UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERÍA

CARRERA DE ESPECIALIZACIÓN EN SISTEMAS EMBEBIDOS

MEMORIA DEL TRABAJO FINAL

Punku, control de accesos

Autor:
Ing. Esteban Daniel Volentini

Director:
Ing. Juan Manuel Cruz (FIUBA, UTN-FRBA)

Jurados:
Esp. Ing. Eric Pernia (FIUBA, UNQ)
Esp. Ing. Diego Brengi (INTI)
Esp. Ing. Alejandro Permingeat (FIUBA, USAT-Motion)

Este trabajo fue realizado en la Ciudad de San Miguel de Tucumán, entre marzo de 2019 y marzo de 2020.

Resumen

El presente documento describe el desarrollo de Punku, un equipo destinado a controlar el acceso en una puerta utilizando tarjetas de proximidad. Surge por la necesidad la empresa EQUISER de renovar un equipo existente que hoy resulta obsoleto por los avances de la tecnología. Se espera que el producto desarrollado que brinde más funcionalidad con un costo de fabricación menor al del equipo actual.

El proyecto de desarrollo incluyó la especificación de requisitos, la definición de las pruebas de aceptación, el diseño del hardware contemplando la producción en escala y el desarrollo del firmware utilizando un sistema operativo de tiempo real. Para verificar el correcto funcionamiento del equipo se realizaron pruebas unitarias y de integración automatizadas.

Agradecimientos

Esta sección es para agradecimientos personales y es totalmente **OPCIONAL**.

Índice general

Índice de figuras

Índice de Tablas

Dedicado a... [OPCIONAL]

Capítulo 1

Introducción General

En el presente capitulo se presentan los aspectos generales del trabajo desarrollado y una breve introducción a las tecnologías utilizadas en el mismo.

1.1. Descripción del problema

El control de las personas que acceden a un ambiente es una de las aplicaciones que se benefician desde hace largo tiempo con los avances de la electrónica. El reemplazo de las cerraduras mecánicas y sus correspondientes llaves por sistemas electrónicos lleva mas de 30 años, y continua en plena expansión. Actualmente existe en el mercado una oferta de equipos muy amplia y variada, que utilizan diferente medios para identificar a las personas que intentan acceder. Los métodos de identificación mas difundidos en la actualidad son:

- Clave numérica: para la identificación del usuario se le asigna una clave numérica que se ingresa mediante un teclado que forma parte del equipo. Este esquema es el mas económico pero también el más inseguro ya que la clave puede fácilmente darse a conocer a personas no autorizadas.
- Tarjetas de proximidad: para la identificación se utilizan unos sistemas electrónicos que se alimentan al aproximarlos a un lector y transmiten información que permite identificar al portador. Las tarjetas en realidad pueden adoptar otros formatos como llaveros o etiquetas autoadhesivas. Este esquema resulta más costoso pero también más seguro que el anterior ya que las tarjetas no pueden replicarse fácilmente, aunque si es posible prestarlas a personas no autorizadas.
- Reconocimiento de huella digital: para la identificación se toma una imagen de un dedo del usuario y se reconoce la geometría de las huellas digitales del mismo. Este esquema es el mas costos y seguro de todos, ya que duplicar una huella digital es una tarea realmente compleja.

Independientemente del medio utilizado para la identificación del usuario, todos los equipos tienen una forma de operación y configuración similar, la que puede ser clasificada en tres grandes grupos:

- Equipos autónomos: son los más económicos y fáciles de instalar, ya que solo requieren alimentación y la conexión con el mecanismo que libera la puerta para permitir el acceso. Dentro de este grupo podemos encontrar incluso equipos que se integran dentro de una cerradura tradicional y se alimentan con baterías, lo que simplifica al máximo la instalación de los

mismos. La principal desventaja de este tipo de equipos es la gestión de las personas autorizadas a ingresar. En general estos equipos integran unos teclados muy básicos con los que se pueden agregar y borrar las personas autorizadas mediante secuencias de códigos numéricos bastante poco amigables con los usuarios finales.

- Equipos en linea: son los mas seguros pero también los mas costos y complejos de instalar. Estos equipos incorporan una interfaz de comunicaciones para validar cada operación de acceso con un servidor central en tiempo real. De esta forma la gestión de las personas autorizadas se realiza en forma centralizada sobre dicho servidor mediante un programa informático mucho mas simple de utilizar. Este esquema puede ademas incorporar mayor complejidad en las validaciones efectuadas para autorizar el ingreso de una persona. La principal desventaja de este esquema es que resulta muy sensible a una falla en la red de comunicaciones o en el servidor de autorizaciones.
- Equipos gestionados: son equipos autónomos que incorporan una interfaz de comunicaciones para permitir la gestión de los mismos en una forma más simple. En muchos casos son equipos que pueden ademas operar en linea. Podría pensarse que estos equipo combinan las desventajas de los dos anteriores, pero esto no es verdad. Si bien el costo es mayor que el de un equipo autónomo, no requiere toda la infraestructura de los equipos que operan en linea, lo que disminuye significativamente el costo total de la solución. A cambio de ese aumento en el costo permiten una gestión mas simple ya que es posible utilizar una computadora con un software amigable.

Como se desprende del análisis anterior resulta muy difícil encontrar un equipo adecuado para el mercado hogareño o de pequeñas oficinas. A pesar de que la oferta del mercado es muy amplia no existen mucho equipos que combinen adecuadamente las características de precio con la facilidad de instalación y gestión necesarias en un ambiente donde el usuario final posee conocimientos técnicos muy limitados. Por estas razones la mayoría de los equipos destinados a este mercado corresponden al grupo de los equipos gestionados. Sin embargo la mayoría de los mismos utilizan interfaces de comunicaciones cableadas, las que complican la instalación y permiten la gestión unicamente desde una computadora.

Punku nace como una propuesta de la firma EQUISER para resolver el problema del control de accesos en hogares, pequeñas oficinas, consorcios de departamentos y cocheras. Las características mas importantes de este mercado son la poca cantidad de puertas controladas, falta de personal técnico para la gestión del equipo, y en el caso de los consorcios y cocheras, frecuentes cambios en la lista de personas autorizadas. Para lograr la mejor relación entre seguridad, precio y facilidad de gestión, el equipo puede funcionar con tarjetas de proximidad o con controles remotos. Ademas utiliza una interfaz *Bluetooth* que permite gestionarlo desde un dispositivo móvil, que puede ser una computadora portátil, un teléfono celular inteligente o una tableta. También incorpora una entrada para un sensor que permite detectar la apertura de la puerta, y una salida de alarma para informar cuando la misma permanece abierta por más tiempo del adecuado. En la figura 1.1 se puede ver una imagen del equipo actual con su correspondiente lectora de proximidad.

FIGURA 1.1: Fotografía del equipo actual

En la tabla 1.1 se puede ver un cuadro comparativo del producto actual con otros equipos existentes en el mercado. Como se puede observar la oferta se polariza en dos tipos de equipos: totalmente autónomos gestionados mediante un teclado numérico muy limitado o equipos con conexiones cableadas (ethernet o usb) que solo pueden ser gestionados desde computadoras de escritorio o portátiles. En el mercado internacional si existen equipos que se pueden gestionar desde un dispositivo móvil, pero tampoco en este escenario la oferta es abundante. Por estas razones Punku constituye una solución atractiva que busca imponerse principalmente por la facilidad de manejo por parte del usuario final.

TABLA 1.1: Cuadro comparativo con otros equipos del mercado

Equipo	Tecnología	Forma de gestión	Valor
EQUISER Punku	Proximidad y remotos RF	Gestionado desde un celular usando bluetoth	$ 3.000
Tebas 208NW [1]	Proximidad	Teclado numérico integrado en el equipo	$ 4.000
ZK MA300IS [2]	Proximidad y huellas	Computadora conectada mediante Ethernet	$ 10.000
ANVIZ T5 Pro [3]	Proximidad y huellas	Computadora conectada mediante Ethernet o USB	$ 8.000

1.2. Motivación

En la figura 1.2 se puede observar un diagrama de bloques del equipo que se produce actualmente. En el mismo encontramos dos unidades funcionales:

- La lectora de proximidad: es la responsable de generar la el campo magnético que alimenta a las tarjetas y decodificar la información enviada por estas.
- El procesador: que es el responsable de determinar si la tarjeta leída puede o no acceder, registrar los movimientos de acceso, accionar las salidas para

autorizar el ingreso, supervisar el estado de la puerta y comunicarse con el equipo móvil para permitir gestionar la configuración del mismo.

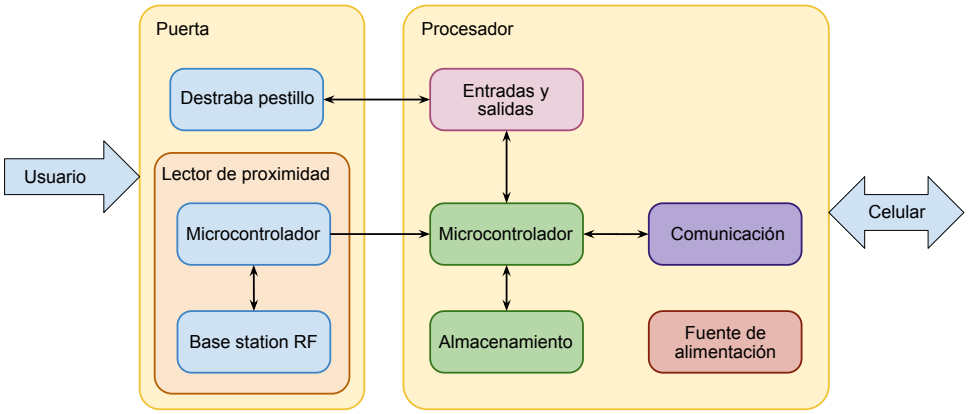

FIGURA 1.2: Diagrama de bloques del equipo actual

La versión en producción del equipo fue diseñada en el año 2013 y los cambios de tecnologías de estos últimos seis años demandaban las siguientes actualizaciones en el diseño del mismo:

- Cambio del procesador principal: para el desarrollo original se utilizó un microcontrolador de la familia *ColdFire* producidos por la empresa *Freescale*. Con el avance de los procesadores *Cortex* el fabricante fue dejando de lado el desarrollo de esta gama de productos, por lo que en este momento el microcontrolador utilizado resulta más costoso que un procesador más nuevo con mayores prestaciones. Lamentablemente no existe una oferta por parte del fabricante de un microcontrolador con una disposición de terminales pensada para efectuar un reemplazo directo del utilizado actualmente.
- Cambio de la interfaz de comunicaciones: el equipo actual utiliza para la comunicación una interfaz *Bluetoth* 2. Poco tiempo después del desarrollo se aprobó la versión 4 de este protocolo, la cual fue adoptado rápidamente por la firma *Apple*. Esta nueva versión del protocolo no es compatible con la anterior, y si bien algunos equipos pueden funcionar en ambos modos de trabajo, este no es el caso de los equipos *iPhone*, donde para privilegiar la duración de la batería solo pueden operar con *Bluetooth* 4.
- Incorporación de un reloj: al comercializar las primeras unidades surgió el requerimiento de algunos clientes para disponer de un registro de acceso con fecha y hora de cada evento. El equipo actual no dispone de un *Real Time Clock* (RTC) que le permita mantener la fecha y hora cuando el mismo no dispone de alimentación eléctrica. De esta forma si bien el equipo registra los eventos con fecha y hora, la misma vuelve a una fecha inicial preestablecida cada vez que se reinicia el mismo, y es necesaria una comunicación desde el celular para reajustar el reloj interno. El resultado es que la mayoría de los registros de accesos no tienen una fecha y hora validas.
- Soporte para cerraduras motorizadas: uno de los principales obstáculos para la instalación de equipos para el control de accesos en el mercado al cual

esta destinado Punku son los cortes de alimentación eléctrica. Según el tipo de cerradura que se utilice, ante una falla de energía la puerta quedará cerrada y no se podrá acceder, o peor aun quedará abierta en forma permanente. Una solución a este problema es combinar una cerradura con llave y un sistema motorizado que permita la liberación y el bloqueo de la puerta por cualquiera de los medios. Para esto el equipo debe poder invertir la alimentación en la salida que controla al motor, y de esta forma poder liberar o bloquear el mecanismo en función del sentido de giro del mismo.

- Gestión desde la nube: con el avance en la conectividad a Internet se volvió más común disponer de equipos que pueden ser gestionados en forma remota. En el caso de un control de accesos siempre resulta atractiva la posibilidad de cambiar el permiso de acceso de una persona en forma inmediata sin necesidad de estar cerca del equipo. El uso de *Bluetooth* como interfaz de comunicaciones resulta un obstáculo para esta funcionalidad por su corto alcance y porque nunca se popularizaron equipos equivalente a los *routers* de *WiFi* que permitan el acceso a Internet utilizando Bluetooth.

1.3. Objetivos y alcance

El objetivo general del trabajo desarrollado fue el diseño y la implementación de un prototipo de una nueva versión del equipo para control de accesos Punku que resuelva los problemas mencionados en la sección 1.2. Los objetivos particulares definidos para el mismo fueron:

1. Diseñar el nuevo equipo utilizando un módulo de la familia ESP-32 del fabricante Espressif, el cual incorpora interfaces de comunicación *Wifi* y *Bluetooth* en las versiones 2 y 4.
2. Agregar al nuevo equipo un circuito integrado RTC con respaldo de batería que le permita mantener la fecha y hora validos cuando se producen interrupciones en el suministro de energía eléctrica.
3. Agregar al nuevo equipo la posibilidad de invertir la polaridad de alimentación en la salida que libera la cerradura de forma tal que se pueda utilizar un sistema motorizado para destrabar la puerta.
4. Mantener las características generales del equipo actual en el nuevo diseño, tratando en lo posible de mejorar aun mas la facilidad de gestión del equipo y de disminuir el costo del mismo.
5. Desarrollar el firmware del equipo desde cero, utilizando un sistema operativo de tiempo real y un diseño modular que permita escalar las funcionalidades del equipo.

El resultado esperado es entonces un prototipo totalmente funcional del equipo, que incorpore las mejoras ya mencionadas acompañado de la siguiente documentación:

1. Diagrama esquemático del equipo con en el programa KiCad.
2. Diseño de la placa electrónica realizada en el programa KiCad.

3. Documento con la especificación de requisitos del firmware según el estandar IEEE-830.
4. Documento con la arquitectura y el diseño detallado del firmware modelado utilizando diagramas UML.
5. Documento con las pruebas de aceptación para validar el correcto funcionamiento del equipo escritas en metalenguaje Gherkin.
6. Código fuente del firmware para el control del equipo con documentación y comentarios adecuados que faciliten la compresión del mismo.

Capítulo 2

Introducción Específica

En el presente capitulo se presentan en mayor profundidad las distintas tecnologías utilizadas en el equipo. A continuación se detallan los requisitos y casos de uso relevados, junto a las pruebas de aceptación definidas para validar el correcto funcionamiento del prototipo. Finalmente se presenta brevemente la planificación del proyecto efectuada oportunamente.

2.1. Tarjetas de proximidad

La identificación por radiofrecuencia o *Radio Frecuency Identification (RFID)* es una tecnología que permite el intercambio de información sin contacto entre un equipo lector y un dispositivo de almacenamiento denominado transpondedor. También denominadas etiquetas RFID, estos dispositivos pueden ser activos si cuentan con alimentación propia, o pasivos si se alimentan del campo electromagnético generado por el equipo lector.

En el ámbito de las sistemas para el control de accesos la mayoría de las etiquetas RFID son pasivas y adoptan la forma de una tarjeta plástica, un llavero o una etiqueta autoadhesiva que contiene el chip electrónico junto con la bobina que cumple la función de antena receptora y transmisora. Las distancias de lectura generalmente son del orden de los 10 cm pero pueden extenderse hasta las 15 metros en los sistemas desarrollados para control de vehículos. En el mercado actual de Argentina podemos encontrar, principalmente, cuatro tipos de tarjetas de proximidad:

- Tarjetas EM4100: son las más económicas y muy difundidas en el control de accesos. Desarrolladas originalmente por la empresa E&M Marine fueron ampliamente copiadas por los fabricantes chinos. Estas tarjetas operan con una portadora de 125 KHz, la que modulan en amplitud para transmitir una trama fija de 64 bits, que transmite un número de serie prefijado en el fabricación de 24 bits.
- Tarjetas HID: son el grupo menos difundido en nuestro país, principalmente por el costo y dificultad para adquirir las mismas. Estas tarjetas operan también con una portadora de 125 KHz, pero la modulan en frecuencia. Existen tres variantes en las tramas transmitidas que serie prefijado en el fabricación de 24 o de 36 bits según la versión de tarjeta.
- Tarjetas MIFARE: son las utilizadas por los sistemas de monederos electrónicos y pagos de pasajes en el transporte público de pasajeros. Fueron

desarrolladas originalmente por la empresa Philips Semiconductors y hoy son mantenidas por NXP Semiconductors. Estas tarjetas tienen la capacidad de proteger la memoria en base a un par de claves criptográficas para impedir la lectura o escritura por parte de equipos no autorizados. Se encuentran comprendidas dentro de la norma emitida por la Organización Internacional de Normalización (ISO) para regular la operación de tarjetas de proximidad (ISO 14443).

- Tarjetas UHF: son las utilizadas en los sistema de telepeaje y sistemas para control vehiculares, porque pueden alcanzar distancias de lecturas de hasta 15 metros. Estas tarjetas también tienen la capacidad de proteger la memoria utilizando criptografía para impedir la lectura o escritura por parte de equipos no autorizados. Se encuentran normalizadas por la Organización Internacional de Normalización (ISO) para regular la operación de tarjetas de sin contacto de largo alcance (ISO 18000-6C).

En la tabla 2.1 se puede observar un cuadro comparativo entre los distintos tipos de tarjetas de proximidad utilizadas en los sistemas para control de accesos. De estas opciones de decidió que el nuevo opere con el estándar MIFARE, lo que permite utilizar todas las tarjetas de pago electrónico para el transporte publico como medio de identificación y acceso, disminuyendo de esta forma la inversión inicial de la instalación.

TABLA 2.1: Cuadro comparativo con las tarjetas de proximidad más utilizadas para el control de accesos

Nombre	Frecuencia	Distancia	Capacidades
EM4100	125 KHz / ASK	10 a 15 cm	Solo lectura
HID	125 KHz / FSK	10 a 15 cm	Solo lectura
MIFARE	15.56 KHz /ASK	10 a 30 cm	Lectura/Escritura
UHF	850 a 915 MHz /ASK	Hasta 15 m	Lectura/Escritura

2.2. Protocolos inalámbricas

El aumento del uso de dispositivos móviles con un poder de computo cada vez mayor por parte del publico en general abre la puerta a nuevas aplicaciones para estos equipos. En particular para el trabajo desarrollado, la intención es utilizar un dispositivo móvil como un teléfono inteligente o una tableta, para gestionar y configurar el equipo para control de accesos. Para esto es necesario que la interfaz de comunicaciones implementada sea del tipo inalámbrica, ya que si bien es técnicamente posible utilizar una interfaz USB cableada para conectarse a la mayoría de teléfono o tabletas, esta opción no resultaría cómoda ni comercialmente atractiva. En la actualidad dos protocolos de comunicación inalámbricos dominan el mercado:

- Bluetooth: es un protocolo diseñado para una red de área personal, con un alcance típico de 10 metros, con bajas tasas de transferencias y optimizado para extender la duración de las baterías. Existen dos versiones principales de este protocolo: la versión 2 y la 4, las cuales no son compatibles entre si. La mayoría de los dispositivos móviles actuales soportan ambas versiones

del protocolo, excepto todos los equipos móviles de la firma Apple, que solo soportan la versión 4 de bajo consumo. En este protocolo la conexión se realiza entre un maestro y un esclavo, y si bien teóricamente se pueden generar redes de dispositivos en la practica esto nunca se implementa.

- WiFi: es un protocolo diseñado para una red de área local, con un alcance típico de 100 metros y altas tasas de transferencias. Existen varias versiones de este protocolo, las cuales se pueden agrupar en dos familias: las que utilizan una portadora de 2.4 GHz y las de 5 GHz. Las versiones mas nuevas pueden utilizar ambas frecuencias simultáneamente para aumentar aun más el ancho de banda. En este protocolo la conexión se realiza generalmente entre un dispositivo y un punto de acceso, que normalmente brinda conexión con una red mayor y eventualmente con Internet.

En la tabla 2.2 se puede ver un resumen con las características mas importantes de las diferentes variantes de ambos protocolos de comunicación. Para el desarrollo del equipo se decidió utilizar WiFi, de esta forma resulta igual de sencillo establecer una conexión punto a punto entre dispositivo móvil y el equipo que se quiere gestionar, como conectarlo a la red existente en el lugar y gestionarlo desde cualquier ubicación que tenga conexión con dicha red. Incluso permite en un futuro el acceso a Internet del equipo, lo que permitiría la gestión del mismo desde cualquier lugar del mundo.

TABLA 2.2: Cuadro comparativo entre las diferentes variantes de los protocolos Wifi y Bluetooth

Nombre	Alcance	Frecuencia	Velocidad
Bluetooth 2.0	10 metros	2,4 GHz	2 MBits/s
BLE	10 metros	2,4 GHz	2 MBits/s
Wifi 802.11a	100 metros	5 GHz	54 MBits/s
Wifi 802.11b	100 metros	2,4 GHz	11 MBits/s
Wifi 802.11g	100 metros	2,4 GHz	54 MBits/s
Wifi 802.11n	100 metros	2,4 y 5 GHz	600 MBits/s

La utilización de la interfaz WiFi implica casi inevitablemente el uso del conjunto de protocolos TPC/IP, lo que permite disponer de una serie de opciones estandarizadas para la capa de aplicación del protocolo de gestión y configuración del equipo. De estas opciones disponibles se decidió implementar una interfaz Full REST Api utilizando el protocolo HTTP. El motivo de esta elección fue simplificar la comunicación con aplicaciones híbridas para celulares, como se explica en la sección 2.3 y paginas WEB, lo que también permitirá en un futuro la gestión del equipo desde Internet

2.3. Aplicaciones para dispositivos móviles

El mercado de los dispositivos móviles se encuentra polarizado en dos sistemas operativos: Android e iOS. Lamentablemente las herramientas de desarrollo e incluso los lenguajes utilizados por cada plataforma son totalmente incompatibles, esto significa que para desarrollar una aplicación que se encuentre disponible para ambas plataformas requiere el doble de esfuerzo.

Una solución a este problema son las denominada aplicaciones híbridas, las cuales en realidad son paginas WEB encapsuladas en una con el correspondiente navegador de cada plataforma en una aplicación nativa. Estas aplicaciones se desarrollan entonces en JavaScript y uno de los entornos de desarrollo más difundidos para este tipo de aplicaciones es el conjunto Ionic Cordoba, el cual permite desarrollar una aplicación para móviles utilizando exclusivamente tecnología web.

Dado que en realidad estas aplicaciones son paginas web tienen una serie de restricciones, principalmente en las comunicaciones que pueden realizar y en la interacción con los dispositivos del equipo móvil como la cámara o el GPS. Algunas de estas restricciones son resueltas utilizando *plugins*, fragmentos de código nativo escrito para cada plataforma que funcionan a modo de adaptador para que la pagina web pueda acceder a estos servicios.

La forma más natural de comunicación para este tipo de aplicaciones es utilizando conexiones HTTP para enviar o recuperar objetos codificados según el estándar JSON. Por esta razón, y aun cuando el desarrollo de la aplicación de gestión para el dispositivo móvil esta fuera de los alcances del trabajo, se decidió implementar toda la gestión del equipo utilizando esta tecnología.

2.4. Características del equipo

Dado que el objetivo del trabajo fue el diseño de un equipo comercial se planteó la necesidad de permitir que el mismo pueda adaptarse a diferentes instalaciones. La primera de las opciones de instalación corresponde al tipo de dispositivo que se utiliza para impedir la apertura de la puerta. En este apartado podemos encontrar dos opciones:

- Destraba pestillo eléctrico: es un sistema mecánico que actúa como traba para el pestillo de la puerta. Este se libera al energizar una bobina y que por la acción de un resorte vuelve a bloquearse automáticamente cuando se retira la energía eléctrica. De esta forma mientras el mismo permanece energizado es posible abrir la puerta.
- Cerradura electromagnética: es simplemente un electroimán que cuando permanece alimentado ejerce una fuerza que impide la apertura de la puerta. En este caso la puerta puede abrirse únicamente cuando la cerradura permanece sin alimentación
- Cerradura motorizada: en este caso el sistema mecánico de bloqueo es accionado por un motor en lugar de por una bobina. Para liberar la puerta es necesario alimentar el motor con una determinada polaridad por un tiempo determinado, o hasta que acciona un sensor que detecta el final del recorrido del mecanismo. En este caso la puerta permanece liberada hasta que se alimenta el motor con la polaridad contraria durante un tiempo determinado, o hasta que se acciona un nuevo sensor que detecta el final del recorrido en el sentido contrario al inicial

Como se puede deducir de la descripción anterior cada tipo de cerradura requiere una señal de control diferente. En particular la mayor diferencia esta dada entre los sistemas electromecánicos y los motorizados, debido a la necesidad de una inversión en la alimentación para efectuar el bloque de la puerta.

La otra opción de instalación que podrá definir el usuario final corresponde al uso de un sensor para detectar la apertura de la puerta. En el diseño del equipo se contempla la posibilidad de utilizar este sensor para poder determinar si una persona autorizada ingresa al espacio controlado, y para ademas informar mediante una señal de alarma cuando la puerta permanece abierta por mas tiempo del adecuado. De una análisis rápido resulta claro que el comportamiento del equipo debe ser diferente cuando el usuario decide no instalar el sensor para determinar la apertura de la puerta.

La combinación de las dos opciones antes analizadas determina cuatro modos de funcionamiento principales, los cuales se resumen en la tabla 2.3.

TABLA 2.3: Resumen de los modos de funcionamiento del equipo en función la cerradura y la instalación del sensor de puerta.

Cerradura	Sensor	Forma de operación
Electromagnética	Sin instalar	Se libera la cerradura, cambiando el estado de la alimentación, por un tiempo predefinido. Al finalizar el mismo se bloquea la cerradura volviendo la alimentación al estado inicial.
Electromagnética	Instalado	Se libera la cerradura, cambiando el estado de la alimentación, hasta detectar la apertura de la puerta sin exceder un tiempo máximo predefinido. Se supervisa que la puerta no permanezca abierta por mas de tiempo máximo
Motorizada	Sin instalar	Se libera la cerradura alimentando el motor por un tiempo predefinido. Al finalizar el mismo la puerta permanece liberada por un tiempo máximo. Al terminar el mismo se bloquea la cerradura alimentando el motor con polaridad inversa durante el mismo tiempo que al inicio.
Motorizada	Instalado	Se libera la cerradura alimentando el motor por un tiempo predefinido. Al finalizar se supervisa la apertura y cierre de la puerta. Al detectar la apertura de la puerta, o exceder un tiempo máximo, se bloquea la cerradura alimentando el motor con polaridad inversa durante el mismo tiempo que al inicio.

2.4.1. Requisitos del equipo

Uno de los primeros puntos que detalla el estándar IEE-830 para especificación de requisitos son las interfaces externas de la aplicación. Dado que el desarrollo analizado corresponde al firmware de un sistema embebido las interfaces del software tienen relación directa con las entradas y salidas de la placa electrónica. En la tabla 2.4 se detallan las interfaces de entradas y salidas que debe implementar el nuevo equipo, y que por lo tanto constituyen las interfaces de firmware del mismo.

TABLA 2.4: Lista de entradas y salidas del requeridas en el equipo

Nombre	Tipo	Descripción
PNK-ES001	Puerto SPI	Circuito integrado del lector RFID
PNK-ES002	Entrada digital opto-aislada	Sensor de puerta abierta
PNK-ES003	Salida digital con inversión de polaridad	Actuador de la cerradura de puerta
PNK-ES004	Entrada digital sin aislación	Sensor de cerradura liberada
PNK-ES005	Entrada digital sin aislación	Sensor de cerradura bloqueada
PNK-ES006	Entrada digital opto-aislada	Pulsador para apertura manual
PNK-ES007	Salida digital de contacto seco	Salida de alarma
PNK-ES008	Salida modulada en frecuencia	Indicador sonoro para el usuario
PNK-ES009	Salida digital con inversión de polaridad	Indicador luminoso para el usuario

Como se explicó en el inicio de la sección 2.4 uno de los requerimientos importantes del equipo es poder configurar el comportamiento del mismo para adaptarlo a diferentes tipos de instalaciones. Por esta razón se decidió identificar cada uno los parámetros de configuración requeridos para lograr la capacidad de personalización desea. La lista de parámetros definidos puede verse en la tabla 2.5.

Se detallan las restricciones impuestas por el cliente el proceso de desarrollo, materiales y características del equipo a desarrollar

2.4.2. Casos de uso

Se describen los casos de uso principales del equipo

2.4.3. Pruebas de aceptación del equipo

Se detallan las pruebas a ejecutar una vez terminado el equipo para considerar el desarrollo del mismo como completo

2.5. Planificación

Análisis inicial del proyecto

Se listan las tareas que se deben desarrollar para completar el proyecto con una breve descripción para cada una

Se listan los recursos necesarios y los periodos de tiempo en los cuales los mismos deberán estar disponibles para el desarrollo del equipo

TABLA 2.5: Lista de parámetros para configurar el comportamiento del equipo según las opciones de instalación

Nombre	Tipo y Rango	Descripción
PNK-PO001	Númerico100ms a 2.500ms	Tiempo de accionamiento del indicador luminoso PNK-ES009 cuando se produce la lectura de una tarjeta
PNK-PO002	100ms a 2.500ms	Tiempo de accionamiento del indicador sonoro PNK-ES008 cuando se concede el acceso a una tarjeta
PNK-PO003	100ms a 2.500ms	Tiempo de accionamiento del indicador sonoro PNK-ES008 cuando se deniega el acceso a una tarjeta
PNK-PO004	1s a 10s	Tiempo máximo que la puerta permanece liberara para permitir la apertura de la misma
PNK-PO005	100ms a 2.500ms	Tiempo máximo de accionamiento del motor en cerraduras motorizadas
PNK-PO006	1s a 60s	Tiempo máximo que la puerta puede permanece abierta antes de generar una señal de alarma
PNK-PO007	0 ó 1	El sensor de puerta abierta se encuentra conectado
PNK-PO008	0 ó 1	El sistema de liberación de la puerta requiere inversión de polaridad
PNK-PO009	0 ó 1	El sistema de liberación de la puerta dispone de sensor para indicar el estado del mismo

TABLA 2.6: Requisitos funcionales para el control de accesos

Nombre	Característica
Elemento	Valor

Se presenta el análisis de riesgos efectuado al iniciar el proyecto

Se presenta la planificación realizada al iniciar el desarrollo del equipo

FIGURA 2.1: Fotografía del equipo actual

De aquí en adelante solo esta la estructura del documento

TABLA 2.7: Requisitos funcionales para el accionamiento de los actuadores

Nombre	**Característica**
Elemento	Valor

TABLA 2.8: Requisitos funcionales para la gestión del equipo

Nombre	**Característica**
Elemento	Valor

TABLA 2.9: Restricciones impuestas por el cliente en el desarrollo de hardware

Nombre	**Característica**
Elemento	Valor

TABLA 2.10: Restricciones impuestas por el cliente en el desarrollo de firmware

Nombre	**Característica**
Elemento	Valor

TABLA 2.11: Caso de uso Acceso por pulsador

Nombre	**Característica**
Elemento	Valor

TABLA 2.12: Caso de uso Acceso por tarjeta de proximidad

Nombre	**Característica**
Elemento	Valor

TABLA 2.13: Caso de uso Configuración del equipo

Nombre	**Característica**
Elemento	Valor

TABLA 2.14: Caso de uso Gestión de las personas autorizadas

Nombre	**Característica**
Elemento	Valor

TABLA 2.15: Caso de uso Consulta de la bitácora de accesos

Nombre	**Característica**
Elemento	Valor

FIGURA 2.2: Fotografía del equipo actual

TABLA 2.16: Lista del desglose de tareas del proyecto

Nombre	**Característica**
Elemento	Valor

TABLA 2.17: Lista de recursos requeridos por el proyecto

Nombre	**Característica**
Elemento	Valor

TABLA 2.18: Tabla de riesgos mitigados del proyecto

Nombre	**Característica**
Elemento	Valor

Capítulo 3

Diseño e Implementación

Párrafo introductorio.

3.1. Diseño del hardware

Bloques constructivos del hardware, se presenta el diagrama de bloques y se describen los mismos

FIGURA 3.1: Diagrama de bloques del equipo desarrollado

Selección de los componentes, se presentan los criterios utilizados para en la selección de los componentes.

3.2. Prototipo del hardware

Diseño y construcción de la placa electrónica, se presentan los criterios y el proceso utilizado para el diseño y construcción de la placa electrónica del prototipo.

Montaje del prototipo, se detallan los problemas de construcciones del primer prototipo y se mencionan las correcciones en el diseño de la placa electrónica efectuadas a partir de los problemas de montaje de los componentes.

FIGURA 3.2: Errores encontrados durante el montaje del primer prototipo

3.3. Diseño del firmware

3.3.1. Arquitectura del firmware

Se presenta la arquitectura seleccionara para el firmware del equipo, se presenta el diagrama de componentes de software del mismo y se describen brevemente las capas del mismo

FIGURA 3.3: Diagrama de componentes del firmware del equipo

FIGURA 3.4: Diagrama de clases del firmware del equipo

3.3.2. Capa de abstracción del hardware

Se describen las clases que componen la capa de abstracción de hardware

3.3.3. Capa de controladores

Se describen las clases que componen la capa de controladores

FIGURA 3.5: Diagrama de estado para el control de una puerta, sin sensor de apertura y con liberación electromagnética

FIGURA 3.6: Diagrama de estado para el control de una puerta, con sensor de apertura y con liberación electromagnética

3.3.4. Tareas del sistema

Se describen las tareas del sistema operativo de tiempo real y las interacciones entre las mismas.

3.4. Desarrollo del firmware

3.4.1. Entorno de desarrollo

Se describen las herramientas utilizadas para el desarrollo del software

3.4.2. Uso del tipo de abstracto de datos

Se presenta el patrón de programación denominado tipo abstracto de datos y se explica su uso en la implementación del firmware del equipo

3.4.3. Pruebas de integración en las tareas del sistema

Se presenta la problemática de implementar pruebas automatizadas en tareas del sistema operativo FreeRTOS y se explica la herramienta desarrollada para resolver este problema

FIGURA 3.7: Diagrama de estado para el control de una puerta, sin sensor de apertura y con liberación motorizada

FIGURA 3.8: Diagrama de estado para el control de una puerta, con sensor de apertura y con liberación motorizada

FIGURA 3.9: Diagrama de secuencia para la liberación por pulsador de una puerta, sin sensor de apertura y con liberación electromagnética

FIGURA 3.10: Diagrama de secuencia para la apertura y cierre por tarjeta de proximidad, con sensor de apertura y con liberación electromagnética

FIGURA 3.11: Diagrama de secuencia para la activación de alarma por apertura forzada de la puerta

FIGURA 3.12: Diagrama de secuencia para el cambio de configuración del equipo

TABLA 3.1: Lista de las herramientas utilizadas para el desarrollo del firmware

Nombre	**Característica**
Elemento	Valor

Capítulo 4

Ensayos y Resultados

Párrafo introductorio.

4.1. Pruebas funcionales del hardware

4.2. Prototipo del hardware

Mediciones y verificaciones en el prototipo, se detallan las mediciones y ensayos realizados sobre la placa del prototipo para determinar su correcto funcionamiento

Correcciones en el prototipo: Se detallan los errores encontrados en el diseño y las correcciones efectuadas a partir de los ensayos funcionales en la placa del prototipo"

FIGURA 4.1: Imagen con el error en la definición del encapsulado del reloj de tiempo real

FIGURA 4.2: Imagen con la corrección efectuada en la placa de prototipo

4.3. Pruebas en el firmware

4.3.1. Pruebas unitarias

Se describen las pruebas unitarias implementadas y los resultados obtenidos

4.3.2. Pruebas de integración

Se describen las pruebas de integración implementadas y los resultados obtenidos

4.3.3. Resultados de las pruebas de aceptación del equipo

Se analizan los resultados obtenidos al ejecutar las pruebas de aceptación definidas al inicio del proyecto

4.4. Resultados

Métricas del firmware desarrollado: se presentan métricas para evaluar la calidad del software desarrollado

TABLA 4.1: Tabla resumen con las métricas de calidad obtenidas para el firmware desarrollado

Equipo	**Valor**
Punku	$ 3.000

Comparaciones con productos existentes: se repite la comparación de las prestaciones de los equipos existentes con el equipo anterior y con el nuevo equipo desarrollado en función de los resultados obtenidos

TABLA 4.2: Cuadro comparativo del equipo actual con el anterior y con otros equipos del mercado

Equipo	**Valor**
Punku	$ 3.000

Comparaciones de los riesgos planificados con el resultado del proyecto: se analizan los resultados obtenidos por las acciones destinadas a mitigar los riesgos identificados en la planificación del proyecto

Capítulo 5

Conclusiones

5.1. Resultados Obtenidos

Se presentan brevemente los objetivos del proyecto y las características esperadas del equipo y se contrastan con los resultados obtenidos

5.2. Trabajo Futuro

Se presentan las ampliaciones en la funcionalidad del equipo en un futuro cercano

Bibliografía

[1] Mercado Libre. *Control de acceso TEBAS 208NW*. URL: https://articulo.mercadolibre.com.ar/MLA-782128833-control-acceso-pestillo-electrico-cerradura-puerta-kit-ls-_JM (visitado 15-03-2020).

[2] Mercado Libre. *Control de acceso ZK MA300*. URL: https://articulo.mercadolibre.com.ar/MLA-799230606-control-de-acceso-biometrico-zkteco-huella-tarjeta-personal-_JM (visitado 15-03-2020).

[3] Mercado Libre. *Control de acceso ANVIZ T5-Pro*. URL: https://articulo.mercadolibre.com.ar/MLA-744676463-anviz-t5-pro-control-de-acceso-por-huella-anviz-t5pro-_JM (visitado 15-03-2020).