normalmente abierto, para que solo cierre y llegue la alimentación al cerradero cuando se active la alimentación de la bobina del relé.

Lector MIFARE

La alimentación principal del lector es a 12V y en el cableado de retorno hacia la placa, como son las dos conexiones que permiten la activación del led de estado rojo o verde, y la conexión D0 y D1 para la transmisión de los bits de numeración de las tarjetas MIFARE, entregan todos ellos 5V, aceptados por la LPC1769. En el caso de los leds de estado, se debe configurar el pin de salida de la placa con su función open drain mode para permitir poner el cable correspondiente a GND cuando se active la salida y así activar el led. El conexionado del lector MIFARE se ha mostrado en la figura 16 del capítulo 3.1.5.

Tal y como se ha comentado en el apartado 1.6 de este documento donde se definen los recursos empleados, se ha utilizado como fuente de alimentación una placa electrónica proporcionada por la UOC en la asignatura Tecnología Electrónica del Grado de Tecnologías de Telecomunicación.

Cabe destacar que para que todo el sistema funcione correctamente, el punto de referencia a masa o GND debe ser el mismo para todas las fuentes de alimentación. La placa usada como fuente de alimentación dispone de salidas de tensión de +5V, +12V, +15V, -5V, -12V y -15V, teniendo todas ellas el punto GND en común, por lo que el resto de dispositivos utilizados, también se conectan al mismo punto de referencia a masa.

En la siguiente figura se muestra el esquema de conexionado que se también se adjunta en el anejo:

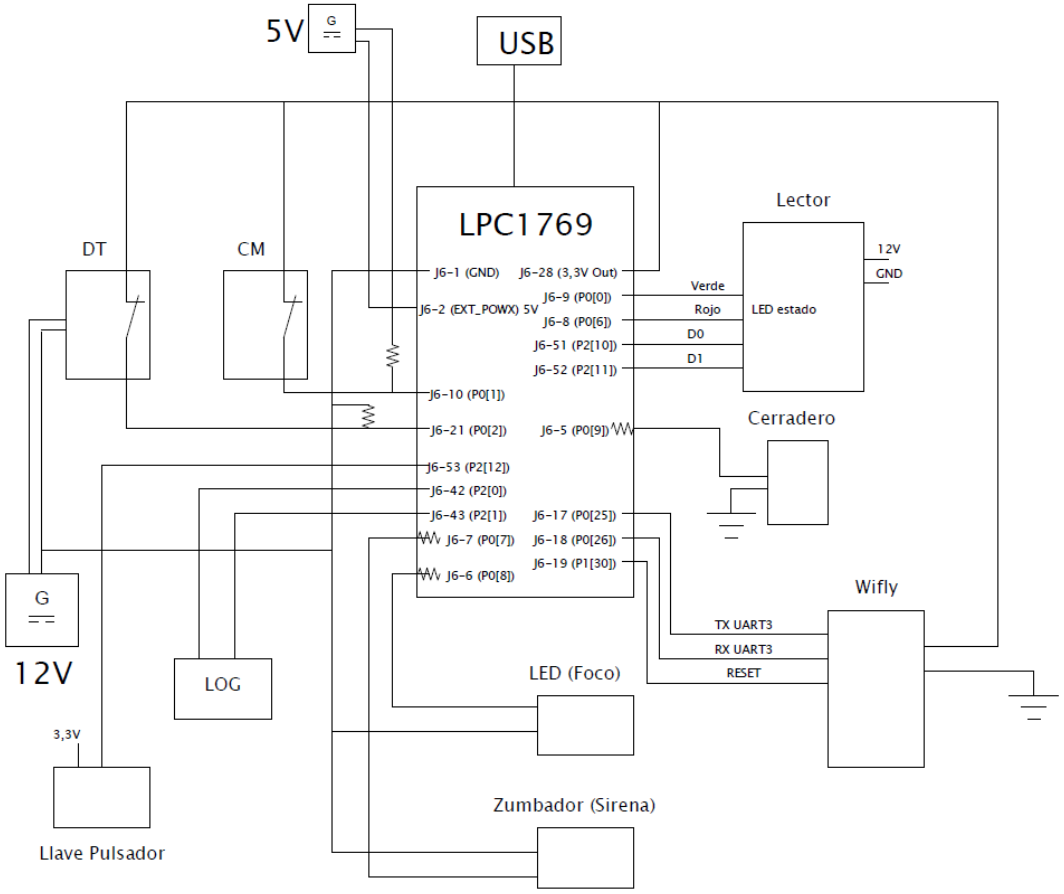



**Figura 36:** Esquema eléctrico de conexión de todo el sistema

## 5. Manual de usuario

En este capítulo se ha realizado un pequeño manual de usuario para mostrar las diferentes acciones que se pueden realizar con el producto, sin tener conocimiento de cómo está diseñado.

Uso mediante llavín de armado/desarmado

Cuando el sistema de intrusión se encuentra armado, indicado por el led de estado en rojo, el usuario deberá introducir la llave en el llavín y girarla en sentido horario para de este modo accionar el pulsador que hará que el sistema pase a modo desarmado. Entonces el led de estado pasará a color verde. En este caso, la apertura de la puerta debe ser manual, no actuará el cerradero electrónico. Se presenta en la siguiente figura el llavín situado en el marco de la puerta y las llaves correspondientes:

***Figura 37:*** *Llavín y llaves para el armado/desarmado*

Del mismo modo, cuando el sistema esté desarmado, con el led de estado en color verde, para armar el sistema al salir de la estancia, se debe girar también en sentido horario la llave para accionar el pulsador que cambiará de estado a modo armado, indicado por el led rojo.

Uso mediante tarjeta MIFARE armado/desarmado y apertura de puerta

Cuando el sistema de intrusión se encuentra armado, indicado por el led de estado en rojo, el usuario deberá pasar la tarjeta por el lector, escuchará un pitido y si la tarjeta es aceptada, el sistema pasará a modo desarmado, indicándolo mediante el led de color verde. En ese momento se activará el cerradero electrónico durante 2 segundos, tiempo durante el que se deberá empujar la puerta para abrirla si así se desea. La persona responsable de la seguridad de la instalación, recibirá una notificación por correo electrónico con la identificación de la tarjeta indicando que se ha desarmado el sistema.

Del mismo modo, cuando el sistema esté desarmado, con el led de estado en color verde, para armar el sistema al salir de la estancia, se debe pasar la tarjeta por el lector, se escuchará un pitido y, si la tarjeta es aceptada, se armará el sistema y se indicará mediante el led de color rojo.

Modo alarma

Si se produce una intrusión o una falsa alarma que hace poner el sistema en modo alarma, inmediatamente se enviará un e-mail de notificación a la persona encargada de la seguridad de la instalación y se activará la sirena (zumbador) y foco disuasorio (diodo led).

Para salir del modo alarma únicamente hay que actuar como si se entrase a la instalación y desarmar el sistema, ya sea mediante llavín o mediante paso de tarjeta por el lector. Entonces el sistema pasará a modo desarmado, cambiando el led de estado de rojo a verde y apagándose la sirena y foco disuasorio. Se enviará un correo electrónico con el mensaje “alarma restablecida” a la persona encargada de la instalación.

## 6. Viabilidad técnica

En este proyecto se ha desarrollado un sistema de intrusión y control de accesos con las funcionalidades básicas de ambos sistemas. Por un lado permite tener vigilada una estancia o instalación para hacer frente a los accesos no controlados por el sistema y por otro permite tener un control sobre las personas que acceden en tiempo real.

A continuación se describen los puntos fuertes y puntos débiles del sistema:

Puntos fuertes

- Detección y activación del protocolo de alarma en local para disuadir a los posibles intrusos y alertar a la población que se encuentre cerca del lugar.
- Aviso en tiempo real al responsable de la instalación mediante correo electrónico al producirse una intrusión.
- Robustez del sistema frente a sustracción de los dispositivos de detección. A pesar de que un posible intruso intente sabotear alguno de los elementos de detección, al perder el contacto con dichos elementos, el sistema entrará automáticamente en alarma.

Puntos débiles

- El sistema no dispone de un modo de configuración por parte del usuario. Si se pretende realizar cualquier cambio en el funcionamiento diferente del diseñado, se debe actuar sobre el código de la aplicación y posteriormente cargarlo en el micro controlador.
- Sería necesario dotar al sistema de una alimentación de tensión alternativa, como baterías o SAI, ya que en caso de falta de suministro intencionado o aleatorio el sistema no funciona.

## 7. Valoración económica

En este apartado se pretende realizar un estudio económico del sistema completo, incluyendo el coste de material, instalación y mantenimiento.

Los productos utilizados para el sistema de intrusión y su coste se desglosan en la siguiente tabla:

| Producto | Unidades | Importe | Importe total |
|---|---|---|---|
| LPC1769 | 1 | 17,90 € | 17,90 € |
| Wifly RN-XV | 1 | 29,90 € | 29,90 € |
| CP2102 | 1 | 18,20 € | 18,20 € |
| Detector Volumétrico | 1 | 56,40 € | 56,40 € |
| Contacto Magnético | 1 | 8,20 € | 8,20 € |
| Cerradero electrónico | 1 | 16,00 € | 16,00 € |
| Llavín | 1 | 4,50 € | 4,50 € |
| Lector MIFARE | 1 | 38,95 € | 38,95 € |
| Tarjetas MIFARE | 5 | 1,00 € | 5,00 € |
| Zumbador | 1 | 3,20 € | 3,20 € |
| Led (pack de 3) | 1 | 2,80 € | 2,80 € |
| Relé + Base | 2 | 6,50 € | 13,00 € |
| Cableado electrico | 1 | 4,20 € | 4,20 € |
| Conexiones (pack cables) | 2 | 2,80 € | 5,60 € |
| Fuente de Alimentación | 1 | 22,95 € | 22,95 € |
| Proto-board | 1 | 19,90 € | 19,90 € |
| | | **Subtotal** | **266,70 €** |
| | | **IVA (21%)** | **56,01 €** |
| **TOTAL** | | | **322,71 €** |

**Tabla 4:** Desglose del coste material del sistema

El coste material de los productos necesarios para la realización del sistema diseñado está dentro de los costes habituales para este tipo de sistemas. No obstante, teniendo en cuenta que se pudiera realizar la fabricación de una gran cantidad de unidades del sistema diseñado, los costes unitarios de los elementos proporcionados por los diferentes proveedores bajaría, permitiendo obtener unos precios finales más rentables.

No obstante, en este desglose no están incluidos los costes de desarrollo del producto ni de instalación. A la hora de sacar a la venta un nuevo producto tecnológico, lo costes de investigación, desarrollo y comercialización son de un importe muy superior a los costes materiales necesarios para la implementación del producto final.

En la siguiente tabla se detallan las fases de desarrollo de la aplicación, diseño de la arquitectura de la aplicación, módulos, comunicación entre dispositivos y se incluye en la última fase la inversión necesaria para la documentación, investigación y desarrollo del material documental para la presentación del producto:

| FASES DEL PROYECTO | ELEMENTOS DESARROLLADOS | | HORAS INVERTIDAS | € / hora | IMPORTE |
|---|---|---|---|---|---|
| FASE 1 | Conexión de periféricos | | 80 | 30,00 € | 2.400,00 € |
| | | Diseño conexión | | | |
| | | Implementación | | | |
| | Detección de sensores y activación de alarmas | | | | |
| | | Módulo GPIO | | | |
| FASE 2 | Implementación del LOG | | 130 | 30,00 € | 3.900,00 € |
| | | Módulo Serial | | | |
| | | Módulo UART | | | |
| | | Módulo LOG | | | |
| | Wifly y e-mail | | | | |
| | | Módulo wifly | | | |
| | | Enviar e-mail | | | |
| | Previa memoria | | | | |
| FASE 3 | Objetivos secundarios | | 130 | 30,00 € | 3.900,00 € |
| | | Módulo Mifare | | | |
| | | Módulo alarmas | | | |
| FASE 4 | Memoria y documentación del producto | | 80 | 30,00 € | 2.400,00 € |
| | | Estructura y redacción | | | |
| | | Formato | | | |
| | | | | **Subtotal** | **12.600,00 €** |
| | | | | **IVA (21%)** | **2.646,00 €** |
| **TOTAL** | | | | | **15.246,00 €** |

**Tabla 5:** Desglose del coste de desarrollo del sistema

Llegados a este punto, podría decirse que el coste de poner en marcha una unidad del sistema de intrusión y control de accesos que se muestra en este proyecto costaría en total:

| | |
|---|---|
| COSTE MATERIAL | 322,71 € |
| COSTE DE DESARROLLO E INVESTIGACIÓN | 15.246,00 € |
| | |
| **TOTAL** | **15.568,71 €** |

**Tabla 6:** Coste total del producto

Como se puede observar, se obtiene un precio imposible de asumir para cumplir el objetivo del producto. Por ello hay que tener en consideración que en el caso de que se llegara a comercializar, el precio debe ser similar al de otro sistema de características similares para obtener un éxito. El método para conseguir bajar el precio del producto consiste en distribuir los costes de desarrollo e investigación en el total de unidades que se esperan vender.

De esta manera, convendría estudiar a partir de qué cantidades de venta es rentable fabricar el producto con un coste de venta al público razonable, y a partir de qué cantidad de unidades se recuperaría la inversión y se empezaría a obtener beneficios. En la siguiente tabla se muestra el coste unitario del producto final para diferentes cantidades de unidades fabricadas:

| Unidades fabricadas | Coste de material | Coste de desarrollo e investigación | Coste final del producto |
|---|---|---|---|
| 25 | 322,71 € | 609,84 € | **932,55 €** |
| 50 | 322,71 € | 304,92 € | **627,63 €** |
| 100 | 322,71 € | 152,46 € | **475,17 €** |
| 500 | 322,71 € | 30,49 € | **353,20 €** |
| 1000 | 322,71 € | 15,25 € | **337,96 €** |

**Tabla 7:** Coste final del producto por unidades fabricadas

Queda demostrado que el coste del producto final con 25 unidades fabricadas ya es mucho más asequible que si se fabricara uno solo. A partir de aquí, se debe realizar un estudio de mercado de productos similares existentes actualmente y el importe que tiene.

Por ejemplo, si la media del importe de los productos similares es de 475 €, si se fabrican y se venden 100 unidades, se recuperaría la inversión realizada en material y desarrollo. A partir de las 100 unidades vendidas, se generarían beneficios. En caso de fabricar 500 unidades, venderlas a 475 €, con coste de fabricación a 337,96 €, generaría unos beneficios de 168.980 €.

# 8. Conclusiones

Una vez finalizado el Trabajo de Final de Grado se evalúan diferentes aspectos relacionados con lo que en este documento se expone y la aplicación desarrollada para alcanzar los objetivos.

## 8.1. Objetivos alcanzados

De los objetivos marcados en el apartado 1.3 y que se vuelven a enumerar a continuación, se han cumplido todos ellos:

**Objetivos básicos**

- Detectar presencia de movimiento mediante detector volumétrico
- Detectar apertura de puerta mediante contacto magnético
- Dotar al sistema de un led de estado para notificar si el sistema está armado o desarmado
- Permitir el armado/desarmado del sistema mediante llavín
- Activar las salidas en caso de intrusión
- Enviar un e-mail de notificación en caso de intrusión para avisar al responsable

**Objetivos secundarios**

- Leer la codificación de una tarjeta mifare que se pase por el lector
- Permitir el acceso si la lectura de la tarjeta es aceptada
- Armar o desarmar el sistema mediante reconocimiento de tarjeta y lector Mifare
- Enviar un e-mail para informar de la identificación de la tarjeta que se ha pasado por el lector

## 8.2. ¿Qué se ha aprendido?

Gracias a la realización de este Trabajo Final de Grado, se han conseguido alcanzar unos conocimientos de programación de micro controladores que hasta el inicio de este proyecto no se disponían.

Se ha conseguido alcanzar un producto final que, a pesar de que puedan surgir mejoras sobre el mismo, ha permitido adentrarse en el mundo de FreeRTOS, conocer cómo funcionan las tareas y como de importante es realizar una buena gestión de las mismas para que el diseño final funcione correctamente según lo requerido.

Se ha conseguido obtener unas nociones básicas de las principales funciones de un micro controlador, configurar pines de entradas y salidas en sus diferentes modalidades, así como gestionar las comunicaciones entre elementos que requieren transferencia de datos como wifly o el módulo log.

Gracias al dispositivo wifly, y en particular a las pautas seguidas desde el inicio de esta asignatura en la PAC correspondiente a wifly, ha facilitado que a la hora de poner en práctica las necesidades de comunicación con el servidor SMTP, se tuviera una cierta soltura para la interacción con el dispositivo mediante código.

Por último, este proyecto ha permitido conocer el funcionamiento del mundo de control de accesos en su versión más básica y conocer qué y de qué manera permite que al pasar una tarjeta MIFARE por un lector, este proporcione la información del ID de la tarjeta.

En global se ha obtenido un conocimiento desconocido hasta ahora en cuanto a sistemas empotrados. La idea que se tenía de un micro controlador era de dispositivos ya diseñados para unas funciones específicas y con unas posibilidades cerradas. En cambio se ha descubierto que, en concreto el micro controlador de NXP Semiconductors LPC1769, permite muchas más opciones de las que se han utilizado para este proyecto.

## 8.3. Autoevaluación

En el apartado 8.1 se han descrito los objetivos marcados inicialmente y se ha indicado que se han cumplido todos los objetivos propuestos. No obstante, cabe destacar que el seguimiento de la planificación no ha sido el correcto.

Inicialmente se realizó una planificación prácticamente a ciegas, distribuyendo uniformemente en el tiempo las diferentes tareas, ya que se carecía de la experiencia necesaria para evaluar dicha planificación. Con la ayuda del consultor, se modificó la planificación en concordancia con su experiencia en la materia de lo que era una planificación más realista.

Aún así, los tiempos marcados en la nueva versión de la planificación tampoco se han ido cumpliendo estrictamente, debido principalmente a la falta de experiencia y conocimientos en cuanto a programación y lo que ello conlleva. Se han dedicado muchas horas, sobre todo al inicio de la programación, para conseguir obtener los resultados que se esperaban de cada tarea.

Una vez terminado el producto final, se han adquirido unos conocimientos globales de diseño y funcionamiento de los diferentes el mentos, que muy probablemente permitirán que para futuros diseños e implementaciones mediante micro controladores, el tiempo necesario para realizar un producto similar se vea reducido considerablemente.

## 8.4. Trabajo futuro

Como tareas pendientes de explorar en cuanto a la realización del sistema de intrusión y control de accesos, han quedado varias que han ido surgiendo a medida que se han ido implementando funciones para el sistema.

Una de ellas y que habría dotado al sistema de un valor añadido es usar los temporizadores. En los sistemas de intrusión es habitual que, ante una detección en uno de los elementos de entrada, el sistema dé un tiempo de reacción a la persona que por error accede a la estancia sin desconectar el sistema. Si transcurrido ese tiempo la persona no actúa desarmando el sistema, se activa la alarma.

En cuanto al diseño de la aplicación, de cara al usuario, aportaría una mejora sustancial un diseño más modular en cuanto a la configuración de ciertos parámetros, como son el nombre de SSID y la contraseña, destinatarios de correo electrónico. Incluir estos datos en unas variables del main de la aplicación podría ser una opción para facilitar al usuario la configuración.

También sería mejorable el diseño de la aplicación para permitir elegir el número de entradas de detección que se desea usar en cada instalación física que se realice del producto. Si se desea cubrir con el sistema de intrusión una pequeña entrada de un recinto, bastará con un único detector volumétrico, pero si por el contrario es un local comercial, se necesitarán varios dispositivos de control y detección. Un diseño más modular a la hora de configurar los periféricos permitiría dedicar un número de pines de la placa LPC1769 para entradas, e indicar cuántos de los disponibles se van a utilizar.

## 9. Glosario

**CCAA** Controles de acceso

**CCTV** Circuito Cerrado de Televisión

**CP2102** Conversor USB a UART

**CSN** Card serial number

**IDE** Integraded Development Environment

**LPC1769** Micro controlador

**MIFARE** Tecnología de lector de tarjetas

**MÚTEX** Indicadores binarios para evitar que recursos compartidos sean usados por más de una función

**TCP** Transmission Control Protocol

**SOCKET** Puerto inicial o de destino al que se enlaza una conexión

**SMTP** Simple Mail Transfer Protocol

**SSID** Service Set Identifier

**SRAM** Memoria RAM estática

**UART** Universal Asynchronous Receiver-Transmitter

**UID** Unique Identifier

**Wiegand** Protocolo de transmisión de datos entre lector y LPC1769

# 10. Bibliografía

**Roving Networks**, Wifly Command Reference, Advanced Features & Applications User's Guide, Los Gatos (California), 2013

**NXP B. V.**, UM10360 LPC176x/5x user manual, Eindhoven (Netherlands), 2014

**Barry, Richard**, Using the FreeRTOS Real Time Kernel – A Practical Guide, 2009

**F. Kurose, James; W. Ross, Keith**, Computer Networking – A Top-Down Approach, PEARSON, Essex (England), 2013

### Recursos Web

Se indica la fecha en que se consultó por primera vez, obviando la fecha de consultas posteriores.

- Wiki de la asignatura (27/09/2016):
http://cv.uoc.edu/webapps/xwiki/wiki/matembeddedsystemslabhome/view/Material/IniciCortexM3?srid=dnjD5dFG

- Placa LPC1769 (3/10/2016):
http://www.nxp.com/

- ARM CMSIS (26/10/2016):
https://www.arm.com/products/processors/cortex-m/cortex-microcontroller-software-interface-standard.php

- Pull-up pull-down resistor (3/11/2016):
http://www.resistorguide.com/pull-up-resistor_pull-down-resistor

- Comunicación UART (26/11/2016):
http://www.circuitbasics.com/basics-uart-communication/

- Protocolo Wiegand (10/12/2016):
https://en.wikipedia.org/wiki/Wiegand_interface

- Tecnología MIFARE (10/12/2016):
https://es.wikipedia.org/wiki/Mifare

- Comparativa de micro controladores (02/01/2017):
http://wonderfulengineering.com/10-best-microcontroller-boards-for-hobbyists-and-engineers

- Micro controlador Beagle (02/01/2017):
https://beagleboard.org/black

- Micro controlador Raspberry (02/01/2017):

https://www.raspberrypi.org

- Honeywell Seguridad (3/01/2017):

https://www.security.honeywell.com

- Imágenes usadas en este proyecto extraídas de diversos sitios web:

www.procasas.com

http://www.nanocomponentes.com/wp-content/uploads/2013/12/intruso.jpg

www.rodych.es

# 11. Anexos

- **Manual Lector MTPX-MF**
- **Esquema eléctrico de conexión del Sistema de Intrusión y Control de Accesos**
- **Esquemático de la placa LPC1769**

# MTPX-MF Surface Mount Mifare Reader

## User Manual

UK FR IT ES DE NL

## Specifications

- Mifare Card Serial Number Reader
- Reads Mifare Classic, Ultralight and Desfire

| | |
|---|---|
| Operating Voltage: | 9 to 14V DC |
| Current consumption: | Max. 130 mA |
| Operating frequency: | 13,56 MHZ |
| Read range: | 1 to 3 cm |
| Reader Data Output: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Cable distance: | 50m |
| Backlight , Buzzer ON/OFF: | yes |
| Green LED: | externally controlled |
| Red LED: | externally controlled |
| Tamper protection: | When Opened or Dismantled |
| Operating Temperatures: | -20°C to +50°C |
| Protection standard: | IP65 |
| Dimensions (mm): | 92 L x 51 W x 25 H |

## Spécifications

- Lecteur de carte de série numéroté Mifare
- Lecture de Mifare Classic, Ultralight et Desfire

| | |
|---|---|
| Alimentation: | 9 à 14V DC |
| Consommation: | Maximum 130 mA |
| Fréquence d'opération: | 13,56 MHZ |
| Distance de lecture du badge: | 1 à 3 cm |
| Protocole de communication: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Distance de câble: | 50m |
| Rétroéclairage, Avertisseur sonore ACTIVÉ/DÉSACTIVÉ: | Oui |
| LED vert: | contrôle externe |
| LED rouge: | contrôle externe |
| Protection anti-sabotage: | Lorsqu'il est ouvert ou démonté |
| Temp.de fonctionnement: | -20°C à +50°C |
| Indice de protection IP: | IP65 |
| Dimensions (mm): | 92 L x 51 l x 25 H |

## Specifiche

- Lettore di tessere numerate Mifare
- Lettura del Mifare Classic, Ultralight e Desfire

| | |
|---|---|
| Alimentazione: | 9 a 14V DC |
| Consumo: | Massimo 130 mA |
| Freq. del sistema operativo: | 13,56 MHZ |
| Distanza di lettura della tessera: | 1 a 3 cm |
| Protocolo di communicazione: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Distanza cavo: | 50m |
| Retroilluminazione , Cicalino ON/OFF: | Si |
| LED verde: | controllato esternamente |
| LED rosso: | controllato esternamente |
| Protezione allarme: | Se aperto o smontato |
| Temperatura di funzione: | -20°C a +50°C |
| Indice di protezione IP: | IP65 |
| Dimensione (mm): | 92 L x 51 l x 25 A |

## Especificación

- Lector de tarjeta de serie numerada Mifare.
- Lectura de Mifare Classic, Ultralight y Desfire

| | |
|---|---|
| Alimentación: | 9 a 14V DC |
| Consumo: | Max. 130 mA |
| Frecuencia de operación: | 13,56 MHZ |
| Distancia de lectura de la tarjeta: | 1 a 3 cm |
| Protocolo de comucación: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Distancia del cable: | 50m |
| Retroiluminado, Buzzer ON/OFF | Si |
| LED verde: | controlado externamente |
| LED rojo: | controlado externamente |
| Protección contra la manipulación: | Cuando se abre o se desmonta |
| Temp. de funcionamiento: | -20°C a +50°C |
| Indice de protección IP: | IP65 |
| Dimensiones (mm): | 92 L x 51 l x 25 A |

## Merkmale

- Mifare-Seriennummerleser
- Liest Mifare Classic, Ultralight und Desfire

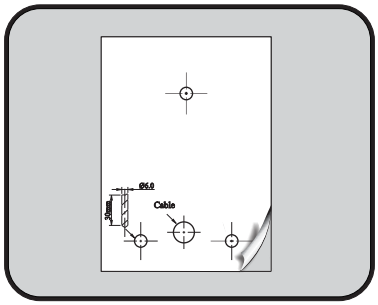
| | |
|---|---|
| Spannungsversorgung: | 9 bis 14V DC |
| Stromaufnahme: | Maximal 130 mA |
| Betriebsfrequenz: | 13,56 MHZ |
| Leseentfernung: | 1 bis 3 cm |
| Datenausgabe Leser: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Kabellänge: | 50m |
| Backlight, Summer AN/AUS: | Ja |
| Grüne LED: | externe Steuerung |
| Rote LED: | exterme Steuerung |
| Sabotageschutz: | Bei gewaltsamer Öffnung oder Ausbrechen |
| Betriebstemperatur: | -20°C bis + 50°C |
| Schutzklasse: | IP65 |
| Abmessungen (in mm): | 92L x 51B x 25T |

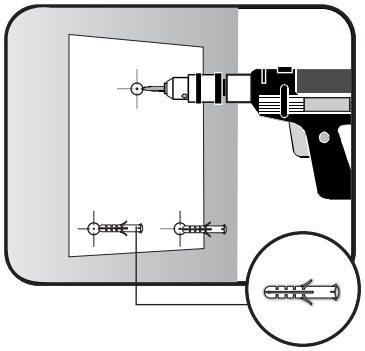
## Specificaties

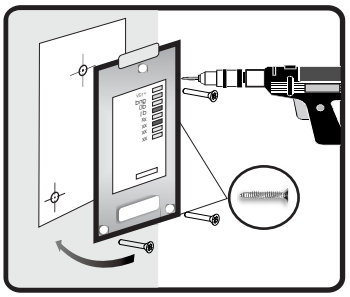
- Mifare Lezer
- Leest Mifare Classic, Ultralight en Desfire

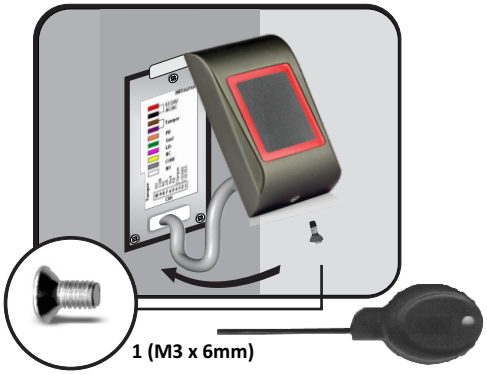
| | |
|---|---|
| Werking spanning: | 9 - 14V DC |
| Stroom opname: | Max. 130 mA |
| Werking frequency: | 13,56 MHZ |
| Lees afstand: | 1 - 3 cm |
| Data Output: | Wiegand 26, 34, 42, 58, 24, 32, 40, 56 bit |
| Kabelafstand: | 50m |
| Achtergrondverlichting , Zoemer AAN/UIT: | Ja |
| Groene LED: | extern aangestuurd |
| Rode LED: | extern aangestuurd |
| Tamperbeveiliging: | In geopende of gedemonteerde staat |
| Werking Temperaturen: | -20°C - +50°C |
| Bescherming standaard: | IP65 |
| Afmetingen (mm) | 92 L x 51 B x 25 H |

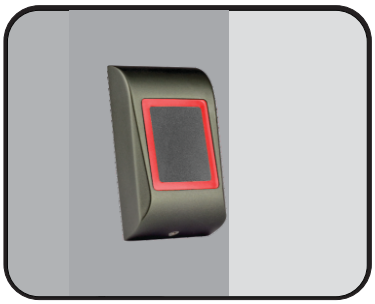
## Mounting/ Montage/ Installazione/ Montaje/ Montage/ Montage

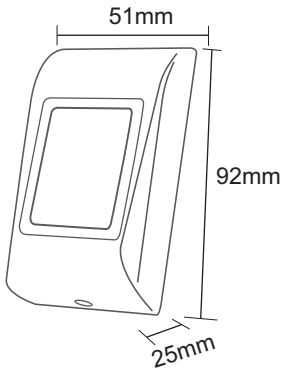









- The reader should not be mounted against metal surface. If there is an installation where the metal surface cannot be avoided, isolation base between the reader and the metal must be used. The thickness of the isolation base should be determined with test.

- Le lecteur ne doit pas être monté sur une surface de métal. Si une installation n'a d'autre possibilité que de monter sur une surface de métal, la base d'isolation entre le métal et le lecteur doit être utilisée. L'épaisseur de la base d'isolation doit être déterminée par test.

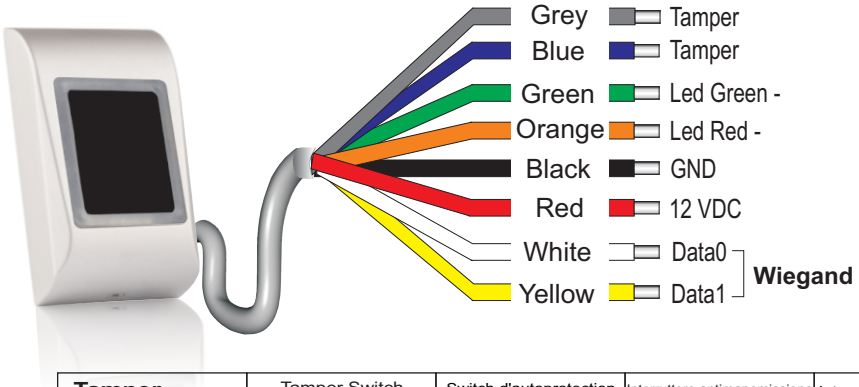
- Il lettore non deve essere montato su superficie mettaliche. Se un installazione non ha altre possibilitá, la base d'isolamento tra il lettore e la superfice mettalica deve essere utilizzata. Lo spessore di questa base d'isolamento puo essere determinata solo con test.

- El lector no tiene que ir montado sobre una superficie de metal. Si en una instalación no hay otro remedio que montarlo sobre una superficie de metal, se tiene que utilizar la base de aislamiento entre el metal y el lector. El grosor de la base de aislamiento tiene que estar determinada por pruebas.

- Der Leser sollte nicht auf metallischem Untergrund montiert werden. Ist die Montage auf metallischem Untergrund unvermeidbar, muss eine Isolierschicht zwischen Leser und Metalluntergrund angebracht werden. Die Stärke der Isolierschicht muss durch Tests ermittelt werden.

- De lezer mag niet worden gemonteerd tegen een metalen ondergrond. Als er een situatie is waarbij men toch op een metalen oppervlak moet installeren dan dient men de lezer te isoleren van de ondergrond. De dikte van de isolatie moet ruim voldoende zijn, een test moet bepalen of het voldoende is.

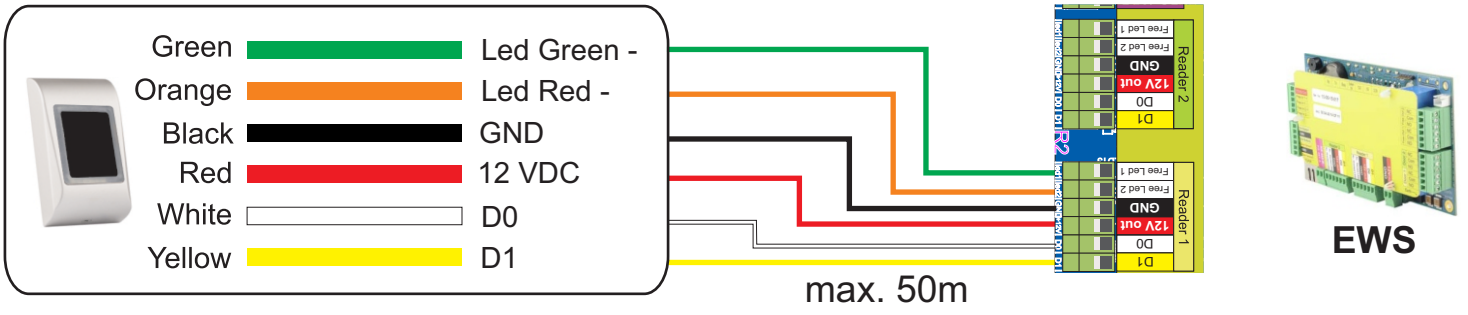
## Wiring / Câblage / Cablaggio / Cableado / Verdrahtung / Verdrahtung




| Colour/ Couleur/ Colore/ Color/ Farbe/ Kleur | Connection/ Connexion/ Connessione/ Conexión/ Anschluss/ Aansluiting |
|---|---|
| Grey/ Gris/ Grigio/ Gris/ Grau/ Grijs | Tamper |
| Blue/ Bleu/ Blu/ Azul/ Blau/ Blauw | Tamper |
| Green/ Vert/ Verde/ Verde/ Grün/ Groen | Led Green - |
| Orange/ Orange/ Arancione/ Naranja/ Orange/ Oranje | Led Red - |
| Black/ Noir/ Nero/ Negro/ Schwarz/ Zwart | GND |
| Red/ Rouge/ Rosso/ Rojo/ Rot/ Rood | 12 VDC |
| White/ Blanc/ Bianco/ Blanco/ Weiß/ Wit | D0 Wiegand |
| Yellow/ Jaune/ Giallo/ Amarillo/ Gelb/ Geel | D1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Tamper** | Tamper Switch | Switch d'autoprotection | Interruttore antimanomissione | Interruptor antisabotaje | Sabotageschalter | Sabotage schakelaar |
| **Tamper** | Tamper Switch | Switch d'autoprotection | Interruttore antimanomissione | Interruptor antisabotaje | Sabotageschalter | Sabotage schakelaar |
| **LED Green -** | Green LED - | LED vert - | Led verde - | Led verde - | Grüne LED | Groene LED - |
| **LED Red -** | Red LED - | LED rouge - | Led rosso - | Led rojo - | Rote LED | Rode LED - |
| **GND** | ground | terre | terra | tierra | Erdung | aarde |
| **12V DC** | 9-14V DC | 9-14V CC | 9-14V DC | 9-14V CC | 9-14V DC | 9-14V DC |
| **D0/ clock** | Data 0 | données 0 | Data 0 | Datos 0 | Datenleitung 0 | Data 0 |
| **D1/ data** | Data 1 | données 1 | Data 1 | Datos 1 | Datenleitung 1 | Data 1 |

## WIEGAND Connection/ Connexion/ Connessione/ Conexión/ Anschluss/ Aansluiting




## DIPSWITCH configuration/ Configuration de Dipswitch/ Configurazione Dipswitch/ Configuración del Dipswitch/ Dipswitch Konfiguration/ Dipswitchconfiguratie

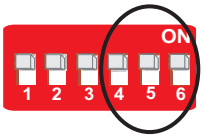
| Dipswitch | Function |
|---|---|
| 1 | Backlight ON/OFF |
| 2 | Buzzer ON/OFF |


| Convert UID | | W 26bit | W 34bit | W 42bit | W 58bit | W 24bit | W 32bit | W 40bit | W 56bit |
|---|---|---|---|---|---|---|---|---|---|
| 3 | **ON** | YES | YES | NO | NO | NO | NO | NO | NO |
| 3 | **OFF** | NO | NO | NO | NO | NO | NO | NO | NO |

**Note:** The conversion from 7byte ID to 4 byte ID is only possible with cards that have 7 byte ID Number. Those are: Mifare plus, Desfire and Ultralight.

### Wiegand selection

| Jumper | | W 26bit | W 34bit | W 42bit | W 58bit | W 24bit | W 32bit | W 40bit | W 56bit |
|---|---|---|---|---|---|---|---|---|---|
| 4 | **Wiegand 1** | OFF | ON | OFF | ON | OFF | ON | OFF | ON |
| 5 | **Wiegand 2** | OFF | OFF | ON | ON | OFF | OFF | ON | ON |
| 6 | **No Parity** | OFF | OFF | OFF | OFF | ON | ON | ON | ON |



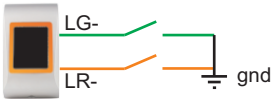

**Default:** Wiegand 26bit

**Use the Dipswitchs no: 4, 5 and 6 to select the desired Wiegand Output**
Utiliser les Dipswitch n° : 4, 5 et 6 pour sélectionner la sortie Wiegand souhaitée
Usa Dipswitch n.: 4, 5 e 6 per selezionare l'uscita Wiegand desiderata
Utilice el Dipswitch DIP número: 4, 5 y 6 para seleccionar la salida Wiegand deseada
Benützen Sie den Dipswitch 4, 5 oder 6 um das gewünschte Wiegand Output zu wählen
Gebruik Dipswitch nr. 4, 5 en 6 voor de selectie van de gewenste Wiegand-uitgang

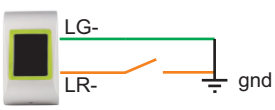
**Note:** All changes can be made live, without power cycling.

## Tricolor LED/ Témoin tricolore/ LED tricolore/ LED tricolor/ Dreifarbige LED/ Driekleurige LED

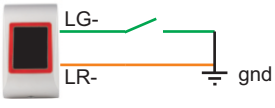
**Orange**(Idle Mode): LG- and LR- not connected
**Orange** (Mode veille): LG- et LR- ne sont pas connectés
**Arancione**: "LG-"(filo verde) e "LR-"(filo arancione) non collegati
**Naranja** (Modo reposo): LG- y LR- no están conectados
**Orange** (Standby): LG- (grünes Kabel) und LR- (orangefarbenes Kabel) sind nicht mit Masse verbunden
**Oranje** ( vrije stand ): draden LG en LR zijn niet aangesloten.




**Green**: LG-(green wire) connected to GND
**Vert:** LG- (câble vert) connecté à GND
**Verde**: "LG-"(filo verde) collegato a GND
**Verde:** LG- (cable verde) conectado a GND
**Grün:** LG- (grünes Kabel) ist mit der Masse verbunden
**Groen:** LG- ( groene draad ) verbonden met massa.

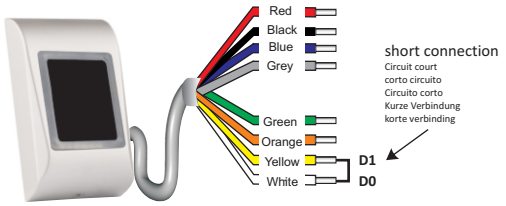



**Red**: LR-(orange wire) connected to GND
**Rouge:** LR-(câble orange) connecté à GND
**Rosso**: "LR-"(filo arancione) collegato a GND
**Rojo:** LR-(cable naranja) conectado a GND
**Rot:** LR- (orangefarbenes Kabel) ist mit der Masse verbunden
**Rood:** LR- ( rode draad ) verbonden met massa.




**No light**: LG-(green wire) and LR-(orange wire) connected to GND
**Sans lumière:** LG-(câble vert) et LR-(câble orange) connectés à GND
**Nessuna luce**: "LG-"(filo verde) e "LR-"(filo arancione) collegati a GND
**Sin luz:** LG-(cable verde) y LR-(cable naranja) conectado a GND
**LED aus:** LG- (grünes Kabel) und LR- (orangefarbenes Kabel) sind mit der Masse verbunden
**Geen verlichting:** LG- (groene draad ) en LR ( oranje draad ) verbonden met massa

# Setting a reader to send fixed site code/ Réglage d'un lecteur pour l'envoi de code site fixé/ Impostazione di un lettore per l'invio di un codice sito fisso/ Ajuste del lector para el envio del Código Sitio fijo Einstellung des Lesers, einen festen Standortcode zu senden/ Een lezer instellen voor het verzenden van een vaste locatiecode




**Turn the power OFF.**

Make short connection between the wires(terminals) D1 and D0.

Set the dipswitch for desired Site Code in binary according to the table bellow.

With 6 Dipswitch positions you can set Site Code from 1-63

**Turn the power ON.**

The reader will start beeping every second. This means setting has been done and saved.

**Turn the power OFF.**

Remove the short connection between D1 and D0 and set your dipswitch to match desired settings for wiegand, card type, for normal use.

**1- ON**
**0- OFF**

| SITE CODE | SW1 | SW2 | SW3 | SW4 | SW5 | SW6 |
|---|---|---|---|---|---|---|
| 01 | 0 | 0 | 0 | 0 | 0 | 1 |
| 02 | 0 | 0 | 0 | 0 | 1 | 0 |
| 03 | 0 | 0 | 0 | 0 | 1 | 1 |
| 04 | 0 | 0 | 0 | 1 | 0 | 0 |
| 05 | 0 | 0 | 0 | 1 | 0 | 1 |
| 06 | 0 | 0 | 0 | 1 | 1 | 0 |
| 07 | 0 | 0 | 0 | 1 | 1 | 1 |
| 08 | 0 | 0 | 1 | 0 | 0 | 0 |
| 09 | 0 | 0 | 1 | 0 | 0 | 1 |
| 10 | 0 | 0 | 1 | 0 | 1 | 0 |
| 11 | 0 | 0 | 1 | 0 | 1 | 1 |
| 12 | 0 | 0 | 1 | 1 | 0 | 0 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 |
| 14 | 0 | 0 | 1 | 1 | 1 | 0 |
| 15 | 0 | 0 | 1 | 1 | 1 | 1 |
| 16 | 0 | 1 | 0 | 0 | 0 | 0 |
| 17 | 0 | 1 | 0 | 0 | 0 | 1 |
| 18 | 0 | 1 | 0 | 0 | 1 | 0 |
| 19 | 0 | 1 | 0 | 0 | 1 | 1 |
| 20 | 0 | 1 | 0 | 1 | 0 | 0 |
| 21 | 0 | 1 | 0 | 1 | 0 | 1 |
| 22 | 0 | 1 | 0 | 1 | 1 | 0 |
| 23 | 0 | 1 | 0 | 1 | 1 | 1 |
| 24 | 0 | 1 | 1 | 0 | 0 | 0 |
| 25 | 0 | 1 | 1 | 0 | 0 | 1 |
| 26 | 0 | 1 | 1 | 0 | 1 | 0 |
| 27 | 0 | 1 | 1 | 0 | 1 | 1 |
| 28 | 0 | 1 | 1 | 1 | 0 | 0 |
| 29 | 0 | 1 | 1 | 1 | 0 | 1 |
| 30 | 0 | 1 | 1 | 1 | 1 | 0 |
| 31 | 0 | 1 | 1 | 1 | 1 | 1 |
| 32 | 1 | 0 | 0 | 0 | 0 | 0 |
| 33 | 1 | 0 | 0 | 0 | 0 | 1 |
| 34 | 1 | 0 | 0 | 0 | 1 | 0 |
| 35 | 1 | 0 | 0 | 0 | 1 | 1 |
| 36 | 1 | 0 | 0 | 1 | 0 | 0 |
| 37 | 1 | 0 | 0 | 1 | 0 | 1 |
| 38 | 1 | 0 | 0 | 1 | 1 | 0 |
| 39 | 1 | 0 | 0 | 1 | 1 | 1 |
| 40 | 1 | 0 | 1 | 0 | 0 | 0 |
| 41 | 1 | 0 | 1 | 0 | 0 | 1 |
| 42 | 1 | 0 | 1 | 0 | 1 | 0 |
| 43 | 1 | 0 | 1 | 0 | 1 | 1 |
| 44 | 1 | 0 | 1 | 1 | 0 | 0 |
| 45 | 1 | 0 | 1 | 1 | 0 | 1 |
| 46 | 1 | 0 | 1 | 1 | 1 | 0 |
| 47 | 1 | 0 | 1 | 1 | 1 | 1 |
| 48 | 1 | 1 | 0 | 0 | 0 | 0 |
| 49 | 1 | 1 | 0 | 0 | 0 | 1 |
| 50 | 1 | 1 | 0 | 0 | 1 | 0 |
| 51 | 1 | 1 | 0 | 0 | 1 | 1 |
| 52 | 1 | 1 | 0 | 1 | 0 | 0 |
| 53 | 1 | 1 | 0 | 1 | 0 | 1 |
| 54 | 1 | 1 | 0 | 1 | 1 | 0 |
| 55 | 1 | 1 | 0 | 1 | 1 | 1 |
| 56 | 1 | 1 | 1 | 0 | 0 | 0 |
| 57 | 1 | 1 | 1 | 0 | 0 | 1 |
| 58 | 1 | 1 | 1 | 0 | 1 | 0 |
| 59 | 1 | 1 | 1 | 0 | 1 | 1 |
| 60 | 1 | 1 | 1 | 1 | 0 | 0 |
| 61 | 1 | 1 | 1 | 1 | 0 | 1 |
| 62 | 1 | 1 | 1 | 1 | 1 | 0 |
| 63 | 1 | 1 | 1 | 1 | 1 | 1 |

**Couper l'alimentation**.
Faire une connexion courte entre les fils (terminaux) D1 et D0.
Régler le dipswitch sur le Code Site souhaité en binaire suivant l'indication du tableau ci-dessous.
Avec 6 positions de Dipswitch vous pouvez régler le code site de 1-63.
**Allumer l'alimentation.**
Le lecteur commencera à émettre des bips et à clignoter chaque segonde (rouge/vert). Ceci signifie que le réglage a été fait et sauvegardé.
**Couper l'alimentation**.
Retirer le circuit court entre le D1 et D0 et régler votre dipswitch afin de correspondre aux réglages souhaités pour le Wiegand, le rétro -éclairage, le buzzer, le type de carte et pour l'utilisation normale.

**Spegnere l'alimentazione.**
Cortocircuitare i terminali dei fili D1 e D0.
Impostare il dip switch per il codice sito desiderato in binario in base alla tabella sottostante.
Avendo a disposizione 6 posizioni del dip switch è possibile impostare il codice sito da 1-63.
**Accendere l'alimentazione.**
Il lettore emette un allarme acustico e lampeggia una volta al secondo (rosso/verde). Ciò significa che l'impostazione è stata eseguita e salvata.
**Spegnere l'alimentazione.**
Rimuovere il cortocircuito tra D1 e D0 e impostare il dip switch in modo che corrisponda alle impostazioni desiderate per Wiegand, controluce, cicalino, tipo di scheda, per il normale utilizzo.

**Desconectar la alimentación.**
Hacer una conexión corta entre los hilos (terminales) D1 y D0.
Ajustar el dipswitch sobre el Código Sitio deseado en binario siguiendo las indicaciones de la tabla abajo.
Con 6 posiciones de Dipswitch puede ajustar el código sitio del 1-63.
**Encender la alimentación.**
El lector empezará a emitir bips y a parpadear cada segundo (rojo/verde). Esto significa que el ajuste se ha realizado y guardado.
**Desconectar la alimentación.**
Quitar el circuito corto entre el D1 y D0 y ajustar su dipswitch con el fin de conseguir los ajustes deseados para el Wiegand, el rétro-iluminado, el buzzer, el tipo de tarjeta y para el uso normal.

**Schalten Sie die Stromversorgung AUS.**
Machen Sie einen kurzen Anschluß zwischen den Anschlußklemmen D1 und D0.
DIP Schalter für den gewünschten Standortcode auf binär entsprechend der untenstehenden Tabelle einstellen.
Mit 6 DIP Schalter-Positionen können Sie den Standortcode von 1-63 einstellen.
**Schalten Sie die Stromversorgung AN.**
Der Leser piept und blinkt im Sekundentakt (rot/grün). Das bedeutet, dass die Einstellung gemacht und gespeichert wurde.
**Schalten Sie die Stromversorgung AUS.**
Entfernen Sie die kurze Verbindung zwischen D1 und D0 und stellen Sie den DIP Schalter auf die gewünschten Einstellungen für Wiegand , Hintergrundbeleuchtung, Summer, Kartentyp, für die Normalanwendung.

**Schakel de stroom UIT.**
Breng een korte verbinding tot stand tussen draden(aansluitingen) D1 en D0.
Zet de dipschakelaar voor de gewenste Locatiecode in binair, in overeenstemming met de onderstaande tabel.
Met 6 standen van de dipschakelaar kunt u de Locatiecode instellen van 1-63.
**Schakel de stroom IN.**
De lezer begint iedere seconde te piepen en te knipperen(rood/groen). Dit betekent dat de instelling is voltooid en opgeslagen.
**Schakel de stroom UIT.**
Verwijder de korte verbinding tussen D1 en D0, en stel de dipschakelaar zo in dat hij afgestemd is op de gewenste instelingen voor wiegand , achtergrondverlichting, zoemer en kaardtype, voor normaal gebruik.

*Example:*
*Site Code:* ***09*** *(001001)*


OFF-OFF-ON-OFF-OFF-ON

To remove previously set Site Code, repeat the setup procedure with dipswitch binary position of all zeros. (all dipswitches should be in OFF position) Note: This will Not set a site code of value zero"0" but will clear any site code previously set, thus setting the reader to send the full card numbers and disabling the "fixed site code" option. This feature works only with Wiegand 24, 26, 32 and 34 bit. The Fixed Site Code changes only the first byte of the message.

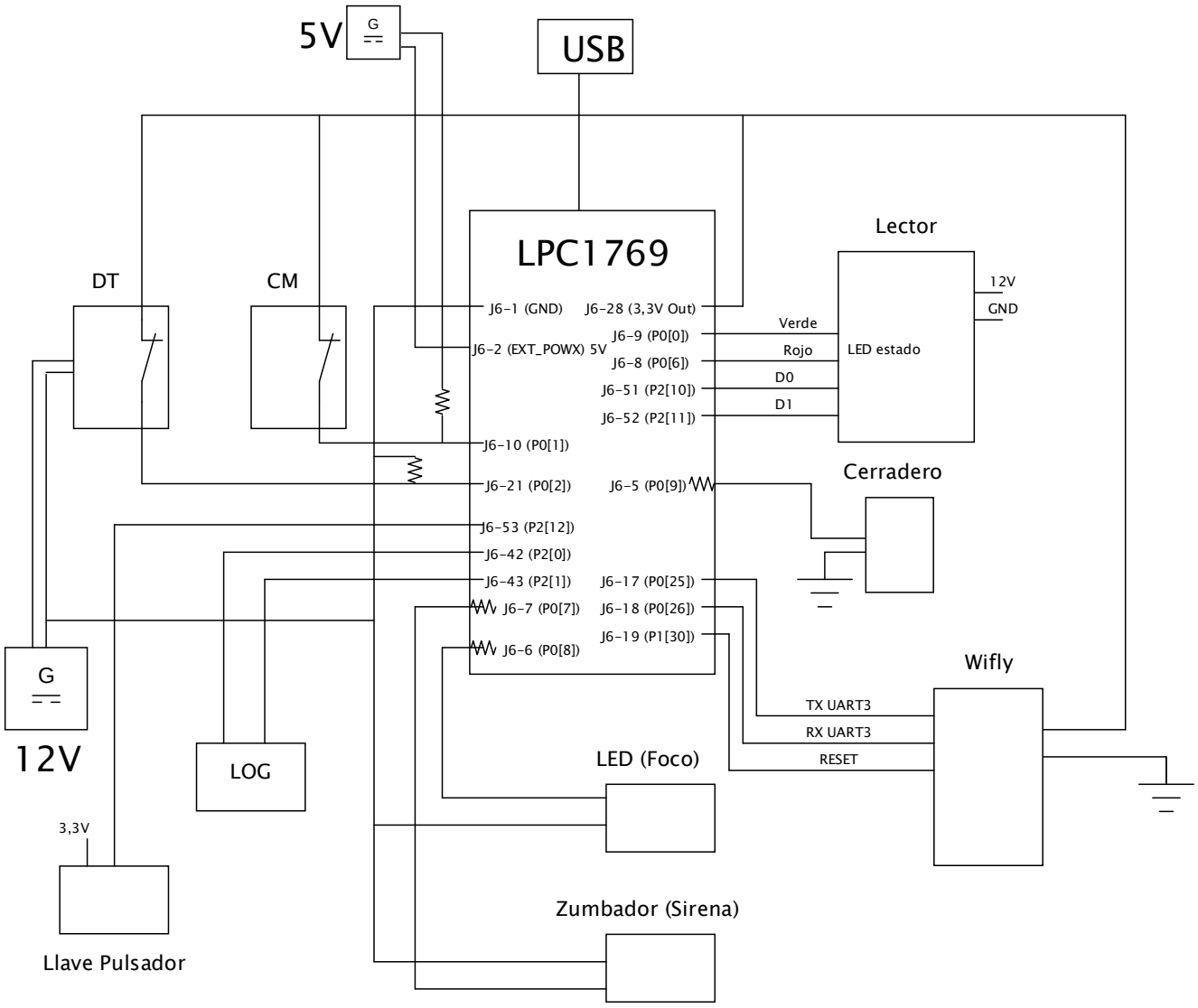
Pour retirer préalablement le réglage du Code Site, répétez la procédure d'installation avec la position du dipswitch binaire sur tous les zéros.(tous les dipswitchs doivent être mis sur la position OFF) Note: Ceci ne réglera pas un Code Site à la valeur zéro "0" mais cela éliminera tout code site préalablement installé, réglant ainsi le lecteur pour l'envoie de numéros de carte entiers et déshabilitant l'option du "code site fixe". Cette caractéristique travaille uniquement avec les Wiegand 24, 26, 32 et 34 bit. Le Code Site fixe change uniquement le premier octet du message.

Per rimuovere un codice sito precedentemente impostato, ripetere la procedura di installazione con la posizione binaria dei dip switch a zero. (tutti i dip switch devono essere in posizione OFF) Nota: Quanto sopra non imposterà un codice sito al valore zero "0", ma eliminerà l'eventuale codice del sito precedentemente impostato, configurando così il lettore per inviare i numeri di scheda completi e disabilitando l'opzione "codice sito fisso". Tale funzione opera solo con Wiegand 24, 26, 32 e 34 bit. Il Codice Sito fisso modifica solo il primo byte del messaggio.

Para eliminar previamente el ajuste del Código Sitio, repetir el proceso de instalación con la posición del dipswitch binario sobre todos los ceros. (todos los dipswitchs tienen que estar puestos en posición OFF) Nota: Eso no ajustará un código sitio al valor cero "0" pero eliminará todo código sitio instalado anteriormente, ajustando por lo tanto el lector para el envío de numéros de tarjeta enteros y deshabilitando la opción del "código sitio fijo". Esta característica funciona sólo con los Wiegand 24, 26, 32 y 34 bit. El Código Sitio fijo cambia sólo el primer byte del mensaje.

Um einen früheren Standortcode zu löschen, wiederholen sie die Einrichtungsprozedur mit dem DIP Schalter in Bitposition auf allen Nullen (alle DIP Schalter sollten in AUS (OFF) Stellung stehen). Anmerkung: Diese Prozedur setzt den Standortcode NICHT auf Null (0), sondern löscht samtliche frühere Standorteinstellungen. Der Leser sendet die vollen Kartennummern und deaktiviert die "fester Standort"-Option. Diese Funktion funktioniert nur mit Wiegand 24, 26, 32 und 34 Bit. Der feste Standortcode verändert nur den ersten Byte der Nachricht.

Om een eerder ingestelde Locatiecode te verwijderen, herhaalt u de installatiepocedure met de dipschakelaar op een binaire stand van allemaal nullen. (alle dipsschakelaars moeten UIT staan) Opmerking: hiermee wordt geen locatiecode met een waarde van "0" ingesteld, maar worden alle eerder ingestelde locatiecodes gewist, om de lezer in te stellen voor de verzending van volledige kaartnummers en om de optie "vaste locatiecode" uit te schakelen. Deze functie werkt alleen met Wiegand 24, 26, 32 en 34 bits. De vaste locatiecode verandert alleen de eerste byte van het bericht.




| Responsible dep. | Technical reference | Created | Approved | |
|---|---|---|---|---|
| **Jordi Becarés** | **TFG** | **Daniel Gómez** | **10/01/2017** | |
| profiCAD | | Document type: **Esquema eléctrico** | Document status: **Aprobado** | Rev.: **3** |
| | | Title, supplementary title: **Sistema de intrusión y control de accesos** | | Scale: |
| | | | Date of issue: **15/01/2017** | Lang.: **ESP** / Sheet: **1/1** |

## Page 2

LPC3154 Powering and Unused parts

## Page 3

LPC3154 Digital I/O

## Page 4

JTAG Interface

## Page 5

LPC17XX

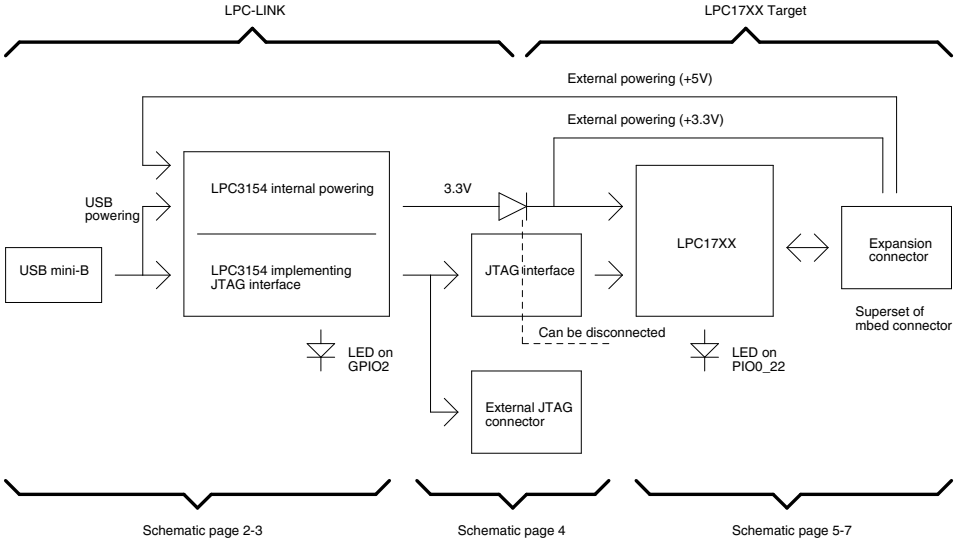
## Page 6

LPC17XX Ethernet and I2C-E2PROM

## Page 7

LPC17XX Expansion connector

## Design Overview

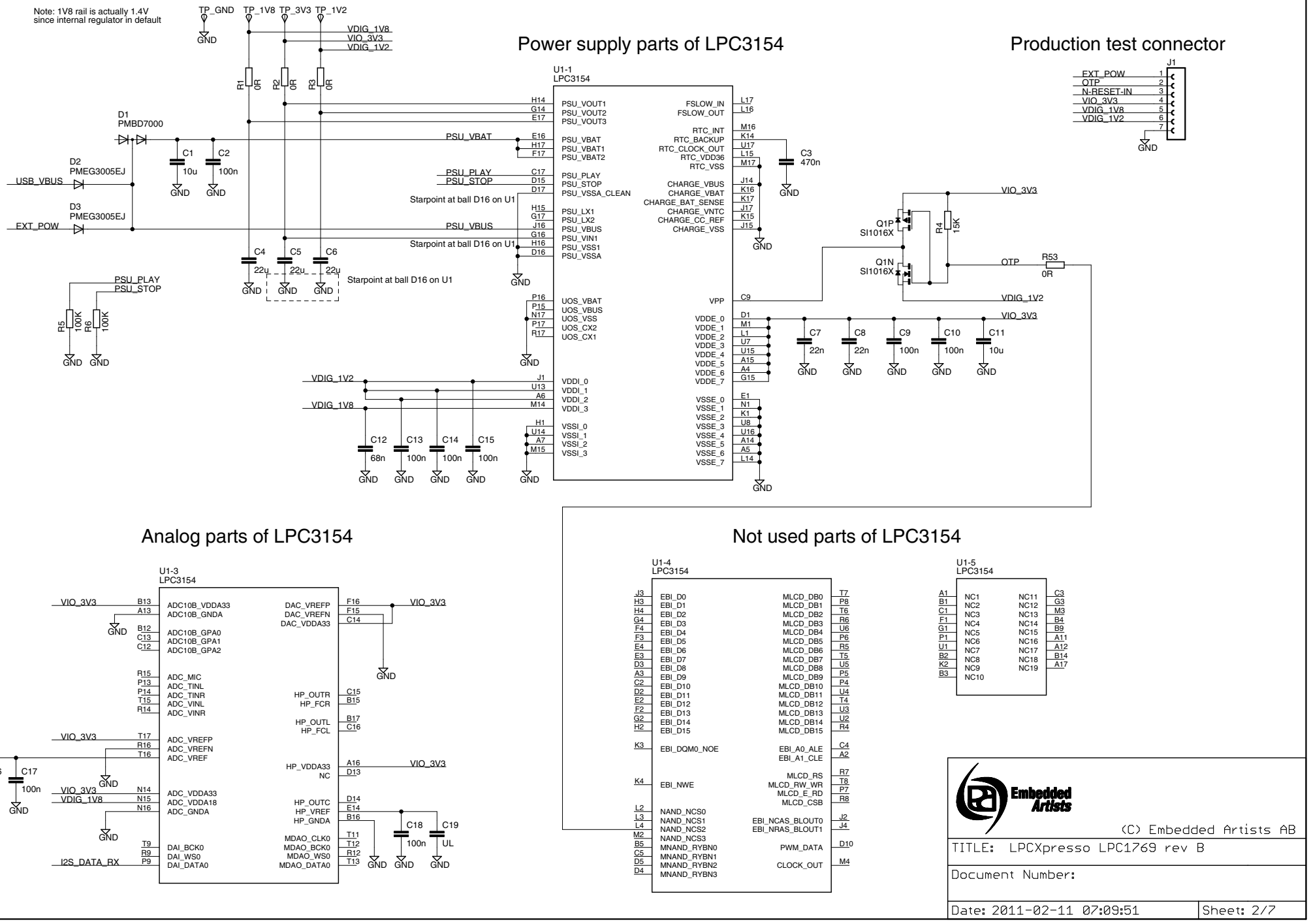


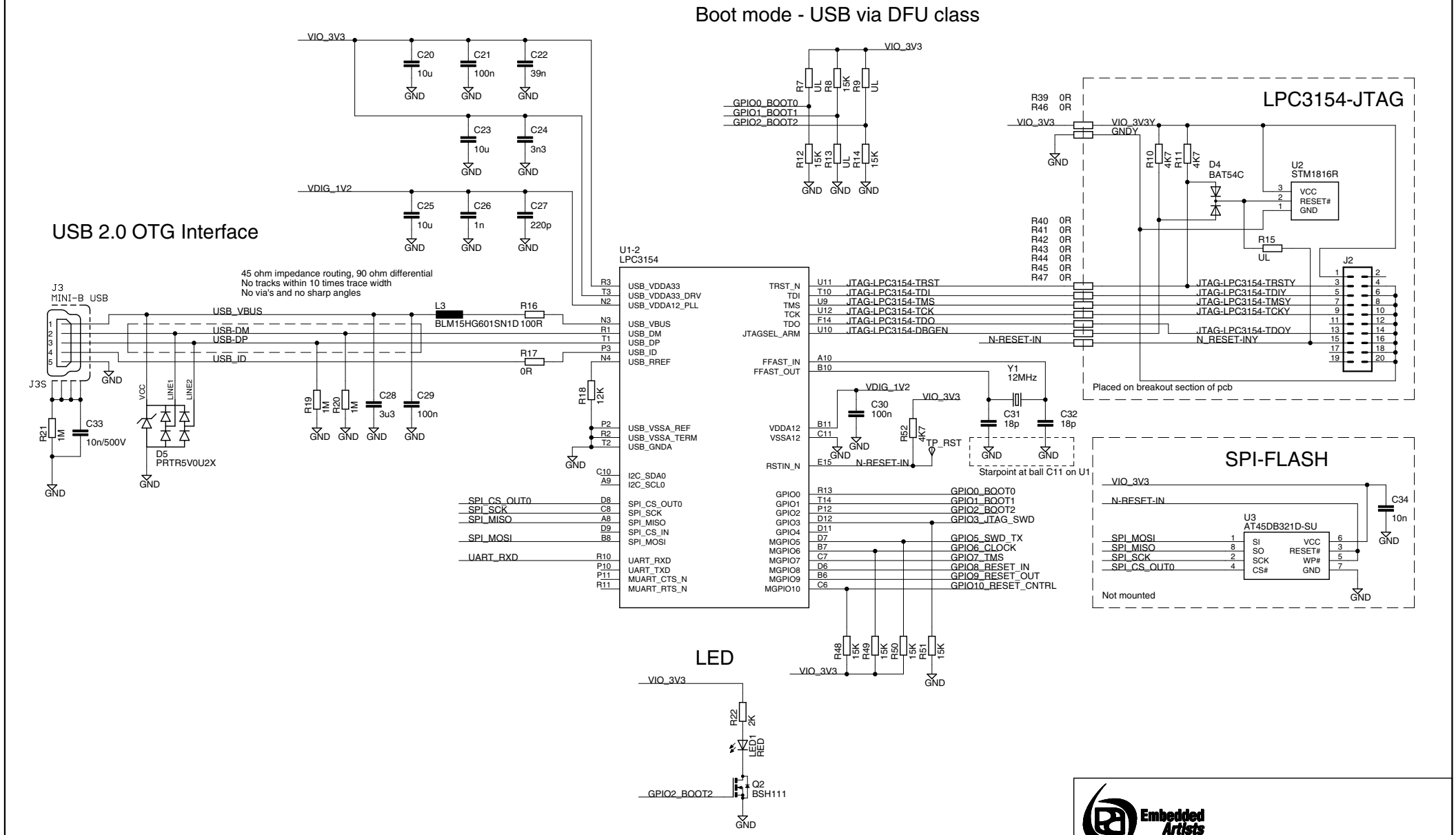

UL = UnLoaded = normally not mounted component.

Default jumper settings are indicated in the schematic.
However, always check jumper positions on actual boards since there is no guarantee that all jumpers are in default place.

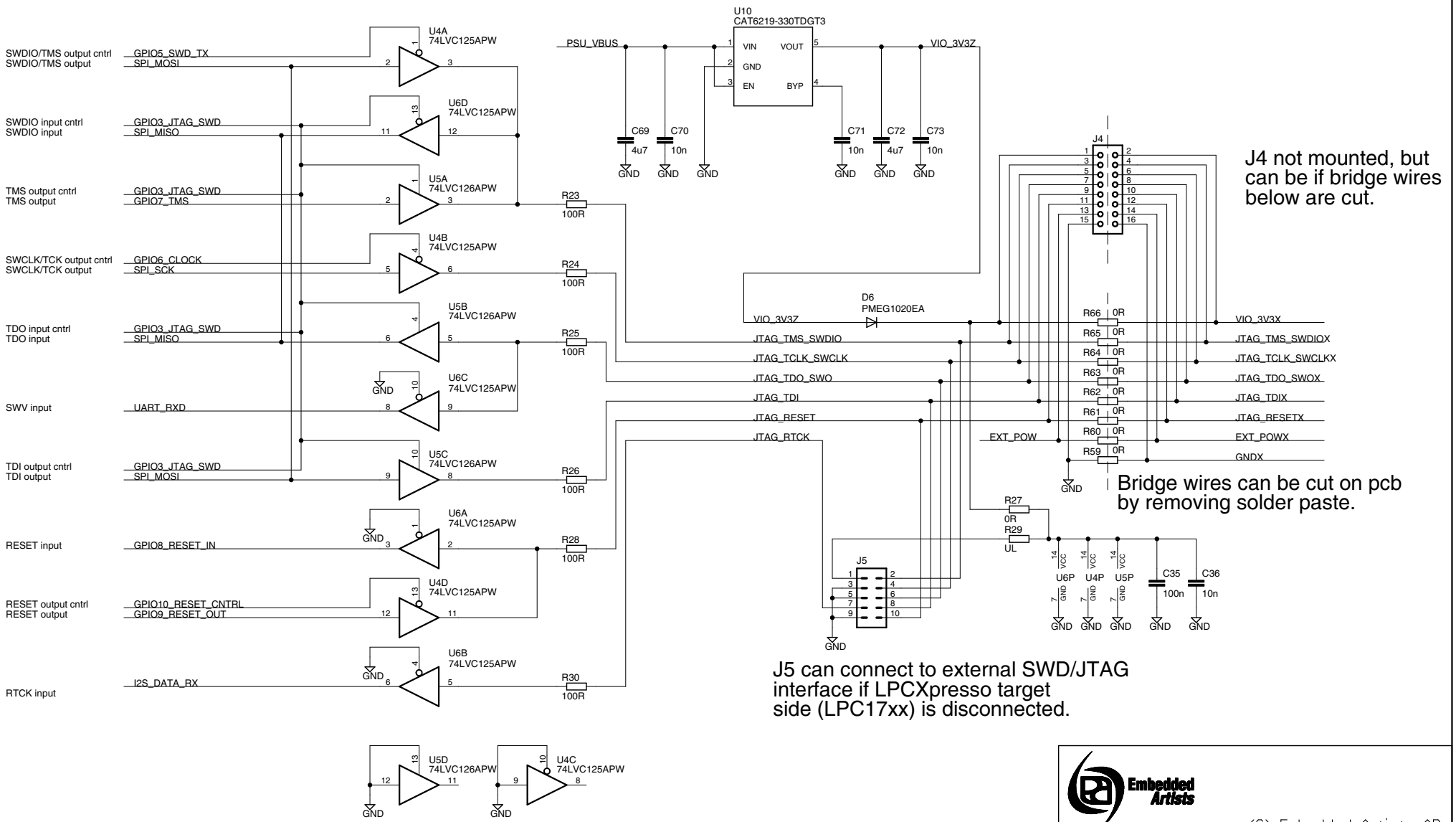


| | |
|---|---|
| TITLE: LPCXpresso LPC1769 rev B | |
| Document Number: | |
| Date: 2011-02-11 07:09:51 | Sheet: 1/7 |


Note: 1V8 rail is actually 1.4V since internal regulator in default
Power supply parts of LPC3154
Production test connector
Analog parts of LPC3154
Not used parts of LPC3154
U1-1 LPC3154
U1-3 LPC3154
U1-4 LPC3154
U1-5 LPC3154
J1
TP_GND TP_1V8 TP_3V3 TP_1V2
VDIG_1V8 VIO_3V3 VDIG_1V2
R1 0R R2 0R R3 0R
D1 PMBD7000
D2 PMEG3005EJ
D3 PMEG3005EJ
USB_VBUS
EXT_POW
C1 10u C2 100n
C3 470n
C4 22u C5 22u C6 22u
PSU_VBAT
PSU_PLAY
PSU_STOP
PSU_VBUS
Starpoint at ball D16 on U1
R5 100K R6 100K
PSU_VOUT1 PSU_VOUT2 PSU_VOUT3
PSU_VBAT PSU_VBAT1 PSU_VBAT2
PSU_PLAY PSU_STOP PSU_VSSA_CLEAN
PSU_LX1 PSU_LX2 PSU_VBUS PSU_VIN1 PSU_VSS1 PSU_VSSA
UOS_VBAT UOS_VBUS UOS_VSS UOS_CX2 UOS_CX1
VDDI_0 VDDI_1 VDDI_2 VDDI_3
VSSI_0 VSSI_1 VSSI_2 VSSI_3
FSLOW_IN FSLOW_OUT
RTC_INT RTC_BACKUP RTC_CLOCK_OUT RTC_VDD36 RTC_VSS
CHARGE_VBUS CHARGE_VBAT CHARGE_BAT_SENSE CHARGE_VNTC CHARGE_CC_REF CHARGE_VSS
VPP
VDDE_0 VDDE_1 VDDE_2 VDDE_3 VDDE_4 VDDE_5 VDDE_6 VDDE_7
VSSE_0 VSSE_1 VSSE_2 VSSE_3 VSSE_4 VSSE_5 VSSE_6 VSSE_7
C7 22n C8 22n C9 100n C10 100n C11 10u
C12 68n C13 100n C14 100n C15 100n
Q1P SI1016X Q1N SI1016X
R4 15K
R53 0R
OTP
VIO_3V3 VDIG_1V2
EXT_POW OTP N-RESET-IN VIO_3V3 VDIG_1V8 VDIG_1V2
ADC10B_VDDA33 ADC10B_GNDA
ADC10B_GPA0 ADC10B_GPA1 ADC10B_GPA2
ADC_MIC ADC_TINL ADC_TINR ADC_VINL ADC_VINR
ADC_VREFP ADC_VREFN ADC_VREF
ADC_VDDA33 ADC_VDDA18 ADC_GNDA
DAI_BCK0 DAI_WS0 DAI_DATA0
I2S_DATA_RX
DAC_VREFP DAC_VREFN DAC_VDDA33
HP_OUTR HP_FCR HP_OUTL HP_FCL
HP_VDDA33 NC
HP_OUTC HP_VREF HP_GNDA
MDAO_CLK0 MDAO_BCK0 MDAO_WS0 MDAO_DATA0
C16 UL C17 100n C18 100n C19 UL
EBI_D0 EBI_D1 EBI_D2 EBI_D3 EBI_D4 EBI_D5 EBI_D6 EBI_D7 EBI_D8 EBI_D9 EBI_D10 EBI_D11 EBI_D12 EBI_D13 EBI_D14 EBI_D15
EBI_DQM0_NOE
EBI_NWE
NAND_NCS0 NAND_NCS1 NAND_NCS2 NAND_NCS3 MNAND_RYBN0 MNAND_RYBN1 MNAND_RYBN2 MNAND_RYBN3
MLCD_DB0 MLCD_DB1 MLCD_DB2 MLCD_DB3 MLCD_DB4 MLCD_DB5 MLCD_DB6 MLCD_DB7 MLCD_DB8 MLCD_DB9 MLCD_DB10 MLCD_DB11 MLCD_DB12 MLCD_DB13 MLCD_DB14 MLCD_DB15
EBI_A0_ALE EBI_A1_CLE
MLCD_RS MLCD_RW_WR MLCD_E_RD MLCD_CSB
EBI_NCAS_BLOUT0 EBI_NRAS_BLOUT1
PWM_DATA
CLOCK_OUT
NC1 NC2 NC3 NC4 NC5 NC6 NC7 NC8 NC9 NC10 NC11 NC12 NC13 NC14 NC15 NC16 NC17 NC18 NC19
GND
Embedded Artists
(C) Embedded Artists AB
TITLE: LPCXpresso LPC1769 rev B
Document Number:
Date: 2011-02-11 07:09:51
Sheet: 2/7


Boot mode - USB via DFU class
USB 2.0 OTG Interface
LPC3154-JTAG
SPI-FLASH
LED
U1-2
LPC3154
J3
MINI-B USB
45 ohm impedance routing, 90 ohm differential
No tracks within 10 times trace width
No via's and no sharp angles
Placed on breakout section of pcb
Starpoint at ball C11 on U1
Not mounted
D5
PRTR5V0U2X
BLM15HG601SN1D
U2
STM1816R
U3
AT45DB321D-SU
D4
BAT54C
Y1
12MHz
LED1
RED
Q2
BSH111
(C) Embedded Artists AB
TITLE: LPCXpresso LPC1769 rev B
Document Number:
Date: 2011-02-11 07:09:51
Sheet: 3/7

# SWD/JTAG Interface




Embedded Artists



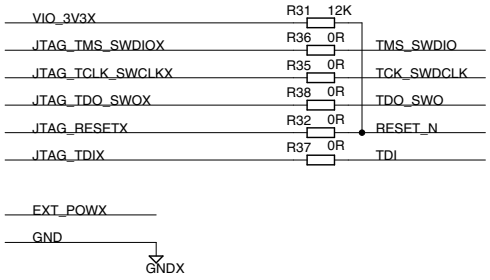
TITLE: LPCXpresso LPC1769 rev B

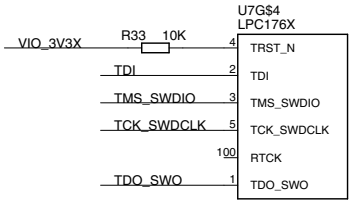
Document Number:

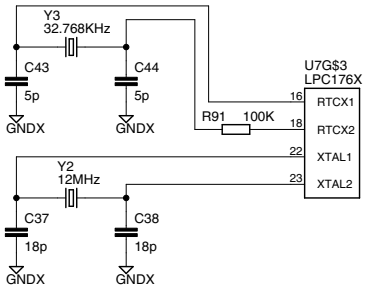
Date: 2011-02-11 07:09:51 | Sheet: 4/7

From LPC-LINK Side

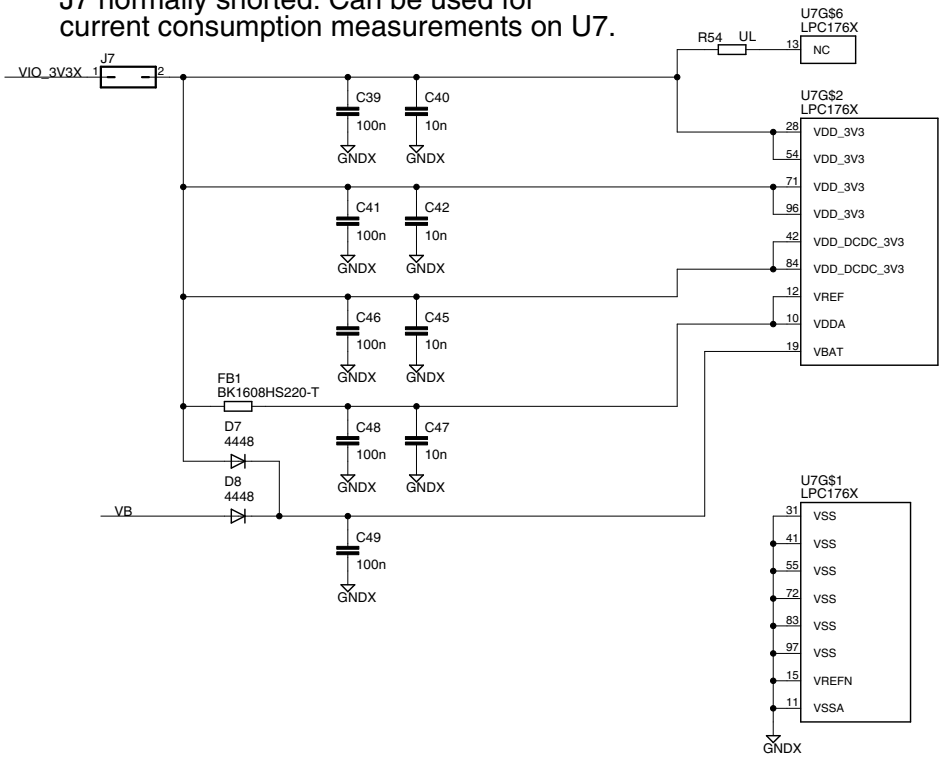
LPC176X Target Side

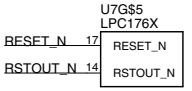


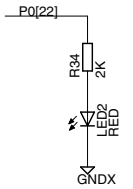




J7 normally shorted. Can be used for current consumption measurements on U7.



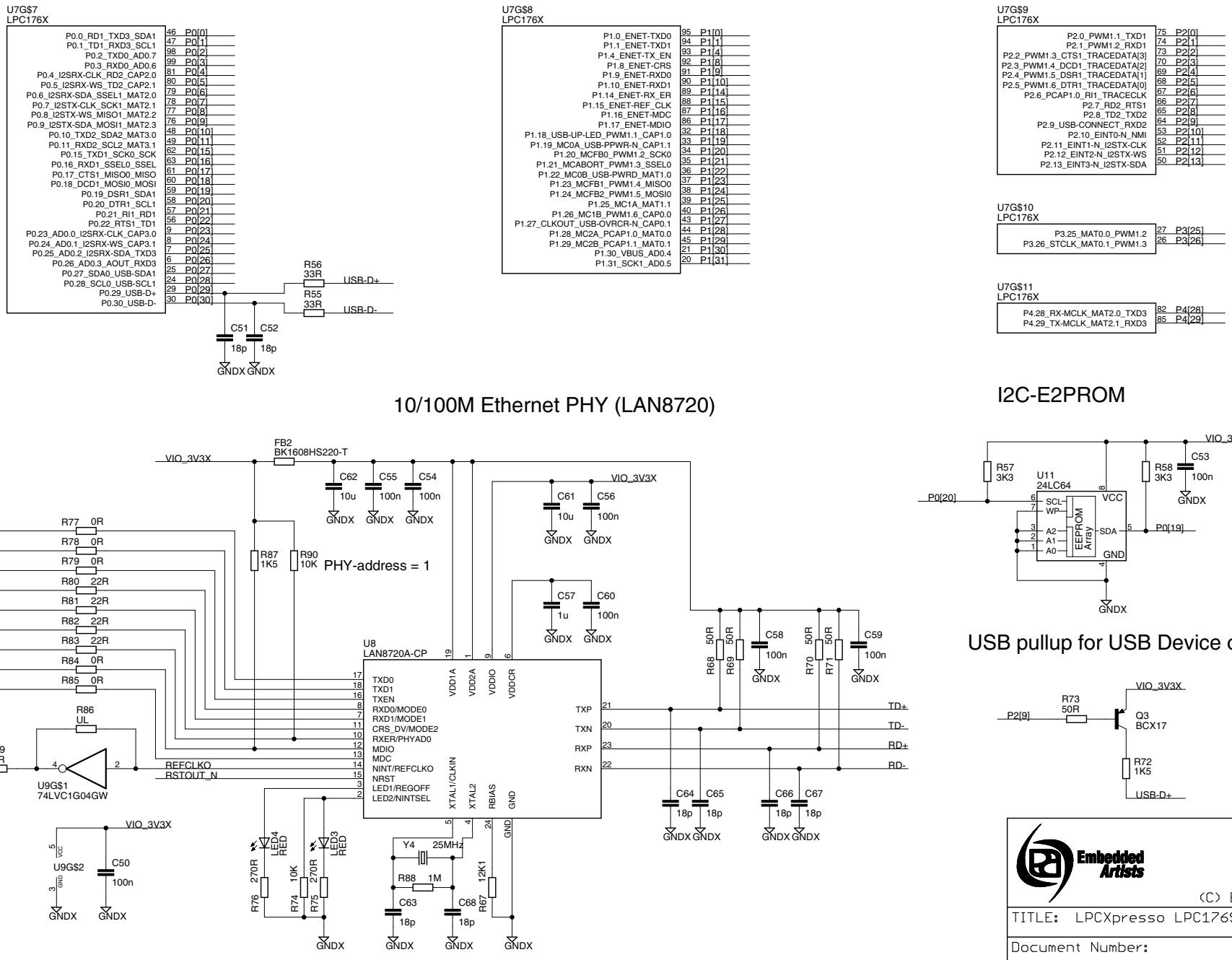



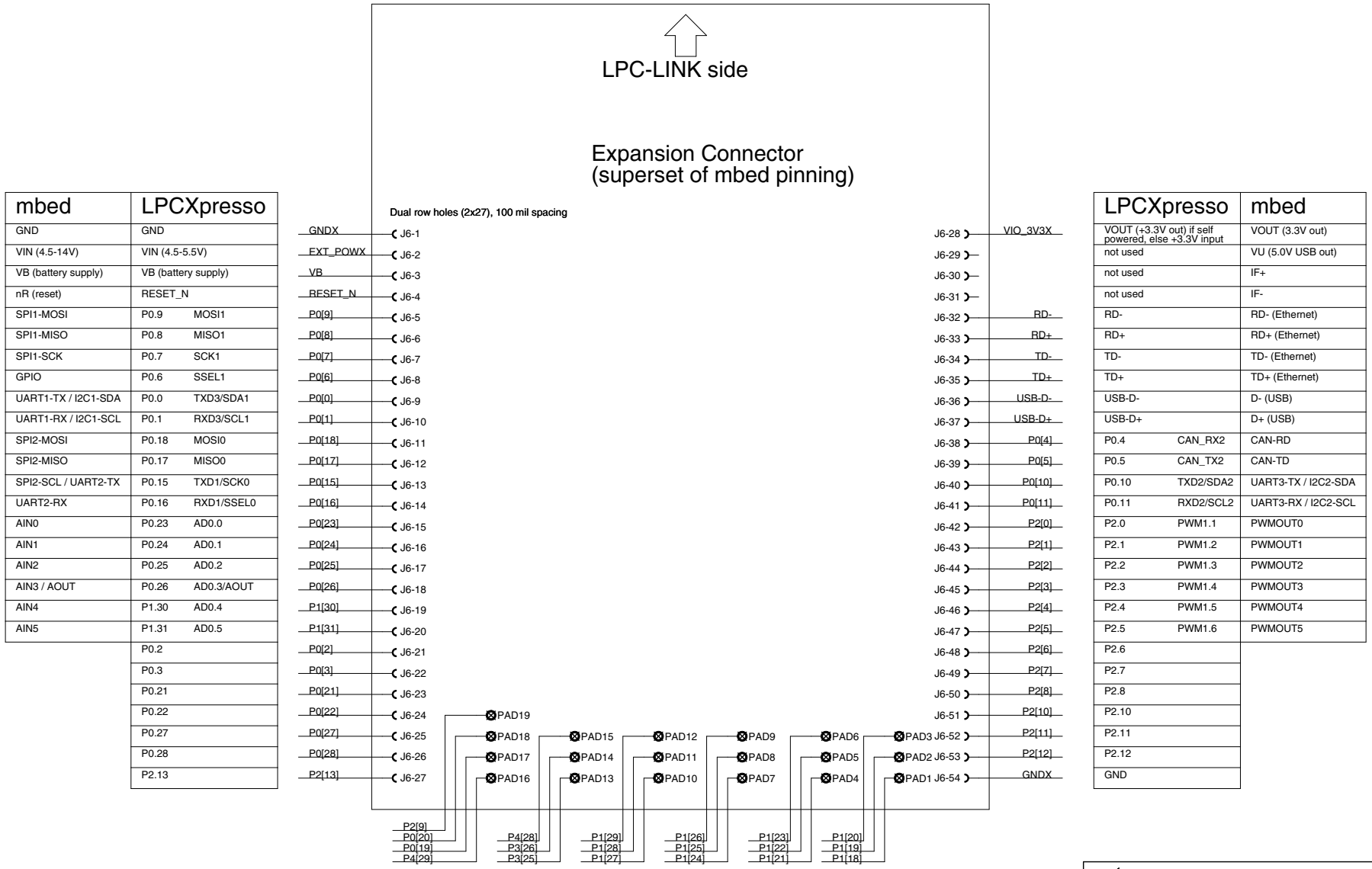

LED






| | |
|---|---|
| TITLE: LPCXpresso LPC1769 rev B | |
| Document Number: | |
| Date: 2011-02-11 07:09:51 | Sheet: 5/7 |


U7G$7
LPC176X
P0.0_RD1_TXD3_SDA1
P0.1_TD1_RXD3_SCL1
P0.2_TXD0_AD0.7
P0.3_RXD0_AD0.6
P0.4_I2SRX-CLK_RD2_CAP2.0
P0.5_I2SRX-WS_TD2_CAP2.1
P0.6_I2SRX-SDA_SSEL1_MAT2.0
P0.7_I2STX-CLK_SCK1_MAT2.1
P0.8_I2STX-WS_MISO1_MAT2.2
P0.9_I2STX-SDA_MOSI1_MAT2.3
P0.10_TXD2_SDA2_MAT3.0
P0.11_RXD2_SCL2_MAT3.1
P0.15_TXD1_SCK0_SCK
P0.16_RXD1_SSEL0_SSEL
P0.17_CTS1_MISO0_MISO
P0.18_DCD1_MOSI0_MOSI
P0.19_DSR1_SDA1
P0.20_DTR1_SCL1
P0.21_RI1_RD1
P0.22_RTS1_TD1
P0.23_AD0.0_I2SRX-CLK_CAP3.0
P0.24_AD0.1_I2SRX-WS_CAP3.1
P0.25_AD0.2_I2SRX-SDA_TXD3
P0.26_AD0.3_AOUT_RXD3
P0.27_SDA0_USB-SDA1
P0.28_SCL0_USB-SCL1
P0.29_USB-D+
P0.30_USB-D-
46 P0[0]
47 P0[1]
98 P0[2]
99 P0[3]
81 P0[4]
80 P0[5]
79 P0[6]
78 P0[7]
77 P0[8]
76 P0[9]
48 P0[10]
49 P0[11]
62 P0[15]
63 P0[16]
61 P0[17]
60 P0[18]
59 P0[19]
58 P0[20]
57 P0[21]
56 P0[22]
9 P0[23]
8 P0[24]
7 P0[25]
6 P0[26]
25 P0[27]
24 P0[28]
29 P0[29]
30 P0[30]
R56
33R
USB-D+
R55
33R
USB-D-
C51
18p
C52
18p
GNDX GNDX
U7G$8
LPC176X
P1.0_ENET-TXD0
P1.1_ENET-TXD1
P1.4_ENET-TX_EN
P1.8_ENET-CRS
P1.9_ENET-RXD0
P1.10_ENET-RXD1
P1.14_ENET-RX_ER
P1.15_ENET-REF_CLK
P1.16_ENET-MDC
P1.17_ENET-MDIO
P1.18_USB-UP-LED_PWM1.1_CAP1.0
P1.19_MC0A_USB-PPWR-N_CAP1.1
P1.20_MCFB0_PWM1.2_SCK0
P1.21_MCABORT_PWM1.3_SSEL0
P1.22_MC0B_USB-PWRD_MAT1.0
P1.23_MCFB1_PWM1.4_MISO0
P1.24_MCFB2_PWM1.5_MOSI0
P1.25_MC1A_MAT1.1
P1.26_MC1B_PWM1.6_CAP0.0
P1.27_CLKOUT_USB-OVRCR-N_CAP0.1
P1.28_MC2A_PCAP1.0_MAT0.0
P1.29_MC2B_PCAP1.1_MAT0.1
P1.30_VBUS_AD0.4
P1.31_SCK1_AD0.5
95 P1[0]
94 P1[1]
93 P1[4]
92 P1[8]
91 P1[9]
90 P1[10]
89 P1[14]
88 P1[15]
87 P1[16]
86 P1[17]
82 P1[18]
83 P1[19]
84 P1[20]
85 P1[21]
36 P1[22]
37 P1[23]
38 P1[24]
39 P1[25]
40 P1[26]
43 P1[27]
44 P1[28]
45 P1[29]
21 P1[30]
20 P1[31]
U7G$9
LPC176X
P2.0_PWM1.1_TXD1
P2.1_PWM1.2_RXD1
P2.2_PWM1.3_CTS1_TRACEDATA[3]
P2.3_PWM1.4_DCD1_TRACEDATA[2]
P2.4_PWM1.5_DSR1_TRACEDATA[1]
P2.5_PWM1.6_DTR1_TRACEDATA[0]
P2.6_PCAP1.0_RI1_TRACECLK
P2.7_RD2_RTS1
P2.8_TD2_TXD2
P2.9_USB-CONNECT_RXD2
P2.10_EINT0-N_NMI
P2.11_EINT1-N_I2STX-CLK
P2.12_EINT2-N_I2STX-WS
P2.13_EINT3-N_I2STX-SDA
75 P2[0]
74 P2[1]
73 P2[2]
70 P2[3]
69 P2[4]
68 P2[5]
67 P2[6]
66 P2[7]
65 P2[8]
64 P2[9]
53 P2[10]
52 P2[11]
51 P2[12]
50 P2[13]
U7G$10
LPC176X
P3.25_MAT0.0_PWM1.2
P3.26_STCLK_MAT0.1_PWM1.3
27 P3[25]
26 P3[26]
U7G$11
LPC176X
P4.28_RX-MCLK_MAT2.0_TXD3
P4.29_TX-MCLK_MAT2.1_RXD3
82 P4[28]
85 P4[29]
10/100M Ethernet PHY (LAN8720)
I2C-E2PROM
USB pullup for USB Device operation
FB2
BK1608HS220-T
VIO_3V3X
C62
10u
C55
100n
C54
100n
C61
10u
C56
100n
C57
1u
C60
100n
R87
1K5
R90
10K
PHY-address = 1
P1[0]
P1[1]
P1[4]
P1[9]
P1[10]
P1[8]
P1[14]
P1[17]
P1[16]
P1[15]
R77 0R
R78 0R
R79 0R
R80 22R
R81 22R
R82 22R
R83 22R
R84 0R
R85 0R
R86
UL
R89
22R
U9G$1
74LVC1G04GW
REFCLKO
RSTOUT_N
U8
LAN8720A-CP
TXD0
TXD1
TXEN
RXD0/MODE0
RXD1/MODE1
CRS_DV/MODE2
RXER/PHYAD0
MDIO
MDC
NINT/REFCLKO
NRST
LED1/REGOFF
LED2/NINTSEL
VDD1A
VDD2A
VDDIO
VDDCR
TXP
TXN
RXP
RXN
XTAL1/CLKIN
XTAL2
RBIAS
GND
TD+
TD-
RD+
RD-
R68 50R
R69 50R
C58
100n
R70 50R
R71 50R
C59
100n
C64
18p
C65
18p
C66
18p
C67
18p
U9G$2
C50
100n
LED4
RED
LED3
RED
R76 270R
R74 10K
R75 270R
Y4 25MHz
R88 1M
C63
18p
C68
18p
R67 12K1
GNDX
R57
3K3
U11
24LC64
SCL
WP
A2
A1
A0
VCC
SDA
GND
EEPROM
Array
P0[20]
P0[19]
R58
3K3
C53
100n
R73
50R
P2[9]
Q3
BCX17
R72
1K5
USB-D+
(C) Embedded Artists AB
TITLE: LPCXpresso LPC1769 rev B
Document Number:
Date: 2011-02-11 07:09:51
Sheet: 6/7




| mbed | LPCXpresso | |
|---|---|---|
| GND | GND | |
| VIN (4.5-14V) | VIN (4.5-5.5V) | |
| VB (battery supply) | VB (battery supply) | |
| nR (reset) | RESET_N | |
| SPI1-MOSI | P0.9 | MOSI1 |
| SPI1-MISO | P0.8 | MISO1 |
| SPI1-SCK | P0.7 | SCK1 |
| GPIO | P0.6 | SSEL1 |
| UART1-TX / I2C1-SDA | P0.0 | TXD3/SDA1 |
| UART1-RX / I2C1-SCL | P0.1 | RXD3/SCL1 |
| SPI2-MOSI | P0.18 | MOSI0 |
| SPI2-MISO | P0.17 | MISO0 |
| SPI2-SCL / UART2-TX | P0.15 | TXD1/SCK0 |
| UART2-RX | P0.16 | RXD1/SSEL0 |
| AIN0 | P0.23 | AD0.0 |
| AIN1 | P0.24 | AD0.1 |
| AIN2 | P0.25 | AD0.2 |
| AIN3 / AOUT | P0.26 | AD0.3/AOUT |
| AIN4 | P1.30 | AD0.4 |
| AIN5 | P1.31 | AD0.5 |
| | P0.2 | |
| | P0.3 | |
| | P0.21 | |
| | P0.22 | |
| | P0.27 | |
| | P0.28 | |
| | P2.13 | |

| LPCXpresso | | mbed |
|---|---|---|
| VOUT (+3.3V out) if self powered, else +3.3V input | | VOUT (3.3V out) |
| not used | | VU (5.0V USB out) |
| not used | | IF+ |
| not used | | IF- |
| RD- | | RD- (Ethernet) |
| RD+ | | RD+ (Ethernet) |
| TD- | | TD- (Ethernet) |
| TD+ | | TD+ (Ethernet) |
| USB-D- | | D- (USB) |
| USB-D+ | | D+ (USB) |
| P0.4 | CAN_RX2 | CAN-RD |
| P0.5 | CAN_TX2 | CAN-TD |
| P0.10 | TXD2/SDA2 | UART3-TX / I2C2-SDA |
| P0.11 | RXD2/SCL2 | UART3-RX / I2C2-SCL |
| P2.0 | PWM1.1 | PWMOUT0 |
| P2.1 | PWM1.2 | PWMOUT1 |
| P2.2 | PWM1.3 | PWMOUT2 |
| P2.3 | PWM1.4 | PWMOUT3 |
| P2.4 | PWM1.5 | PWMOUT4 |
| P2.5 | PWM1.6 | PWMOUT5 |
| P2.6 | | |
| P2.7 | | |
| P2.8 | | |
| P2.10 | | |
| P2.11 | | |
| P2.12 | | |
| GND | | |



TITLE: LPCXpresso LPC1769 rev B

Document Number:

Date: 2011-02-11 07:09:51 Sheet: 7/7