MAURÍCIO PERES RAMOS

CONTROLE DE ACESSO BIOMÉTRICO

FLORIANÓPOLIS, 2012

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
CAMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
PÓS-GRADUAÇÃO EM DESENVOLVIMENTO DE SISTEMAS ELETRÔNICOS

MAURICIO PERES RAMOS

CONTROLE DE ACESSO BIOMÉTRICO

Projeto apresentado como pré-requisito para a conclusão do Curso de Especialização em Desenvolvimento de Produtos Eletrônicos do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Orientador: Prof. Charles Borges de Lima, Dr. Eng.

Florianópolis, 2012

CDD 621.382
R175c

Ramos, Maurício Peres
Controle de acesso biométrico [MP] / Mauricio Peres Ramos; orientação de Charles Borges de Lima. – Florianópolis, 2012.

1 v. : il.

Monografia de Pós-Graduação (Desenvolvimento de Sistemas Eletrônicos) – Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Inclui referências.

1. Biometria. 2. Controle. 3. Engenharia. I. Lima, Mauricio Peres. II. Título.

Sistema de Bibliotecas Integradas do IFSC
Biblioteca Dr. Hercílio Luz – Campus Florianópolis
Catalogado por: Ana Paula F. Rodrigues Pacheco CRB 14/1117

CONTROLE DE ACESSO BIOMÉTRICO

MAURICIO PERES RAMOS

Este trabalho foi julgado adequado para obtenção do Título de Especialista em Desenvolvimento de Sistemas Eletrônicos e aprovado em sua forma final pela banca examinadora do Curso de Pós-graduação em desenvolvimento de sistemas eletrônicos do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis, 20 de dezembro de 2012

Banca Examinadora

_____

Charles Borges de Lima, Dr. Eng.

_____

Everton Luiz Ferret dos Santos, M. Eng.

_____

Leandro Schwartz, M. Eng.

AGRADECIMENTOS

Agradeço primeiramente a meus familiares, por nunca medirem esforços para me ajudar e pelo apoio incondicional nas horas difíceis.

Ao coordenador do Curso de Especialização em Desenvolvimento de Produtos Eletrônicos André Luís Dalcastagnê, por concebeu diversas oportunidades para que este trabalho fosse finalizado.

Ao meu orientador Charles Borges de Lima que apesar das grandes dificuldades que tive em manter contato permaneceu me apoiando e me aconselhando para a defesa da banca.

Aos meus amigos e companheiros de trabalho Lucas Marcon Trichez e Sergio de Oliveira que durante todo o decorrer do trabalho me apoiaram dando força a prosseguir e alcançar os meus objetivos.

“Por vezes sentimos que aquilo que fazemos não é senão uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota”.

Madre Teresa de Calcuta.

RESUMO

O presente trabalho descreve o projeto de um equipamento destinado ao controle de acesso através de identificação biométrica. Com uma configuração simplificada serviu como objeto de estudo preliminar com o intuito de realizar a confecção de um protótipo funcional. O estudo foi dividido em quatro etapas para uma melhor compreensão sobre o sistema. Primeiramente, definiu-se o escopo do produto de forma a ter uma visão mais clara e objetiva. Para isso foram utilizadas técnicas de engenharia de software que proporcionaram uma análise minuciosa do sistema. Posteriormente, ouve a etapa de definição dos módulos do hardware. Em seguida, foi realizado um estudo para definir o projeto mecânico utilizado. Finalmente, o projeto foi finalizado com o desenvolvimento do firmware do equipamento. Como antes, prosseguiu-se a utilização de conceitos de engenharia de software com o intuito de desenvolver um software com maior qualidade e visando a portabilidade do sistema. Este trabalho permitiu, através da compilação dos resultados obtidos, ampliar a visão da solução onde foi possível identificar pontos para melhoria e implementações futuras. Sendo assim, este trabalho pode servir de referência para o autor para o desenvolvimento de um controle de acesso mais avançado tecnologicamente para a empresa HDL da Amazônia Indústria Eletrônica Ltda. Visando tornar este um produto comercial diferenciado no mercado.

Palavras-chave: Biometria. Controle. Engenharia. Firmware. Hardware.

ABSTRACT

The present work describes the design of a device designed to control access through biometric identification. With simplified configuration served as the primary object of study in order to accomplish the construction of a functional prototype. The study was divided into four steps to a better understanding of the system. First, we defined the scope of the product in order to have a clearer vision and objective. For this we used software engineering techniques that provided a thorough analysis of the system. Later, he hears the step of defining the hardware modules. Then a study was conducted to define the mechanical design used. Finally, the project was completed with the development of firmware device. As before, we continued to use concepts of software engineering in order to develop software with higher quality and portability of the system. This work enabled by compiling the results, expand the vision of the solution where it was possible to identify points for improvement and future implementations. Therefore, this work can serve as a reference for the author to develop an access control most technologically advanced company for HDL Amazon Electronics Industry Ltda. Aiming to make this a commercial product differentiated market.

Keywords: Biometrics. Control. Engineering. Firmware. Hardware.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ASCII – American Standard Code for Interchange of Information

CER – Crossover Error Rate – Taxa de Intersecção de Erros

DAC - Digital-to-Analog Converter

Dpi – Dots per inch.

DSP - Digital Signal Processing.

DX - Deal Extreme

EC – Emissor Comum

EEPROM - Electrically-Erasable Programmable Read-Only Memory

FAR – False Acceptance Rate

FRR – False Rejection Rate

Hz – Hertz

I2C - 2-Wire Serial

IBG. - International Biometric Group

IDE – Integrated Development Environment

K – kilo

M – Mega

MB – Megabyte

mm – milímetro

OEM - Original Equipment Manufacturer

PLL – Phase Locked Loop

REF – Requisito Funcional

RFID - Radio-Frequency IDentification

s – segundo(s)

SD-Card - Secure Digital Card

SPI – Serial Peripheral Interface

UART - Asynchronous Receiver/ Transmitter

uC – microcontrolador

V – Volts

W – Watts

SUMÁRIO

1 INTRODUÇÃO

A necessidade do ser humano pela identificação data desde os primórdios da humanidade. Há diversas evidências, desde a antiguidade, do interesse humano pela busca de uma ferramenta individualizante. Egípcios e gregos estudavam e observavam a relação das diversas partes do corpo. Achados arqueológicos, localizados na região do Turquestão, evidenciam a utilização da digital como forma de autenticação de acordos, através de placas cerâmicas com os dizeres: "'Ambas as partes concordam com estes termos que são justos e claros e afixam as impressões dos dedos que são marcas inconfundíveis'" (Wikipédia, 2012). Existem diversas referências sobre a identificação de indivíduos através de suas características físicas ou parâmetros mensuráveis como altura, cor dos olhos, marcas, cicatrizes, etc.

Muitos países adotavam como forma de marcar ladrões a mutilação de uma parte do corpo, como a mão ou a marcação por ferro quente, entretanto, métodos extremos como estes desapareceram da maioria dos países na primeira metade do século XVIII com o surgimento dos sistemas de leis criminais. Com estes sistemas de leis vigorando criminosos reincidentes sofriam punições mais severas, fato que levava os mesmos a omitir seus delitos anteriores assumindo falsas identidades. Com o passar do tempo ficou notório que muitos delinquentes eram julgados como primários já que não se existia um método de identificação eficaz, desta forma, a sociedade começou a ter a necessidade de estigmatizar os criminosos.

Marcello Malphighi, professor de anatomia da Universidade de Bolonha, Itália, utilizando o recém-inventado microscópio por Antonie van Leeuwenhoek (1632 - 1723), realizou estudos sobre a superfície da pele onde se observou, na região do dedo, a existência de cumes elevados dos quais descreveu sendo " 'da laçada a espirala' "(Wikipédia, 2012).

Posteriormente, já no século XIX, foram realizadas intensas pesquisas relacionadas à criminalística com o intuito de relacionar 12 características físicas com tendências criminais o que resultou na invenção de diversos dispositivos de

mensuração além da coleta de diversas informações. Entretanto, os resultados destas pesquisas não foram conclusivos.

Em 1823, outro professor de anatomia, agora da Universidade de Breslau, um tcheco chamado Johannes Evangelista Purkinji publicou uma tese na qual mencionava nove padrões de impressões digitais. Até então, apesar dos temas de pesquisa correlacionados, nenhum deles apresentava seu foco de pesquisa na busca por uma ferramenta de identificação.

Então, finalmente em 1879, o francês Alphonse Bertillon desenvolveu um método científico de identificação, o qual foi amplamente aceito, chamado de Antropometria também conhecido por Bertillonage em homenagem ao seu criador. Este método se baseava na combinação de medidas físicas que deveriam ser coletadas através de procedimentos prescritos e precisos formando um sistema de identificação humana complexo, mas completo. Dentre as informações captadas neste método, associado às medições físicas, somava-se descrições, sinais particulares, fotos do identificado de perfile e frente e posteriormente em 1894, foram introduzidas à impressão digital. Contudo, a impressão digital, no método de Bertillonage, se representava como um entre outros elementos de identificação visto que a chave deste método é baseada na antropometria.

Paralelamente, aos trabalhos de Alphonse Bertillon, um cirurgião britânico chamado Henry Faulds realizou estudos sobre impressões digitais como meio de identificação o que resultou na criação de um método de classificação. A partir de um artigo de Faulds em 1880, sobre impressões digitais e sua utilização como meio de identificação pessoal, surge o método de utilização de tinta de impressora como meio de extração da impressão, método este que perdurou até os dias atuais.

Através dos estudos de Faulds e Herschel, outro estudioso do assunto, Francis Galton, antropólogo britânico, iniciou seus trabalhos e em 1892 publicou seu livro chamado “Impressões digitais”. Este livro possuía o primeiro sistema de classificação de impressões digitais, no qual, três padrões básicos de impressões digitais eram classificados alfabeticamente: laçada, arqueada e whorl (verticilo). Estes eram distribuídos entre os dedos das mãos sendo que cada dedo adotava uma classificação. Com seus estudos, Galton provou cientificamente que as impressões

digitais não se alteram no curso da vida do indivíduo e que as impressões não são exatamente iguais entre si.

> Galton identificou também as características pelas quais podem ser identificadas as impressões digitais. Estas características são as mesmas usadas hoje, e freqüentemente chamadas de detalhes de Galton. (Marcico. Disponível em: http://www.papiloscopia.com.br/historia.html. Acesso em: 10 de dez. 2012).

Todas estas pesquisas sobre a impressão digital e sobre a mensuração de características físicas prosseguiram e se transformaram em métodos internacionais utilizados para a identificação e verificação. Devido a essa diversidade de estudos realizados e frequentes debates surgiram diversos critérios utilizados para a verificação de uma impressão digital em torno do mundo, nos quais, cada país adota o seu.

O fascínio desta tecnologia e a sua possibilidade de estabelecer a identidade e reforçar a segurança. O avanço das tecnologias e da eletrônica e principalmente dos processamentos, levou ao pensamento das organizações a possibilidade de automatizar o processo de verificação e identificação da impressão digital.

A tecnologia biométrica, antes com um status de restrita a utilizações de segurança militar ou alto valor agregado, hoje ganhou popularidade e sua utilização é presente em diversos escopos de projeto como em aviões, bancos, prédios, sistemas de pagamento, redes de computadores, no processo eleitoral brasileiro, embarque de passageiros em aeroporto, e recentemente no novo registro de identificação brasileiro. Todas estas áreas de aplicação da tecnologia biométrica tem em comum a suscetibilidade a brechas de segurança, fato que determinou a escolha desta tecnologia de forma a minimizar esta característica.

Em paralelo ao desenvolvimento da identificação por digital, foram desenvolvidos e já estão presentes na atualidade, outros métodos biométricos. Nota-se na atualidade um avanço nas pesquisas utilizando biometria através de escaneamento de íris e reconhecimento facial, principalmente pela ausência de

contato com o usuário. Muitos destes métodos tiveram e tem suas pesquisas e desenvolvimento impulsionados por necessidades militares e de segurança.

As organizações em geral, cada vez mais utilizam os métodos biométricos nos seus sistemas de informação, áreas de segurança e controle de pessoas com o intuito de proporcionar uma maior segurança, conforto e confiabilidade aos seus usuários.

Em sua essência, os métodos de segurança são baseados em três conceitos fundamentais: segurança baseada em algo físico, algo que você possui (uma chave), segurança baseada em algo de seu conhecimento (uma senha) ou segurança com base em quem você é. Entretanto, um objeto físico, como a chave ou uma informação, como uma senha, podem ser facilmente compartilhados, perdidos ou até mesmo roubados. Já o conceito de segurança baseada em quem somos não permite sua duplicação ou sua perda pelos usuários ou até mesmo que sejam roubadas. Aliado a isso, o conforto proporcionado aos usuários que não mais necessitam carregar consigo algo físico como cartões ou chaves e não mais necessitam recordar de senhas proporcionam um nível mais elevado de segurança comparado aos demais.

No mercado brasileiro há diversos equipamentos direcionados a aumentar o nível de segurança de um local. Dentre eles os controles de acesso apresentam destaque sendo oferecidos em diversos formatos e composições. As empresas pertencentes a este nicho de mercado vêm buscando aos poucos inserir em seu portfólio equipamentos com tecnologia biométrica, visto que produtos biométricos atingem os mais altos níveis de segurança.

Entre os equipamentos existentes no mercado, baseados em tecnologia biométrica, são mais presentes os de reconhecimento por impressão digital, contudo os de reconhecimento facial vêm ganhando espaço, sobretudo por não necessitarem de contato físico com o usuário.

FIGURA 1 - Control de acesso com reconhecimento facial.

FONTE: BIOMETRUS, 2012.

Os produtos voltados a controle de acesso, como o da figura 1, geralmente possibilitam outros meios de identificação como leitores de cartões magnéticos, leitores RFID ou teclados para entrada de senhas. Mas nem sempre esses produtos são oferecidos com opções modulares, sendo desta forma, ofertados no formato de equipamentos de uma linha como mostra a figura 2. Além disso, muitos dos fabricantes operam na modalidade *Original Equipment Manufacturer* (OEM), importando os equipamentos e simplesmente inserindo sua marca.

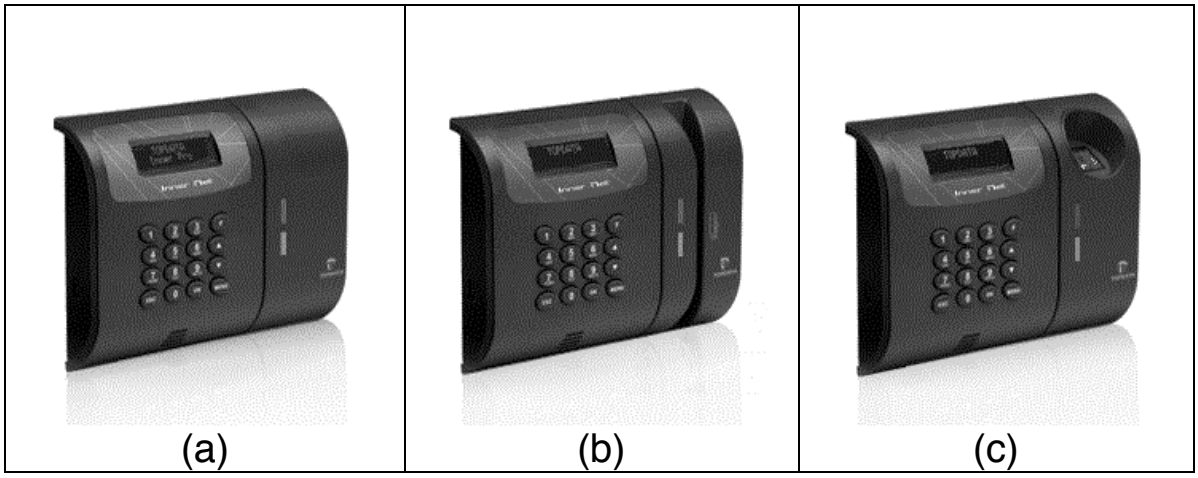


FIGURA 2 - Controles de acesso com funcionalidades diferenciadas. (a) equipamento com leitor de RF-ID, (b) equipamento com leitor de código de barras, (c) equipamento com leitor de impressão digital.

Também se observa que equipamentos, coletores de dados, são ofertados como controle de acesso, entretanto, tem seu foco mais voltado ao controle de ponto eletrônico. Essa característica mostra uma tendência do mercado de integrar funcionalidades ao produto de forma a agregar valor ao mesmo.

Diante do mercado existente este trabalho propõe realizar uma coleta de dados sobre as tecnologias, existente na área de reconhecimento biométrico, utilizadas na atualidade, em produtos presente no mercado, visando, com base nas conclusões encontradas, dar prosseguimento a um projeto de desenvolvimento de um equipamento eletrônico de controle de acesso com identificação biométrica por reconhecimento de impressão digital com características encontradas neste estudo.

1.1 JUSTIFICATIVA

Na atualidade é nítida a crescente utilização de tecnologias biométricas em diversas áreas do nosso cotidiano, principalmente através do reconhecimento de impressões digitais.

Muitos fatores se mostram influentes nesse crescimento, dentre eles podemos citar o aumento na capacidade de processamento dos componentes eletrônicos, como microcontroladores, aliado a queda de seu custo. Este cenário vem de encontro com a necessidade das pessoas e organizações por uma maior confiabilidade na segurança no acesso a ambiente e informações restritas.

A escolha do tema deste trabalho foi baseada no portfólio de produtos da empresa HDL da Amazônia Ltda., a qual possui uma linha de equipamentos voltados ao controle de acesso, dentre os quais não há ainda um com tecnologia biométrica.

Diante desse cenário, a ideia é desenvolver um estudo focado na biometria por impressão digital associado ao controle de acesso de forma a conhecer seus nuances e permitir, com esta base, desenvolver um protótipo inicial de um controle de

acesso onde se possam identificar possibilidades de redução de custos, melhorias, e necessidades para um futuro projeto.

Esse produto, em fase inicial, deve possuir características de acessibilidade customizáveis de acordo com níveis variados de segurança exigidos de acordo com o local de sua utilização.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

O presente trabalho tem como objetivo desenvolver e um equipamento voltado ao controle de acesso através de identificação biométrica. Este equipamento simplificado para controle de acesso, voltado ao estudo desta solução, deve possuir características semelhantes às presentes em equipamentos existentes no mercado.

1.2.2 OBJETIVOS ESPECÍFICOS

Para atingir os objetivos propostos pelo trabalho deverão ser desenvolvidos os seguintes itens que compõe o projeto:

- Explorar a bibliografia e documentação referente a identificação e reconhecimento de impressões digitais;
- Pesquisa e especificação do equipamento a ser desenvolvido;
- Desenvolver o hardware do equipamento;
- Desenvolver o firmware do controle de acesso;
- Realizar a confecção de um protótipo funcional.

2 REVISÃO DA LITERATURA

Esta sessão trata da literatura utilizada como base para o desenvolvimento deste trabalho desde o embasamento das características biométricas, métodos de identificação biométricos, utilizações da biometria, de forma a construir um bom entendimento do tema até controlador de display e métodos de engenharia de software para adquirir maior qualidade na definição e resolução do problema.

2.1 BIOMETRIA NA ATUALIDADE

O mercado das tecnologias biométricas vem crescente nos últimos anos e possui uma projeção de receita de 11 bilhões de dólares no ano de 2017.

O gráfico abaixo, figura 3, mostra a projeção para os próximos anos do crescimento da indústria biométrica.

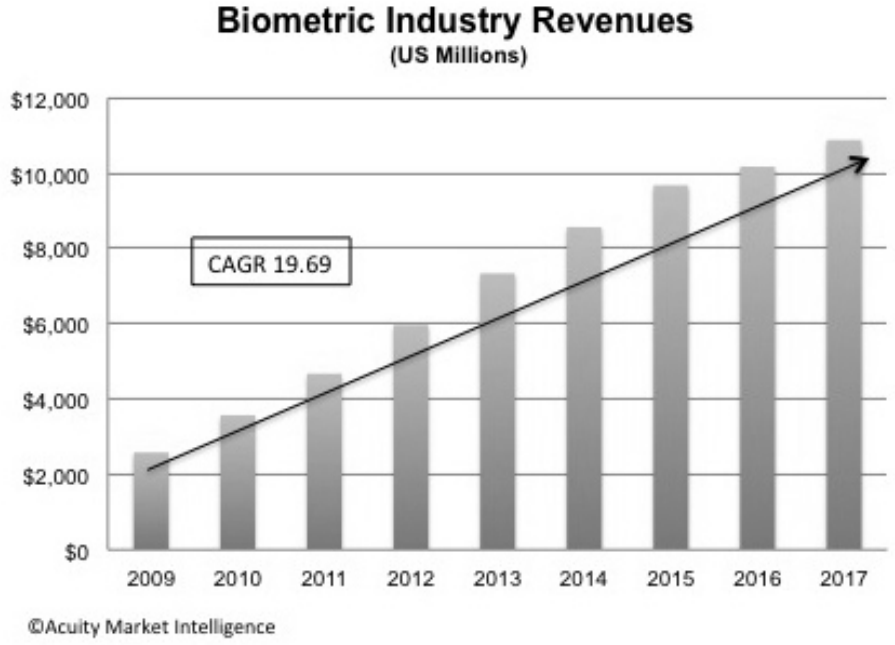


FIGURA 3 - Receitas da indústria biométrica.

FONTE – .GTA/ UFRJ, 2005.

2.2 CARACTERÍSTICAS BIOMETRICAS

A biometria vem sendo inserida em uma vasta variedade de aplicações o que dificulta encontrar uma definição que abranja sua utilização. Segundo o IBG, podemos definir biometria da seguinte maneira:

IBG (2012, tradução nossa) define: “O uso de características fisiológicas ou comportamentais para determinar ou verificar a identidade.”.

Dessa forma, a biometria pode ser vista dividida em dois métodos de trabalho, nos quais, um se baseia na medição das características fisiológicas, enquanto o outro, nas características comportamentais.

A biometria fisiológica é baseada em medições e dados provenientes da parte do corpo humano enquanto que a biometria comportamental é baseada em medições de características de forma indireta e de dados relacionados a uma ação tomada por uma pessoa. Um dos métodos adotados na

biometria comportamental é a métrica, a qual subdivide um comportamento em começo, meio e fim.

2.3 MÉTODOS DE IDENTIFICAÇÃO BIOMÉTRICA

2.3.1 RECONHECIMENTO DE FACE

O reconhecimento facial é o método mais natural de identificação biométrica e o mais utilizado diariamente e de forma intuitiva. O reconhecimento facial automático utiliza como meio de verificação uma série de medidas como distância entre os olhos, nariz e olhos, distância entre boca e olhos, distância entre boca e queixo, linhas dos cabelos, entre outros. Essa verificação é uma tarefa de grande complexidade visto que a face sofre diversas variações com o tempo. Além dessas variações, diferenças nas expressões faciais, no ângulo entre a cabeça e a câmera, mudanças no estilo de cabelo, condições de luz, vem a dificultar este processo de verificação. Este método de reconhecimento possui a vantagem de possuir um baixo índice de intrusão, ou seja uma baixa sensação de estar sendo invadido pelos usuários. Inicia com a captura de uma imagem da face através de uma câmera digital, na qual é executado um algoritmo de verificação dos pontos faciais. Desta forma, podem-se realizar comparações com imagens existentes em uma base de dados.

2.3.2 IMPRESSÃO DIGITAL

A identificação por reconhecimento de impressão digital também conhecido por Finger Scan é o método mais difundido e utilizado em todo o mundo (International Biometric Group, 2009) e que apresenta baixo custo de implantação e de alto grau de confiabilidade.

Neste método é realizado um escaneamento do dedo para capturar, com legibilidade, de detalhes chamados de minúcias. Após o mapeamento das minúcias um processo de leitura e comparação com um banco de dados.

Na verificação da impressão digital é analisada a posição das minúcias, tais como terminações, bifurcações de sulcos, arcos e voltas que se apresentam no dedo.

2.3.3 GEOMETRIA DA MÃO

Esta técnica se baseia no fato de que não existem duas pessoas com mãos idênticas e que a mão não sofre tantas alterações com o passar da idade. É um método que requer pouca atenção do usuário durante a verificação.

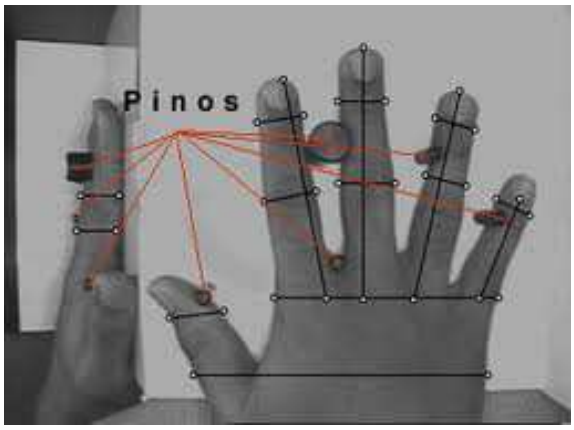


FIGURA 4 - Exemplo de pontos de medição.

FONTE – GTA/ UFRJ, 2007.

A imagem da mão é capturada através de um leitor, no qual o usuário posiciona a mão com os dedos alinhados. A figura 4 ilustra o posicionamento da mão para realização da leitura. O leitor possui uma câmara posicionada acima da mão a qual faz a leitura das características da mão como o comprimento do dedo, largura e área. Outro método de reconhecimento da mão se baseia na identificação das linhas, saliências entre outros detalhes o que se faz semelhante ao reconhecimento por impressão digital.

Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e através de uma câmara posicionada acima da mão a imagem é capturada. Medidas tridimensionais de pontos selecionados são extraídas e o sistema realiza medições que geram um identificador matemático único na criação do modelo. Um modelo típico requer cerca de nove bytes de armazenamento.

2.3.4 RECONHECIMENTO DE RETINA

Este método se utiliza o padrão de veias da retina que por sua vez é considerado uma das características de maior unicidade de uma pessoa. Entretanto, apesar da unicidade, as características da retina que se pensavam ser estáveis são afetadas por doenças, muitas vezes sem conhecimento do indivíduo.

Estes vasos sanguíneos são visualizados através de uma imagem focada obtida com o auxílio de um laser de baixa intensidade e por uma câmara. Com esta imagem o analisador mede os padrões de vasos sanguíneos. A figura 5 mostra a imagem de uma retina e seus vasos sanguíneos utilizados para análise de padrões.

FIGURA 5 - Imagem da retina.

FONTE – GTA/ UFRJ, 2010.

A análise da retina é um dos métodos mais seguros e que não se tem conhecimento de fraudes. Entretanto, esta técnica é

considerada invasiva já que o usuário necessita colocar o olho perto da câmara para obter a imagem. Este procedimento deixa muitos usuários temerosos em adquirir algum tipo de problema ao expor os olhos a uma luz.

2.3.5 RECONHECIMENTO DE ÍRIS

Devido ao processo de reconhecimento biométrico por retina ser um processo invasivo, este abriu as portas da pesquisa por outros métodos como o do reconhecimento da íris.

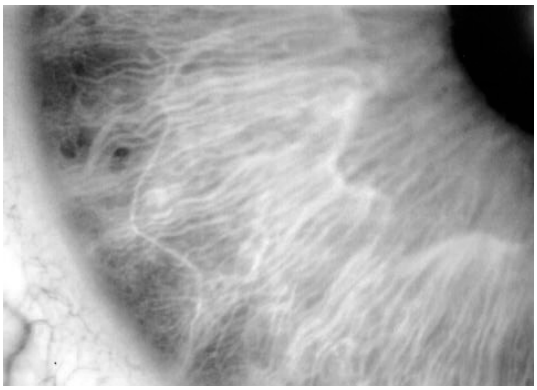


FIGURA 6 - Imagem de uma íris.

FONTE – Senado, 2007.

A Íris, como apresentado na figura 6, é o anel colorido de envolve a pupila. Ela possui um padrão complexo e único que permite ser utilizado na identificação de uma pessoa.

O método utiliza uma imagem monocromática para analise da íris e identificação do seu padrão. Esta imagem é processada de forma a se identificar à íris e extrair as suas características. Estas características são comparadas com informações de outras íris armazenadas em um banco de dados de forma a se encontrar uma compatível.

Os sistemas que utilizam este método de identificação capturam a imagem da íris através de uma câmera a uma distância aproximada de 30 cm ou mais. As informações armazenadas em banco, do padrão da íris, ocupam aproximadamente 512 bytes.

Este método de reconhecimento tem seis vezes mais características distintivas que as impressões digitais, não são cirurgicamente modificadas sem prejuízo à visão e possui a vantagem de possibilitar sua autenticidade através de sua reação a estímulos luminosos. Entretanto, os sistemas que utilizam este método necessitam ajustar a câmera, que captura a imagem, a altura dos olhos inclusive para portadores de deficiência como usuários de cadeira de roda.

2.3.6 RECONHECIMENTO DE VOZ

Esta forma de reconhecimento utiliza-se da analise da voz humana de forma a reconhecer um modelo previamente cadastrado. A voz humana se diferencia pela ressonância gerada pela região vocal, a qual varia o seu comprimento, no formato da boca e cavidades nasais.

Os sistemas com reconhecimento de voz se baseiam em tecnologia de processamento de fala a qual utiliza análise de Fourier para encontrar o espectro de frequência que amostram as características da voz. Após a formação de um padrão em cima da fala devido a fatores físicos e comportamentais, uma imitação seria impossível. Entretanto, esta tecnologia necessita de várias gravações de voz para se identificar um padrão, exige do usuário clareza na voz e fala em tempo apropriado ao utilizar o sistema sem contar com problemas com as condições ambientais já que ruídos são difíceis de serem isolados. Estas características do sistema e outros problemas como: variação da voz devido à gripe e resfriado, estado emocional, estresse, e a possibilidade de duplicação através de um gravador fazem com que este método não tenha uma grande utilização.

2.3.7 RECONHECIMENTO DE ASSINATURA MANUSCRITA

Há duas técnicas de reconhecimento de assinatura manuscrita. Entre elas a primeiro examina uma assinatura já escrita de forma a compará-la a uma imagem armazenada. Uma das desvantagens deste método é que não se consegue detectar fotocópias das assinaturas. O segundo método estuda a dinâmica da assinatura. Dentro do estudo da dinâmica se observa o ritmo da escrita, contato com a superfície, tempo total, pontos de curva, laços, sua velocidade e aceleração.

Como em outros métodos as características comportamentais como a variação de humor, ao ambiente, a caneta, ao papel, além disso, algumas pessoas têm assinaturas muito consistentes enquanto outras variam muito.

2.3.8 RECONHECIMENTO POR DINÂMICA DA DIGITAÇÃO

A dinâmica da digitação é um método de biometria comportamental que analisa o padrão de digitação de um usuário em um teclado de forma a identificar o indivíduo através de seu ritmo habitual. Este padrão pode ser considerado único já que o mesmo possui fatores neurofisiológicos semelhantes aos encontrados nas assinaturas manuscritas. Este processo não se baseia no que se digita, mas sim na sua forma.

Nesta analise dinâmica podem ser levados em conta diversos fatores como o tempo decorrido entre o pressionamento da primeira e segunda tecla, tempo que uma tecla permanece pressionada, posição do dedo, pressão aplicada sobre as teclas, a velocidade de digitação geral, certos dígrafos, digitação de duas letras adjacentes, etc.

O procedimento de identificação e verificação requer que o usuário possua um perfil ou modelo armazenado, este é utilizado na operação de verificação com o perfil de digitação identificado.

No geral, é considerado pouco confiável, entretanto na digitação de sentenças regulares, como o nome de usuário, este

método é bem confiável e de baixo custo de implantação. Uma de suas vantagens é que o usuário não percebe quando está sendo autenticado, além disso, este método apresenta seu cadastramento e verificação não são invasivos.

2.3.9 RECONHECIMENTO VASCULAR

O reconhecimento vascular compreende no ato de reconhecer um indivíduo através dos padrões das veias da mão, rosto, punho, dedo, etc.

Estes padrões de veias são visualizados através de sensores que captam a reflexão de raios infravermelhos irradiados sobre a superfície analisada. O fato de ser analisada uma região interna ao corpo humano garante uma maior segurança contra possíveis fraudes. Esta tecnologia não necessita que o usuário tenha contato direto com o leitor, sendo assim, demostra-se ser menos invasivo e de maior higiene.

2.4 APLICAÇÕES DA BIOMETRIA

As aplicações da tecnologia biométrica são extremamente diversificadas. Segundo a empresa de consultoria Consultores Biométricos associados (CBA, 2012), pode-se categorizar em aplicações voltadas ao uso de forças policiais ou ao uso civil.

No campo civil, basicamente, todas as aplicações utilizadas neste segmento envolvem alguma forma de controle de acesso considerando acessos físicos de pessoas a áreas restritas como em segurança de dados sensíveis. Este é um mercado em expansão devido à necessidade crescente e constante de evitar fraudes.

Dentre as áreas de utilização da tecnologia biométrica podemos citar os bancos, sistemas de pagamentos, sistemas de computadores, também identificados como Acesso de Controle Lógico, Imigração, Identificação nacional, Acesso Físico, Prédios

e delegacias, controle de ponto e monitoramento. Obviamente, as aplicações não são restritas às áreas citadas e consequentemente se expandirão a outros mercados.

Uma das aplicações de destaque é na identificação nacional. Os governos, como o Brasil, estão utilizando a tecnologia para cadastramento da população. Com isso, ele se previne contra fraudes, por exemplo, durante as eleições, e tem como identificar os cidadãos.

A figura 7 mostra o novo Registro de Identificação Civil brasileiro. Este projeto pretende substituir as carteiras de identificação impressas por cartões com chip. A grande vantagem é que cada cidadão passará a ter um número único de identificação baseado em suas impressões digitais no Cadastro Nacional de Registro de Identificação Civil. Pretende-se com isso integras bases de dados de órgãos de identificação no território brasileiro.

FIGURA 7 - Registro de Identificação Civil.

FONTE – Mercado em Ação, 2012.

2.5 FUNCIONAMENTO DA AUTENTICAÇÃO BIOMÉTRICA

O primeiro passa em equipamentos biométricos e o processo de cadastramento. O sistema extrai amostras das características biométricas que são convertidas em um código matemático que, por usa vez é armazenado como um padrão da

biometria em um banco de dados. Esta é à base de funcionamento do sistema, no qual sempre deve haver um modelo biométrico armazenado para que no processo de autenticação seja comparada a impressão digital do usuário. O sistema biométrico então decide se a impressão lida combina com o modelo armazenado.

2.6 IDENTIFICAÇÃO E VERIFICAÇÃO

Basicamente, os processos de autenticação biométrica podem ser divididos em processo de identificação e de verificação.

A identificação biométrica é um processo um para muitos (1:N), na qual, uma amostra é comparada com toda a base de dados de modelos de forma a encontrar um registro idêntico. Já a verificação é um processo um para um (1:1), no qual a amostra é comparada com um modelo específico.

O processo de verificação biométrica é mais rápido do que a identificação, já que aquele não necessita comparar a amostra com todo o banco de dados de modelos do sistema. Esta característica é evidente quando se possui um banco de modelos muito extenso.

2.7 CONTROLADOR DE LCD PCD8544

O componente PCD8544 é um controlador de LCD desenvolvido para acionamento de um display de com resolução de 48 linhas por 84 colunas. Segundo a folha de dados (NXP, 2012) é mantida internamente uma matriz de bits de 48 linhas por 84 colunas armazenadas em memória RAM. Esta matriz permite ser escrita de oito em oito bits por vez, sendo que nesta situação, sua configuração pode ser interpretada como na figura 8 constituída com seis bytes verticais por 84 bytes horizontais.

Este controlador possui dois modos de varredura durante a escrita dos bits: modo vertical e modo horizontal.

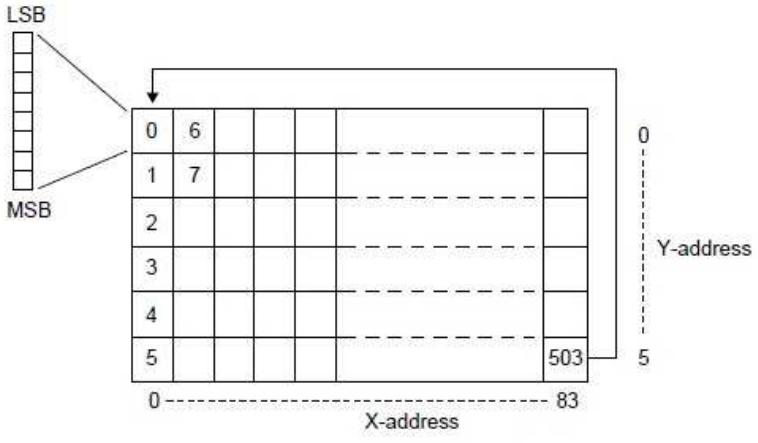


FIGURA 8 - Organização da matriz do controlador PCD8544.

Através da figura 8 se pode visualizar a ordem de escrita dos bytes na matriz no modo de varredura vertical. A cada byte escrito é incrementada o endereço Y automaticamente. Ao final da escrita da coluna Y é incrementada a posição da coluna e reiniciada a posição de Y. O modo de varredura horizontal opera similarmente ao Y, entretanto o seu movimento de escrita ao invés de ser vertical é horizontal como seu nome sugere.

Através do terminal D/C o controlador é informado sobre o tipo de byte que será transmitido. Caso esteja em nível lógico baixo entenderá que é um comando e caso nível baixo, um dado.

A transmissão do byte é sempre iniciada com o seu bit mais significativo, *Most Significative Bit* (MSB) e finalizado com o menos significativo, Least Significative Bit (LSB).

O controlador, através do terminal SCE, pode ser habilitado ou desabilitado com uma borda de descida e subida respectivamente.

Através do terminal SDIN a transmissão dos bytes ocorre. O estado dele é lido pelo controlador na ocorrência de uma borda de subida no terminal de sincronismo SCK. Para isso acontecer, o terminal SCE deve estar habilitado.

Na escrita dos dados na matriz o próprio controlador realiza o incremento da posição de armazenamento na matriz de bits somente sendo necessário efetuar o envio dos bytes.

A figura 9 demonstra a forma de onda dos sinais de controle para a escrita da matriz de bits do controlador.

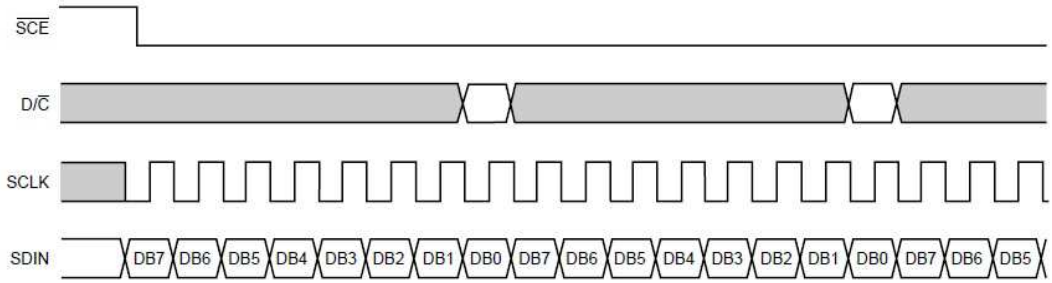


FIGURA 9 - Sinais na transmissão de bytes ao controlador PCD8544.
FONTE – NXP,2012.

2.8 ENGENHARIA DE SOFTWARE

A engenharia de software surgiu no final da década de 60 com a disseminação do uso de computadores. Na época, as mudanças de tecnologia nos recursos de hardware possibilitaram que produtos de software mais complexos fossem criados e com isso surgiram problemas de identificação de requisitos, problemas de interação entre engenheiros e clientes, baixa produtividade, baixa qualidade, o que muitas vezes culminava em um produto errado.

Segundo André (Koscianski, 2007,p.22), baseado em documentos da década de 70, os problemas enfrentados nos dias atuais, mais de quarenta anos depois, são os mesmos.

A engenharia de software pode ser descrita como um ramo da engenharia que está voltada aos aspectos da produção de um software englobando etapas desde a especificação do sistema até sua manutenção. Ela surgiu como uma ferramenta para auxiliar a minimizar os problemas existentes e proporcionar a produção de softwares com maior qualidade e com custos adequados.

Nas palavras do Dr. Reginaldo fica enfatizado que:

> A engenharia de software não está relacionada apenas como os processos técnicos de

> desenvolvimento de software, mas também com atividades como o gerenciamento de projeto de software e o desenvolvimento de ferramentas, métodos e teorias que apoiem a produção de software. (Arakaki, 2007, p.5)

3 DESENVOLVIMENTO

3.1 ENGENHARIA DE REQUISITOS

A engenharia de requisitos corresponde a uma subárea da engenharia de software na qual é adotado para se realizar um estudo do sistema de forma a se criar um modelo. Através desse modelo, por sua vez, pretende detalhar tecnicamente o projeto a fim de analisá-lo, permitindo um maior entendimento de suas características antes de sua implementação de forma a elicitar seus requisitos e obter uma maior qualidade do produto.

3.1.1 DOMÍNIO DO PROBLEMA

O trabalho de engenharia de requisitos foi iniciado buscando entender o domínio do problema. Aqui se pretende entender as reais necessidades a fim de resolver os objetivos propostos. Esta etapa é fundamental para o bom desenvolvimento do projeto, pois, partindo-se deste ponto, se construiu a orientação para todo o processo de identificação de requisitos do sistema.

Embasado nos objetivos deste projeto foram listadas as necessidades, de maneira ampla, que resultaram em na tabela 1.

TABELA 1 - Lista de necessidades

N°	Necessidades
1	Controlar o acesso de usuários a áreas restritas.
2	Realize o controle através de identificação biométrica.
3	Que permita sua utilização em empresas e residências.
4	Que permita acesso rápido à área restrita.
5	Que possa bloquear o acesso de pessoas sem permissão.
6	Que possa customizar as configurações de permissão de usuário.

3.1.2 DOMÍNIO DA SOLUÇÃO

Tendo-se conhecimento sobre o problema ao qual se deve solucionar, foi iniciado um processo de identificação, com base nas informações sobre o problema, das características e requisitos do sistema. Este procedimento pretende estabelecer um escopo mais refinado do trabalho que necessita ser realizado. Como resultado deste trabalho foi obtido às características listadas na tabela 2.

TABELA 2 - Lista de características do sistema.

N°	Característica
1	O sistema deve poder se comunicar, sem fio, com um módulo de acionamento de fechos da empresa HDL.
2	O sistema deve poder trabalhar com biometria ou biometria e teclado.
3	O sistema deve possuir uma tela de visualização de informações ou orientações.
4	O sistema deve ser capaz de validar usuários.
5	Deve permitir o cadastramento dos usuários pelo próprio equipamento.
6	Deve possuir um teclado numérico para a entrada de informações.
7	Deve apresentar data e hora quando em operação.
8	Deve possuir um acionamento de fecho por fio, independente do módulo de acionamento de fechos.
9	Deve possuir alerta de emergência
10	Deve possuir sinalização luminosa de aprovação ou rejeição.

3.1.2.1 REQUISITOS DE SOFTWARE

Com base nas características do sistema foi realizado um detalhamento que deu origem aos requisitos do sistema. Basicamente, podemos dividir os requisitos do sistema em duas categorias: requisitos funcionais e não funcionais.

Segundo André (2007, p.174) os requisitos de *software* podem ser definidos como "[...] são as descrições sobre seu comportamento, funções e especificações das operações que deve realizar e especificações sobre suas propriedades ou atributos.". Portanto, pretendeu-se com esta etapa identificar e descrever as funcionalidades do *software* levando em conta suas características e especificações.

Os requisitos foram listados e identificados para que se possa distinguir uns dos outros Cada identificador possui uma sigla que descreve o tipo de requisito ao qual ele pertence e uma numeração única que os individualiza entre os demais requisitos do mesmo tipo. Os requisitos obtidos foram listados na tabela 3.

Outra técnica utilizada durante o levantamento de requisitos é a técnica de cenários.

TABELA 3 - Lista de requisitos funcionais do sistema.

Requisitos funcionais
REF 01 - O sistema deve permitir que um usuário configure através de uma interface externa os parâmetros do equipamento.
REF 02 - O sistema deve permitir que um usuário administrador atribua tipos de perfis diferenciando aos usuários do sistema, ou categorias de acesso diferenciadas de forma a restringir os acessos dos usuários as zonas.
REF 03 - O sistema deve realizar a identificação dos usuários por leitura biométrica de impressão digital.
REF 04 - O sistema deve realizar o acionamento externo para abertura de fechaduras.
REF 05 - O sistema deve permitir que um usuário administrador atribua aos usuários a participação em um grupo.
REF 06 - O sistema deve permitir que um usuário se identifique através de uma interface de teclado, futuramente um leitor de proximidade ou cartão de proximidade;
REF 07 - O sistema deve interagir com sensor de porta
REF 08 - Zone Access Control: controle de acesso por zona, de forma a controlar o acesso do usuário.
REF 09 - O sistema deve permitir que um usuário administrador troque o modo de operação do equipamento;
REF 10 - O sistema deve avisar de forma sonora se o acesso

foi liberado.
REF 11 - O sistema deve permitir que um usuário administrador cadastre uma ou duas impressões digitais por usuário.
REF 12 – O sistema deve gerenciar o controle de acesso das zonas por horário de acesso. Em horários não permitidos o acesso deve ser bloqueado, independentemente que o usuário possua acesso a zona. (*Time Zone Access Control*)
REF 13 - O equipamento deve permitir que um usuário administrador associe grupos e tipos de usuário a uma zona de forma a liberar o acesso a mesma.
REF 14 - Controle de autorizações de entrada e de horas extras;
REF 15 - Sinalização luminosa de aprovação ou reprovação da identificação.
REF 16 - Sistema de Pânico
REF 17 - Cadastramento de usuários
REF 18 - Exclusão de Usuários
REF 19 - O sistema deve permitir que um usuário administrador atribua a um usuário um nível de acesso ou zona de acesso.
REF 20 – O sistema deve manter um ID, correspondente ao aparelho, para que permita sua identificação quando em rede.
REF 21 - Configuração de Ações ao reconhecimento
REF 22 - O sistema deve controlar o acesso dos usuários de acordo com seu perfil, zona e horário.
REF 23 - Ajuste de Tempo de Acionamento.
REF 24 - Modo de acionamento Fecho
REF 25 - O sistema deve permitir que o usuário/ geral realize um ou mais registros.
REF 26 - O sistema deve permitir que um usuário administrador ative.
REF 27 - o sistema deve permitir que um usuário administrador configure um PRÉ tempo antes do acionamento do sistema de pânico.
REF 28 - O sistema deve permitir que um usuário administrador permita o acionamento do fecho ou não quando o sistema de pânico for acionado.
REF 29 - O sistema deve permitir que um usuário, do tipo administrador, habilite o acionamento de uma saída On/Off em caso de ativação do sistema de pânico.

Nesta etapa de análise dos requisitos, são descritos os requisitos não funcionais. Estes informam restrições ao *software*

de forma geral. Estes por sua vez, não possuem relação direta com as funções do produto.

TABELA 4 - Lista de requisitos não funcionais do sistema.

Requisitos não funcionais
RNF 01 - Deve possuir biometria e teclado para possibilitar o trabalho nos modos 1:N e 1:1;
RNF 02 - Pode ser utilizado em aplicações Off line;
RNF 03 - Condições ambientais: Uso interno;
RNF 04 - Deve possuir bateria interna para manter o horário atualizado independente se o equipamento esteja desligado. Evitar a perda do horário durante a queda de luz.
RNF 05 - Abertura de fechaduras.
RNF 07 - O sistema deve possuir uma interface de comunicação ethernet.

De acordo com os requisitos funcionais encontrados podem-se identificar as funcionalidades requeridas ao software embarcado necessárias para que o produto atingisse seus objetivos. Cada um dos requisitos está ligado diretamente a uma ou mais funcionalidades do sistema embarcado ao equipamento que em muitos casos, para cumprir sua função se associa a outros requisitos.

3.1.2.2 REGRAS DE NEGÓCIO

Nesta etapa do projeto foi realizado um trabalho para explicitar as regras de negócios necessárias ao sistema. Podem-se compreender as regras de negócio como um detalhamento dos requisitos. Estas devem especificar como o requisito deve funcionar.

> "Regra de negócio é uma restrição imposta pelo negócio que regulamenta o comportamento de um procedimento operacional do negócio. São políticas definidas pela administração da empresa." (PINTO; Evandro Moreira, 2012)

Aos moldes do trabalho realizado nos requisitos, as regras de negócio foram listadas e identificadas, na tabela 5, de forma a individualizá-la entre as demais.

TABELA 5 - Lista das regras de negócio do sistema.

Regras de Negócio
RNE 01 - Deve-se sempre assegurar que o ID do equipamento, presente no pacote de comunicação, coincide com o ID do equipamento.
RNE 02 - Deve-se sempre assegurar que o cálculo CRC dos dados recebidos seja comparado ao CRC recebido no pacote.
RNE 03 - Pode se atribuir somente um tipo de perfil por usuário.
RNE 04 - A impressão digital deve estar previamente cadastrada.
RNE 05 - O equipamento deve estar programado em um modo de operação que realiza a validação do usuário por impressão digital.
RNE 06 - O equipamento deve estar habilitado para gerar o acionamento externo.
RNE 07 - O usuário deve ser identificado na base de dados.
RNE 08 - O acionamento externo só pode ser realizado se o horário for permitido.
RNE 09 - O acionamento externo só pode ocorrer se o dia for um dia válido (Permitido).
RNE 10 - O acionamento só pode ser realizado se a zona do equipamento for compatível com a do perfil do usuário identificado.
RNE 11 - O equipamento deve estar funcionando em modo teclado ou modo de verificação 1:1 com teclado.
RNE 14 - Para cada equipamento só pode ser atribuida um tipo de área de controle.
RNE 15 - O tipo de área de controle deve ser uma restrição de acesso aos usuários do sistema.
RNE 16 - O usuário deve ter permissão de acesso liberada ao local mediante validação.
RNE 17 - O equipamento somente trabalhar em um único modo de operação por vez.
RNE 18 - Deve ter proteção para que não seja configurado um modo de operação incompatível com o hardware.
RNE 19 - Cada usuário pode participar de um grupo de acesso.

RNE 20 - Um equipamento deve ser capaz de suportar até 10 grupos de acesso.
RNE 21 - O equipamento deve verificar o modo de operação biométrico para identificar se deve cadastrar uma ou duas impressões digitais,
RNE 22 - O usuário administrador só podera cadastrar duas impressões digitais caso o modo de funcionamento seja compatível.
RNE 23 - O cadastro do usuário deve ser associado a um código único.
RNE 24 - O sistema deve ter a opção de incremento automático ou atribuição de um ID para o usuário.
RNE 25 - O sistema deve verificar a inconsistência no novo ID de usuário.
RNE 26 - A exclusão de cadastros tem que ser vinculada ao ID do usuário que é um código único vinculado ao cadastro do usuário.
RNE 27 - Uma exclusão de cadastro deve excluir uma ou mais impressões digitais cadastras associadas ao ID do usuário.
RNE 28 - Cada equipamento só pode possuir um ID que deve ser único.
RNE 29 - O tempo máximo de acionamento da fechadura deve ser de 5 segundos.
RNE 30 - Só pode trabalhar com um modo de funcionamento por vez.
RNE 31 - No modo ON/OFF não depende do tempo de acionamento.
RNE 32 - O sistema deve permitir uma ou mais opções de ação ao reconhecimento.
RNE 33 - Deve-se poder configurar as ações para o sistema de pânico ao reconhecimento do usuário.
RNE 34 - Deve se poder vincular uma ação.
RNE 35 - Somente pode finalizar ao término do reconhecimento.
RNE 36 - Caso não tenha permissão deve sinalizar negativamente. Led vermelho.
RNE 37 - Digitar o código do tipo de registro.
RNE 38 - O Time zone tem que estar ativado.
RNE 39 - Deve verificar se o horário é liberado na zona.
RNE 40 - Deve verificar se o perfil do usuário tem acesso no dia, caso seja um sábado, domingo, feriado ou dia útil.
RNE 41 - Deve verifica se não há uma liberação especial de horário ou dia para o grupo ou perfil

RNE 44 - Deve verificar se o sistema de pânico está ativo.

3.1.2.3 ANÁLISE ATRAVÉS DE CADOS DE USO

Com a definição das regras de negócio, os requisitos funcionais foram subdivididos em módulos de acordo com suas funções no sistema e associados às regras de negócio necessárias para que estes sejam cumpridos. Esta organização possibilita uma melhor visualização do sistema. Através da figura 10 se pode observar como este trabalho foi realizado.

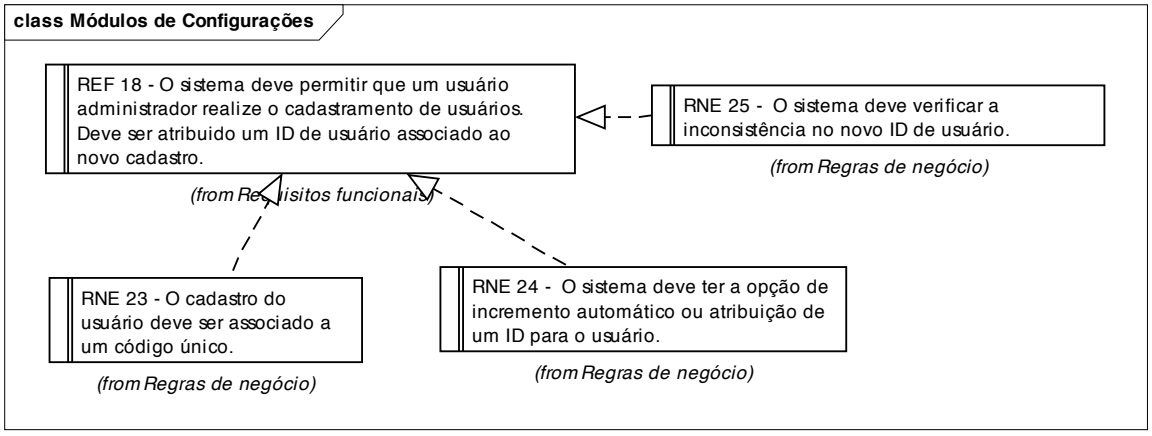


FIGURA 10 - Exemplo de diagrama de realização do módulo de configuração.

Finalizada a organização em módulos ao nível da aplicação, foi utilizada uma técnica de classificação chamada de Casos de Uso. Foram construídos diagramas de caso de uso com o objetivo de identificar as funcionalidades do sistema. Estas funcionalidades são definidas com a execução de um ou mais requisitos do sistema. Que por sua vez, possuem regras de negócio associadas, como no exemplo da figura 10.

A figura 11 apresenta o diagrama de casos de uso do módulo de configurações.

No diagrama de caso de uso o objeto que interage com o sistema, no estudo abaixo representado pelo administrador, é apresentado iniciando funções do sistema. Este estudo é

somente representado aqui, através do módulo de configurações, já que sua apresentação completa seria muito extensa.

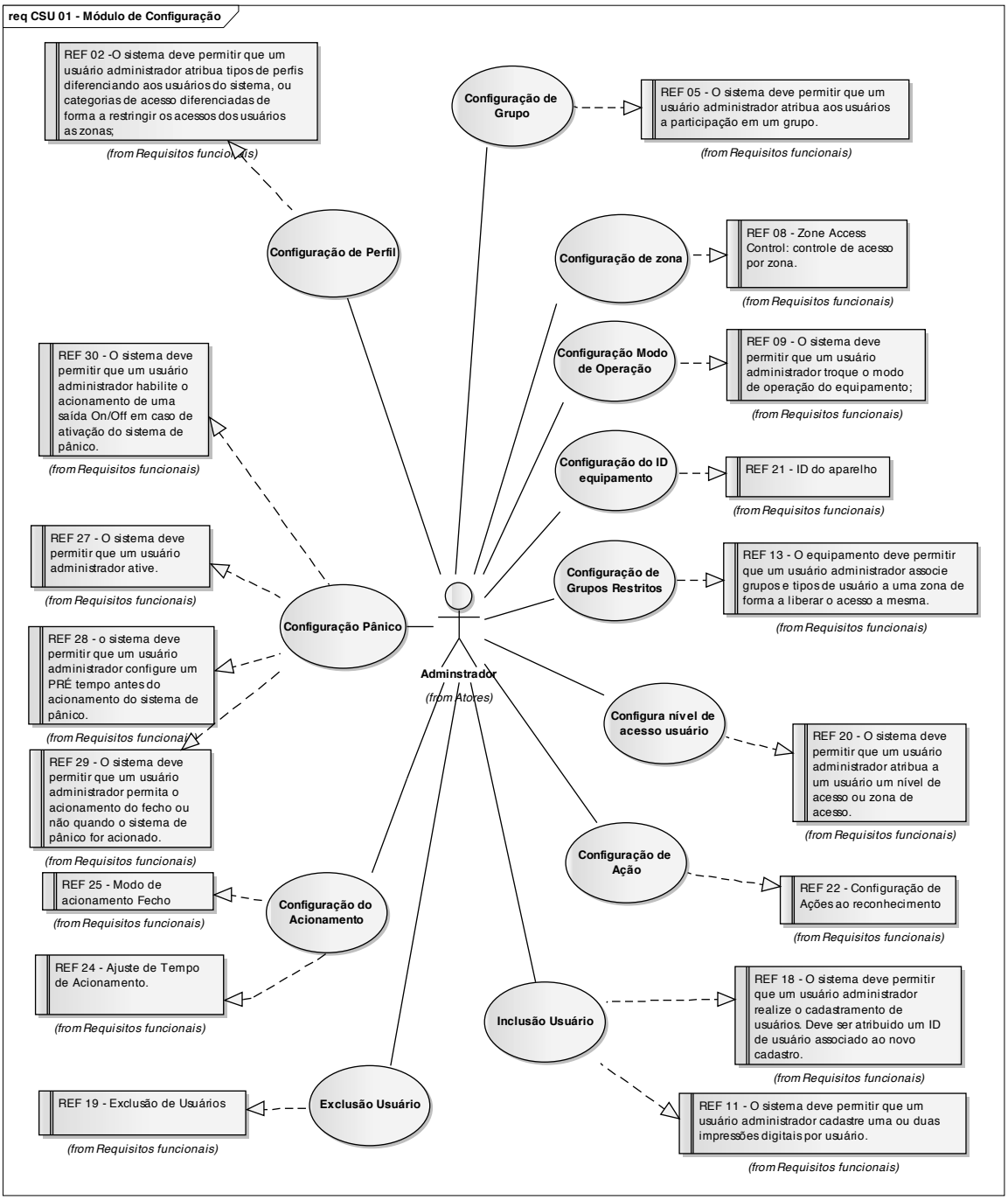


FIGURA 11 - Diagrama de Casos de Uso do módulo de configuração da aplicação.

3.2 MECÂNICA

O produto foi concebido para operar somente com a biometria ou associado à outra interface de entrada de dados, neste caso um teclado. Com o propósito de desenvolver esta interface através de um teclado, optou-se pelo aproveitamento do teclado de um Módulo de Acesso com Teclado (Sem Fio) da empresa HDL (HDL, 2012). Por consequência, utilizou-se o mesmo tipo de mecânica para servir de gabinete para a placa principal do projeto.

3.2.1 GABINETE DA PLACA PRINCIPAL

Em primeiro lugar, alterações na parte externa da mecânica escolhida foram necessárias para se exteriorizar o *display* e o sensor biométrico. Utilizando uma micro retífica foi modificada a sua estrutura de forma a ampliar a área vazada e permitir a visualização dos componentes antes descritos.

FIGURA 12 - Modificação na mecânica do Módulo de Acesso com Teclado da HDL.

Até este momento pretendia-se utilizar um sensor biométrico do tipo capacitivo, todavia foi decidido utilizar em seu

lugar um sensor do tipo óptico. Esta alteração foi baseada no fato de que o produto pode ser instalado em lugares de grande circulação, sendo assim, o sensor óptico apresentaria maior resistência.

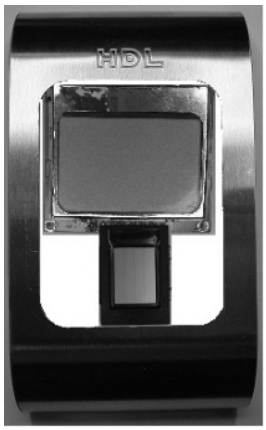


FIGURA 13 - Simulação computacional da mecânica com sensor capacitivo.

Por consequência desta mudança foi desenvolvido um visor de proteção do *display* sem a existência de furações para encaixe da biometria, que por sua vez foi deslocada para uma mecânica específica.

Para a confecção do visor do *display* utilizou-se um retângulo de acrílico com dimensões de 55x72x3 milímetros. Neste foi impresso o formato do orifício de seu encaixe existente na mecânica modificada. Com o auxílio da mini retífica e uma ferramenta de fresa foi executado o rebaixo de 1 milímetro ao redor da área de encaixe.

FIGURA 14 - Visor frontal do gabinete da placa principal.

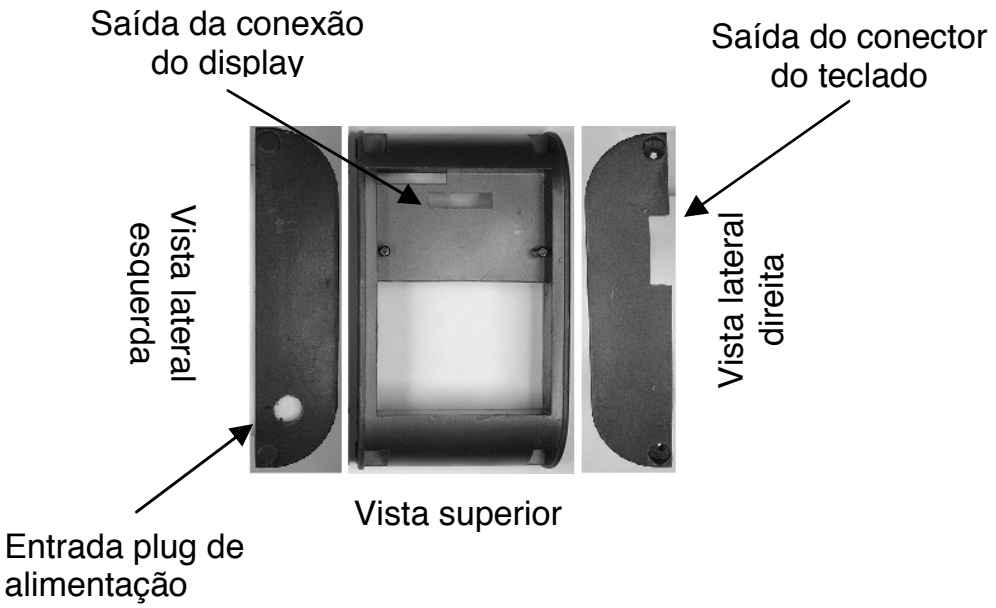


FIGURA 15 - Adaptações realizadas na mecânica.

3.2.2 GABINETE DO TECLADO

Já que o enfoque deste trabalho é o controle de acesso por biometria a adição de uma entrada de dados via teclado se apresentou como uma opção alternativa. Desta maneira, este gabinete necessitou ter uma característica de mobilidade, permitindo a retirada do teclado.

Como no gabinete da placa principal já se havia utilizado uma mecânica de um Módulo de Acesso com Teclado da empresa HDL se decidiu utilizar o teclado deste produto no projeto.

Este teclado possui uma conexão através de um terminal barra pinos, de forma que seus terminais ficam disponíveis facilitando a sua integração no sistema. Também possui iluminação nas teclas que é uma característica importante para sua utilização noturna. Seu design e sua estrutura em aço inoxidável também oferecem uma estética boa, além de resistência no uso.

3.3 HARDWARE

Nesta etapa é constituída pelo projeto, especificação e construção do *hardware* do equipamento para que seja alcançado os objetivos propostos neste trabalho.

A especificação dos requisitos de *hardware* foi baseada nas funcionalidades identificadas durante a etapa de engenharia de requisitos. Por intermédio destas funcionalidades foi possível identificar as necessidades de *hardware* requeridas pelo sistema, que por sua vez, foram associadas a módulos. Cada módulo pretende solucionar a necessidade de uma ou mais funções do equipamento. Com base neste estudo foram identificados os seguintes grupos de módulos:

TABELA 6 - Grupos de módulos adotados no sistema.

Módulos do sistema	
1	Unidade de Processamento Central (CPU)
2	Módulos de acionamento
3	Módulos de armazenamento de dados
4	Módulos de Áudio
5	Módulo biométrico
6	Módulo de teclado
7	Módulo de Display
8	Módulo de comunicação
9	Módulo de Alimentação

Apesar de que os módulos tenham sido projetados separadamente, com o objetivo de cumprir uma ou mais funções, muitos deles apresentam-se agrupados em uma única placa de circuito de forma a possibilitar sua redução física.

Como o *hardware* deste sistema foi segmentado em módulos para melhor atender as necessidades do sistema, assim também será realizada as suas descrições no desenvolvimento.

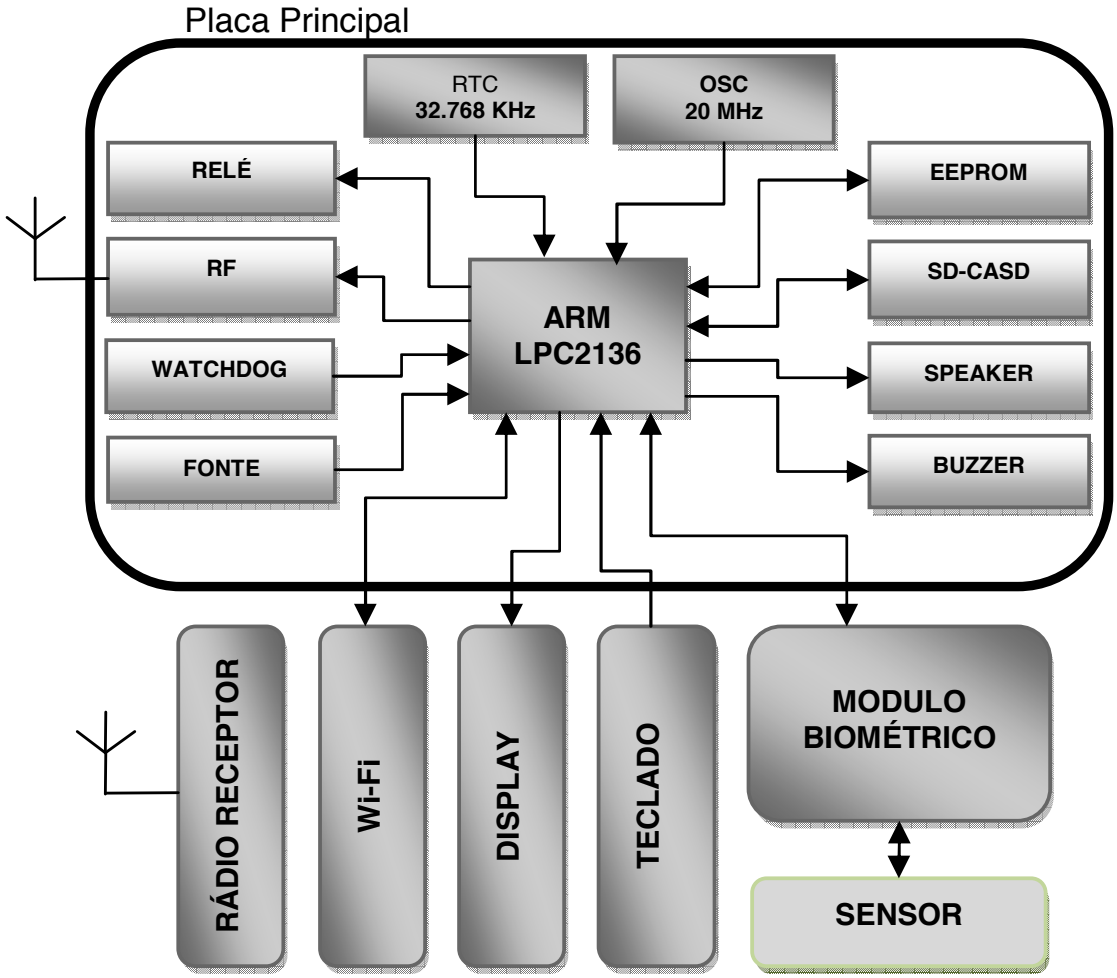


FIGURA 16 - Diagrama de blocos do controle de acesso biométrico.

Através do diagrama apresentado na figura 16, observa-se a distribuição dos módulos presentes no projeto que estão agrupados em blocos relacionados às placas eletrônicas existentes.

3.3.1 UNIDADE DE PROCESSAMENTO CENTRAL (CPU)

O primeiro módulo a ser descrito do hardware do controle de acesso será a CPU. Este tem como seu principal componente um microcontrolador 32-bit ARM7TDMI-S de fabricação da empresa NXP Semiconductors de descrição LPC2136.

Seu circuito de oscilação é constituído por um cristal externo de frequência de 20 MHz, esta, internamente, através de um circuito de *Phase Looked Loop* (PLL) é multiplicada fornecendo ao sistema uma frequência de trabalho de 60 MHz.

3.3.1.1 Relógio Interno

Para auxiliar no desenvolvimento de algumas funcionalidades identificadas no sistema como a apresentação de informações de data e hora ao usuário além de registros de acesso com horário foi concebido este módulo. Desta forma, foi utilizado o *Real Time Clock* (RTC) existente internamente ao microcontrolador. Este circuito, para garantir sua base de tempo recebe um sinal de *clock* externo, proveniente de um cristal, de 32.768 KHz.

O RTC disponibiliza, através de um dos pinos do microcontrolador, um terminal nomeado Vbat no qual se permite conectar uma bateria. Esta bateria corresponde a uma fonte secundária de energia somente do circuito de RTC. Este recurso foi utilizado para que o sistema de relógio mantenha as informações atualizadas após situações de queda de energia. Aqui foi utilizada uma bateria de 3 V, modelo compatível com os utilizados em computadores pessoais. Outra opção que se apresenta como alternativa para substituir a bateria é a utilização de um supercapacitor.

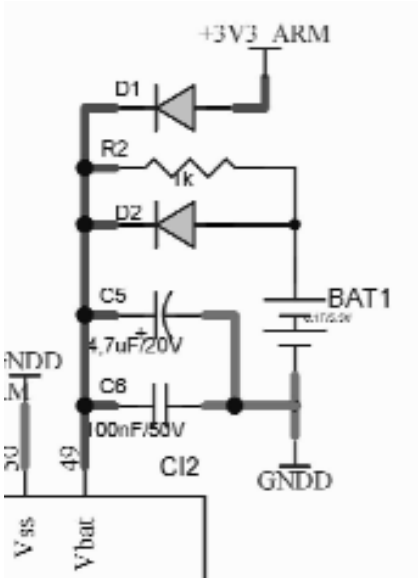


FIGURA 17 - Circuito da bateria do RTC.

Prevendo a utilização de um supercapacitor foi inserido no circuito o componente R2 para a situação de carga do mesmo. Foram utilizados diodos para isolamento da tensão fornecida pelo equipamento e pela bateria de forma que quando o equipamento é energizado o RTC é alimentado pela energia proveniente do equipamento e em sua falta pela bateria. O circuito também garante que a bateria somente fornece energia para o circuito do RTC mantendo os dados referente a data e hora por mais tempo.

3.3.1.2 Circuito de Reset

Para garantir que o sistema mantenha-se sempre em funcionamento minimizando as possibilidades de travamento diante de oscilações de energia, foi utilizada um circuito de reset chamado EM6353. Este circuito monitora a tensão de alimentação e gera o sinal de *reset* apropriado após um tempo fixo. Este componente possui como um de seus parâmetros uma tensão de limite que garante o bom funcionamento do sistema. Sendo assim, a tensão do sistema não pode ser inferior à tensão de limite o que ocasionaria um *reset* do sistema. Sendo assim,

para esta situação foi adotado um circuito de *reset* com tensão limite.

Paralelamente a este circuito de *reset*, foi inserido um *jumper*, CN13, para possibilitar um *reset* manual do sistema pelo desenvolvedor. Para gerar um *reset* manual, basta colocar em curto os pinos desde conector por um curto intervalo de tempo.

3.3.1.3 Led de sinalização

Com o objetivo de dar uma resposta visual quanto ao correto funcionamento do sistema, foi inserido no projeto um LED de sinalização do funcionamento da CPU. Este, além de sinalizar que o sistema está em funcionamento, ele também foi utilizado para verificação e validação de funções durante a etapa de desenvolvimento do *firmware*.

Foi adotado um sinal de 2 Hz para demonstrar o correto funcionamento da CPU.

3.3.1.4 Jumper de operação

Com o objetivo de auxiliar no desenvolvimento e atualização do *firmware* foi adicionado ao projeto um *jumper* de configuração do modo de operação. Basicamente, o *jumper* CN2, permite alternar entre modo de operação normal, posição 1-2, e modo de operação gravação, posição 2-3.

Caso o equipamento esteja em funcionamento, modo normal, e se deseje mudar para modo de gravação, se deve comutar a chave CN2 para a posição 2-3 e na sequencia gerar um pulso no *reset* através do conector CN13.

3.3.2 ACIONAMENTO POR CONTATO SECO

Este circuito foi projetado, principalmente, para acionamento de fecho elétrico, fechadura elétrica ou eletromagnética. Para acionamento destes dispositivos foi utilizado no circuito um relé em miniatura com descrição TR5V L –S-Z. Sua escolha foi baseada na necessidade de reduzir as dimensões da placa principal do equipamento auxiliando em sua adaptação no gabinete definido.

O relé possui potência máxima de comutação, para uma tensão de 240 VA, de 48 *Watt* (W) e uma tensão de acionamento de 12 V. Para seu acionamento, foi utilizado um transistor do tipo NPN como chave na configuração emissor comum (EC).

O diodo D3 na figura 18, paralelo a bobina, é um diodo de roda livre. Sua função é proteger o transístor contra danos provenientes da tensão reversa gerada pela bobina.

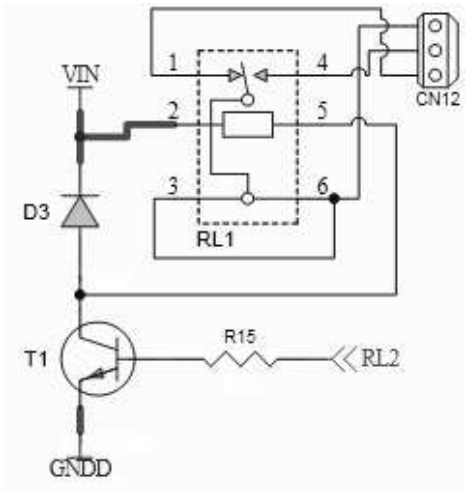


FIGURA 18 - Circuito de acionamento da saída à relé.

O terminar RL2, ligado a base do transístor, está conectado diretamente ao uC. Um nível lógico alto aplicado a este terminal aciona o relé e um nível baixo o desaciona.

3.3.3 ACIONAMENTO POR RF

Este módulo tem por finalidade disponibilizar a opção de acionamento, como no acionamento por contato seco, de fecho elétrico, fechadura elétrica ou eletromagnética, todavia sem fio. Apesar deste foco, pode ser utilizado para acionamentos diversos de acordo com a necessidade.

Para implementar este recurso foi associado a esta solução um receptor para controle remoto, produto fabricado pela empresa HDL da Amazônia Ltda. Sua característica de seleção da tecla de acionamento, existente no controle, permite que o controle de aceso biométrico possua até 4 saídas de acionamento sem fio.

Como módulo de transmissão, foi inserido na placa principal o circuito transmissor de um controle remoto. Este utiliza um o componente HCS201 para gerar o sinal de transmissão codificado. Este é um componente projetado especificamente para utilizações de segurança. Durante seu processo de fabricação é programada, em uma EEPROM interna, uma chave criptografada que tem a função de código de fabricação único o que garante maior segurança no sistema.

A transmissão do código correspondente, a uma das saídas, se faz aplicando aos terminais FECHO_0, FECHO_1 e FECHO_2 a lógica apresentada na tabela 7:

TABELA 7 - Lógica de controle dos acionamentos.

Terminais	Nível Lógico dos Sinais			
	Saída	FECHO_2	FECHO_1	FECHO_0
Código	0	0	0	0
	1	0	0	1
	2	0	1	0
	3	0	1	1
	4	1	0	0

Os terminas de controle, responsáveis pelo acionamento das saídas foram conectados diretamente ao uC.

O componente HCS201 permite ser alimentado com tensões que variam de 0,3 até 13,5 V, desta forma, foi optado alimentar este módulo com 12 V aumentar a potência de transmissor. A tabela 8 e a figura 19 apresentam as especificações técnicas e a imagem do módulo receptor utilizado.

TABELA 8 - Especificação do Receptor para Controle Remoto HDL.

Modelo	Receptor Adicional para Controle Remoto
Código	90.02.02.054
Instalação Elétrica	4 fios (2 para rede elétrica e 2 para a carga acionada)
Tensão de Acionamento	127/220 V no plugue de saída potência máxima de acionamento 300 W
Número de Transmissores	Até 63 transmissores programáveis no receptor
Ajustes	Jumper de seleção (1 a 4) da tecla de acionamento
Frequência de Transmissão	433,92 MHz
Alimentação	127/220 V

FONTE – HDL, 2012.

FIGURA 19 - Receptor Adicional para Controle Remoto.

FONTE – HDL, 2012.

3.3.4 EEPROM

A adição de uma *Electrically-Erasable Programmable Read-Only Memory* (EEPROM) no hardware do projeto está ligada a identificação da necessidade do armazenamento de dados de configuração. Estes dados poderiam ser armazenados na própria memória flash do uC, entretanto, durante a fase de desenvolvimento do firmware essa prática não seria produtiva já que ao reprogramar o firmware se perderiam os dados de configuração.

Foi utilizada no projeto uma memória serial modelo 24AA256. Este componente possui uma interface de comunicação *2-Wire Serial* (I2C) Este componente tem a capacidade de operar na faixa de 1,7 V até 5,5 V o que auxiliou na sua integração ao sistema.

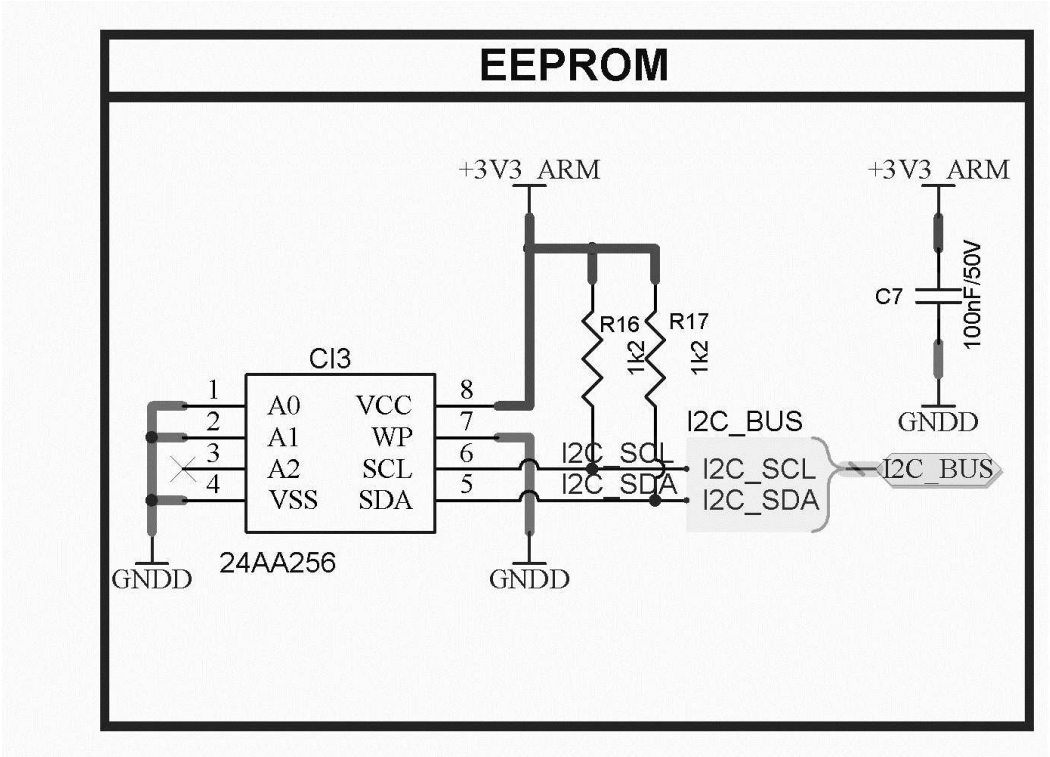


FIGURA 20 - Circuito do módulo de memória EEPROM.

Durante a etapa de projeto do hardware, foi prevista a utilização deste componente com encapsulamento *Micro Small*

Outline Package (MSOP). Desta forma, segundo a folha de dados do componente, se deve garantir nível lógico baixo nos terminais de endereçamento A0 e A1. A figura de número 20 apresenta o circuito elétrico utilizado.

Foram inseridos resistores de pull-up nos sinais de sincronismo e dados para garantir o nível lógico no barramento, principalmente, devido ao último ser um terminal de coletor aberto. Importante ressaltar que os pull-ups apresentam-se na faixa de 2 kilo ohms (kΩ) para que o circuito opere com frequências entre 400 kilo Hertz (kHz) até 1 MHz. (MICROCHIP, 2012).

Para se comunicar com a memória foi utilizada a interface I2C nativa do uC.

3.3.5 SD-CARD

Este módulo deve trabalhar conjuntamente com o sistema de sinalização. Foi introduzido para desenvolvimento de funcionalidades futuras relacionadas à geração de áudio. Servirá de local de armazenamento dos arquivos de áudio. A adoção de um SD-*Secure Digital Card* (SD-Card) foi baseada em sua larga utilização no mercado atual e consequentemente fácil aquisição.

Este dispositivo fornece uma interface SPI de comunicação, sendo que opera, neste trabalho, em modo escravo. Por este motivo, através do terminal SCLK recebe um sinal de relógio fornecido pelo uC durante a comunicação.

A alimentação deste componente possui uma faixa de variação de 2,7 V até 3,6 V, sendo assim, seus terminais puderam ser conectados diretamente ao uC sem necessidade de conversões de nível. Estes terminais foram conectados em uma porta SPI nativa do uC de forma a facilitar o seu controle.

3.3.6 BUZZER

A percepção auditiva é fundamental para nossa vida cotidiana. Este tipo de percepção transpõe barreiras da linguagem possibilitando a comunicação e consequentemente a passagem de informações. Desta maneira, este módulo foi considerado fundamental na composição do produto para emitir respostas audíveis aos usuários do sistema.

Este módulo, constituído por um único componente e de mesmo nome, foi considerado assim, já que conjuntamente com o firmware proporciona, através de diferenciadas cadências, respostas do sistema ao usuário.

Foi utilizado um mini buzzer piezoelétrico que opera com tensão de alimentação de 5 V.

Para gerar as frequências necessárias para o funcionamento do buzzer foi utilizado uma saída *Pulse-Width Modulation* (PWM) nativa do uC.

3.3.7 SPEAKER

Este módulo foi assim nomeado porque proverá uma saída de áudio através de um alto falante para geração de mensagens do sistema de sinalização. Foi inserido para implementações de funcionalidades futuras de natureza descrita acima. Para tais recursos será utilizado um módulo *Digital Signal Processing* (DSP), via software, que utilize uma saída do tipo *Digital-to-Analog Converter* (DAC) nativa do uC para seu funcionamento.

Este circuito é basicamente constituído por um amplificador de áudio ligado a uma saída DAC do uC.

Para amplificar o áudio foi utilizado um circuito integrado amplificador de áudio da fabricante Motorola chamado MC34119 que pode ser visto através da figura 21.

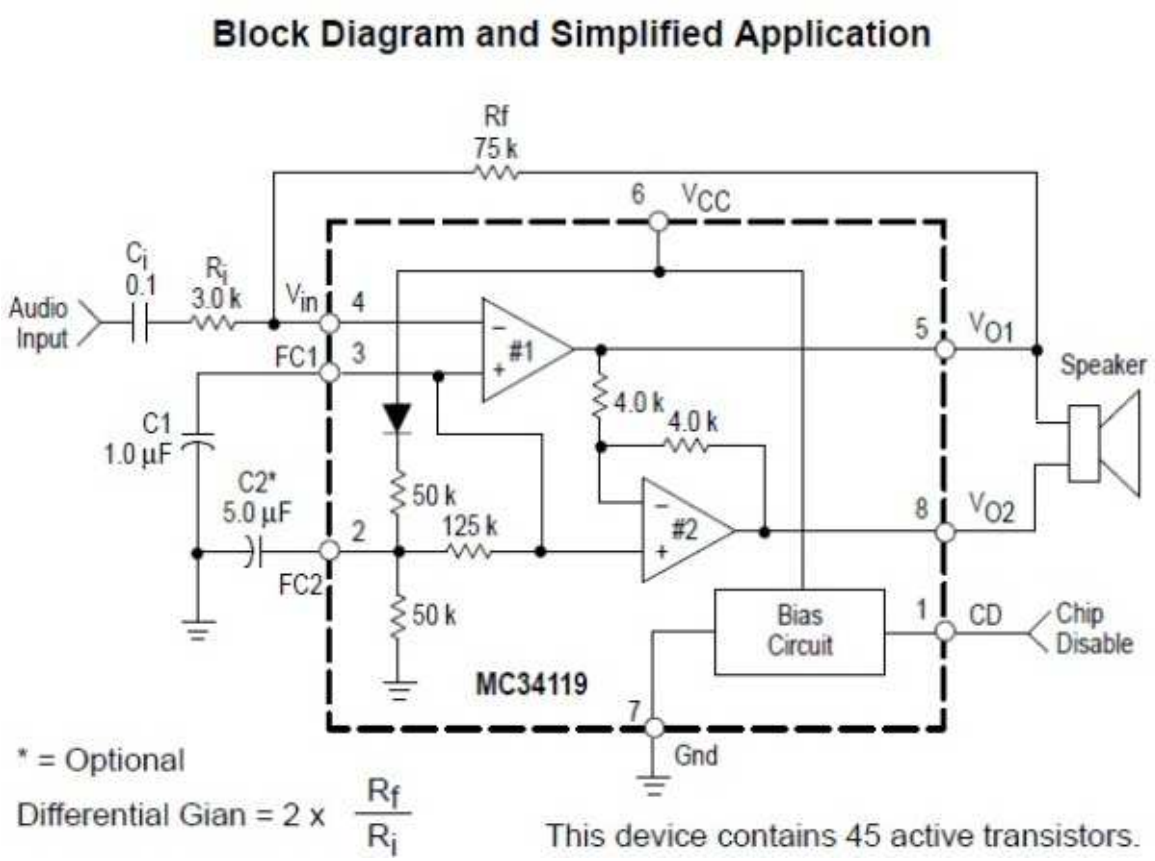


FIGURA 21 - Circuito amplificador com o C.I. MC34119.

FONTE: DATASHEETCATALOG, 2012.

O projeto do circuito amplificador foi retirado da própria folha de dados do componente e pode ser visualizado na figura acima.

3.3.8 MÓDULO BIOMÉTRICO

A leitura biométrica foi implementada através de um módulo embarcado de reconhecimento de impressão digital da empresa Suprema, chamado SFM3020-OP. A escolha deste módulo foi baseada nas suas especificações técnicas e pela acessibilidade a uma amostra o que facilitou o desenvolvimento do produto.

Este módulo possui um Digital Signal Processing (DSP) de 400 MHz que possibilita um rápido registro e identificação com tempo inferior a um segundo. Possui capacidade de

armazenamento de 1900 digitais em um megabyte (MB) de memória compatibilizando o mesmo a ser utilizado em ambientes com grande circulação de usuários. Outra vantagem é que possibilita a expansão da memória para 4 MB onde suportaria 9500 digitais armazenadas.

Acompanhado a este módulo biométrico vem um sensor óptico com resolução de 500 *dots per inch* (dpi) o que proporciona uma alta qualidade na imagem da impressão digital. Como deseja se que o equipamento possa ser utilizado em ambientes com grande circulação de usuários foi optada pela utilização do sensor óptico que acompanha o produto. Este sensor possui uma superfície de leitura sólida resistente. Apesar disso, o módulo biométrico utilizado suporta a utilização de outros modelos de sensores, como sensores capacitivos. Para alterar o sensor basta reconfigurar um dos parâmetros do módulo relacionado ao tipo de sensor utilizado. Esta flexibilidade permite que o produto possua variações em sua composição de forma a atender situações de aplicação diferenciadas.

Este módulo é alimentado com tenção de 3,3 Volts (V) e possui um consumo máximo de 150 miliampère (mA) durante o processo de escaneamento e identificação.

E disponibilizado através dos conectores J1 e J2, figura 22, duas interfaces seriais ao usuário de tecnologia complementary metal-oxide-semiconductor (CMOS) com nível de 3,3 V. Através do conector J4 se conecta o sensor biométrico.

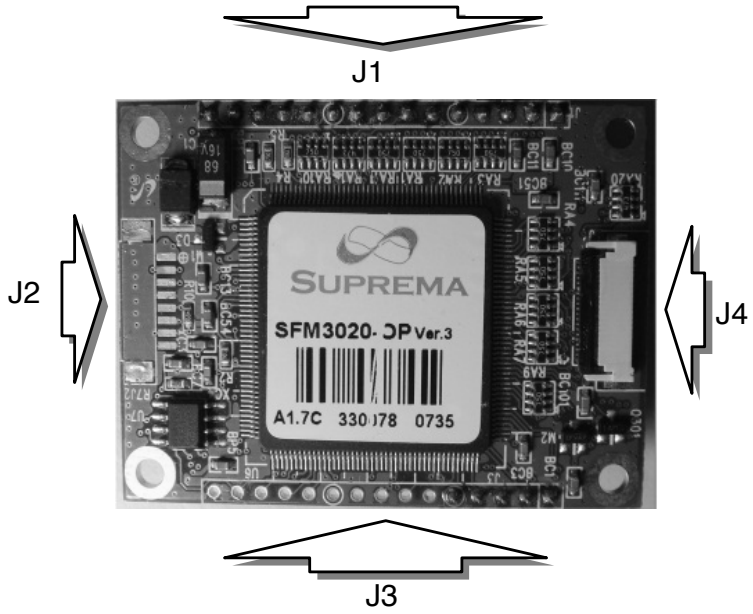


FIGURA 22 - Módulo biométrico SFM3020-OP.

Primeiramente, para se certificar do funcionamento do módulo, foi necessário o desenvolvimento de um protótipo físico, apresentado na figura 23. Através deste, foi possível validar as conexões e dar os primeiros passos no desenvolvimento do protocolo de comunicação. Para isso, foi utilizada uma placa de desenvolvimento do uC LPC2136 que fornece tensões de 3,3 V e é capaz de alimentar o módulo biométrico.

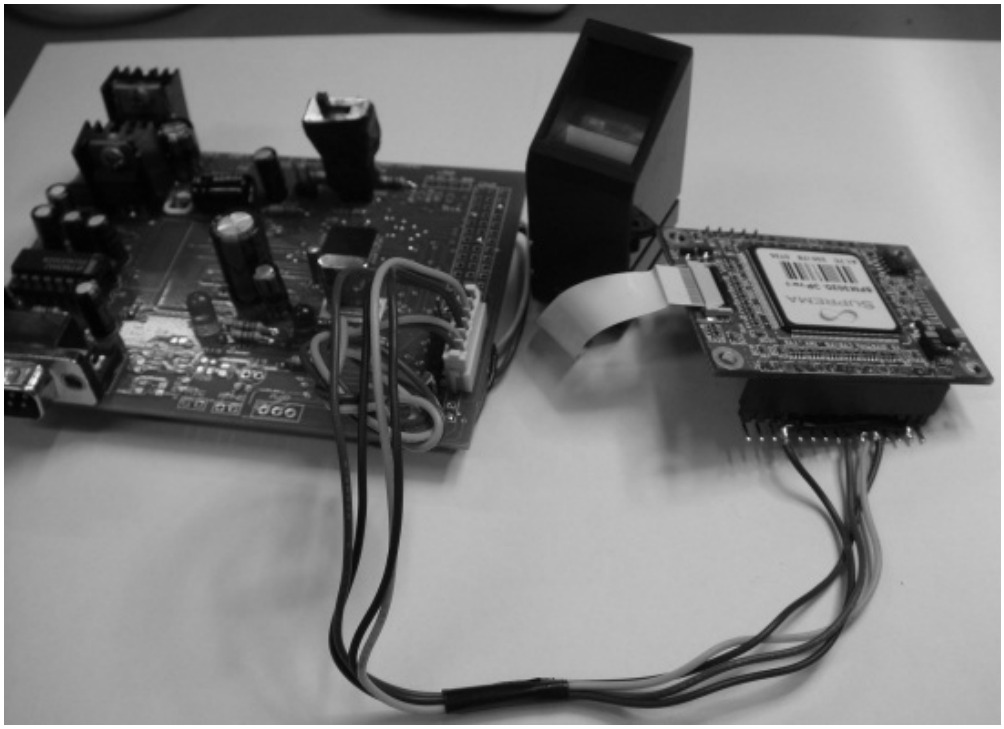


FIGURA 23 - Protótipo físico para testes do módulo biométrico.

TABELA 9 - Terminais utilizados na integração do módulo.

Pino	Descrição
4	Terra
9	Alimentação do módulo 3,3 V
10	Terminal de recepção de dados
11	Terminal de transmissão de dados
14	Terra

A tabela 9 apresenta os terminais utilizado na conexão do módulo biométrico.

3.3.9 MÓDULO TECLADO

Neste projeto foi utilizado um teclado numérico parte de um controle de acesso código 90.02.02.127, produto pertencente à empresa HDL da Amazônia Ltda. Este produto pode ser visualizado na figura 24.

O Teclado utilizado é do tipo Matricial e é constituído por quatro linhas e três colunas. Seu tratamento é realizado exclusivamente pela CPU. Neste além das teclas numéricas existe uma tecla de cancelamento e outra com o símbolo de asterisco. Apresenta teclas iluminadas para sua utilização noturna.

FIGURA 24 - Teclado do controle de acesso HDL.

FONTE - HDL, 2012.

3.3.10 MÓDULO DE DISPLAY

Este módulo se apresenta como uma das interfaces de saída existentes neste projeto. Possui os objetivos de informar, visualmente, estados, orientações, informações e opções do sistema para o usuário.

Foi optado por utilizar aqui um display gráfico possibilitando a montagem de telas para orientação do usuário além de agregar mais valor ao produto. A solução encontrada e de baixo custo foi à utilização do display presente no aparelho de celular da Nokia 3310, figura 25. Estes displays, como outros no mercado, utiliza o controlador PCD8544, que por sua vez,

disponibiliza um barramento do tipo *Serial Peripheral Interface* (SPI) de comunicação o que facilitou sua integração. (NXP, 2012).

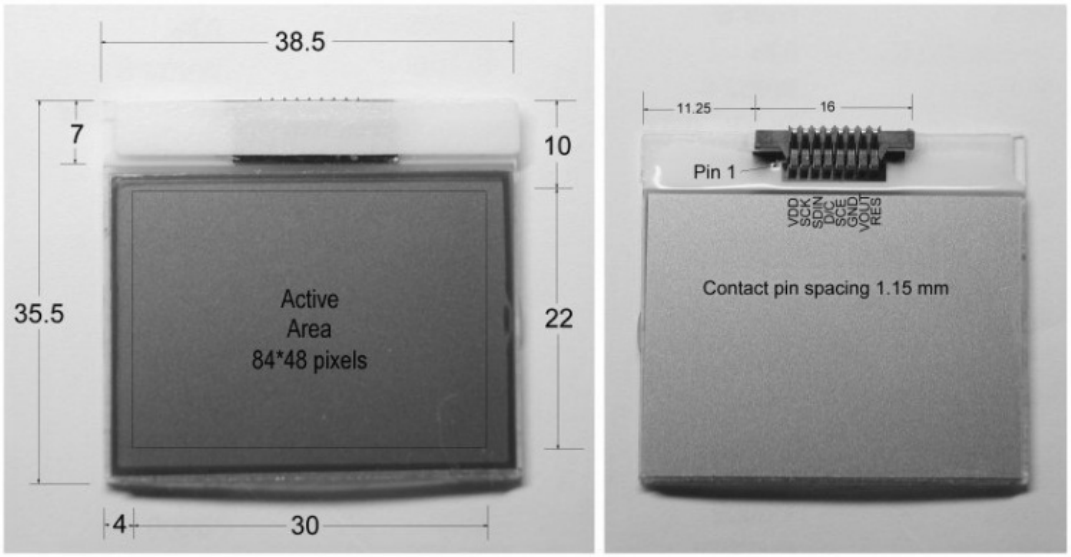


FIGURA 25 - LCD com controlador PCD8544.

Na tabela 10 é apresentado os terminais presentes no display, provenientes do controlador e suas funcionalidades.

TABELA 10 - Pinagem do controlador PCD8544.

Símbolo	Descrição
VDD	Entrada da alimentação 3,3 V.
SCK	Entrada do sinal de sincronismo (clock).
SDIN	Entrada serial de dados.
D/C	Seleção de tipo de dado (Dado/Comando).
SCE	Habilitador do chip
GND	Terra.
VOUT	Entrada do contraste.
RES	Entrada do sinal de reset.

FONTE: Do autor, 2012.

Nesta etapa do projeto, com o objetivo de testar o hardware e depurar o a biblioteca de controle do display, foi construído um protótipo físico com um display proveniente de um celular Nokia 3310. Este protótipo é apresentado na figura 26. Para isso, foi utilizada uma placa de desenvolvimento com o uC LPC2136. As conexões ao LCD foram realizadas com uma placa de refugo de um antigo teclado de telefone. Esta foi escolhida, pois o passo das trilhas, do contato de uma tecla, era compatível ao passo dos terminais do display.

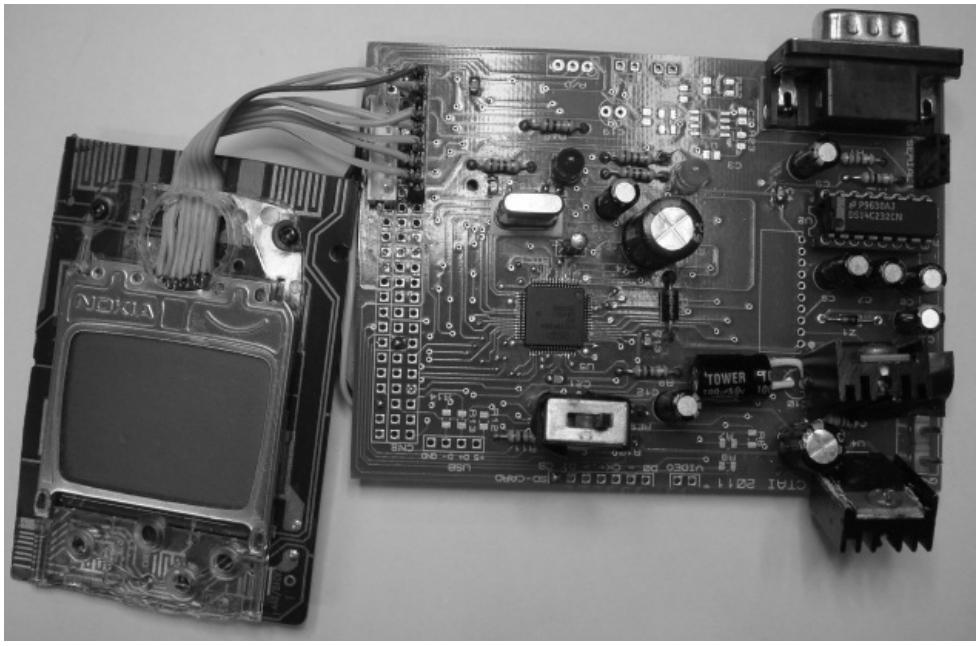


FIGURA 26 - Protótipo físico para teste do LCD.

Posteriormente aos testes realizados com o protótipo foi adquirido um módulo gráfico com display o mesmo display. O display foi adquirido através do site da empresa *Deal Extreme* (DX), site de compras chinês. Infelizmente, logo após a compra, a versão deste produto saiu de linha, mas há outras opções similares disponíveis no mesmo site.

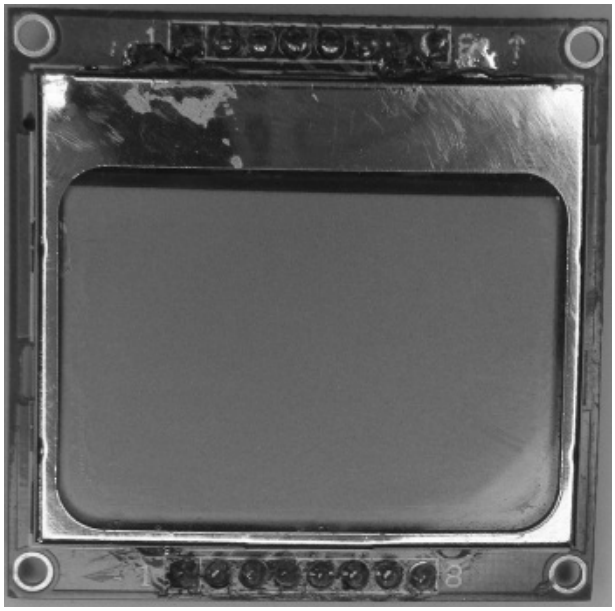


FIGURA 27 - Módulo Nokia LCD (V1.0).

3.3.11 MÓDULO DE COMUNICAÇÃO WI-FI

O módulo de comunicação tem o propósito de disponibilizar uma interface de comunicação com um computador que, por sua vez, pode possuir um software instalado com o fim de programar e gerenciar dados do equipamento.

O funcionamento deste módulo é baseado no módulo XBee Wi-fi RPSMA RF. Este pode se comunicar com o uC através de uma interface *Universal Asynchronous Receiver/ Transmitter* (UART) ou por uma interface SPI. Para integrar o módulo XBee ao uC foi utilizada a sua interface UART.

Sua configuração é realizada através de comandos AT. Os bytes de dados são constituídos por um start bit, oito bits de dados e um stop bit. Opera na frequência de 2.4 GHz.

FIGURA 28 - Módulo XBee Wi-Fi 802.11.

FONTE – INDIA, 2012

Para integrar o módulo XBee Wi-Fi, figura 28, ao projeto foram utilizados os seguintes terminais apresentados na tabela 11.

TABELA 11 - Pinagem do Módulo XBee Wi-fi utilizados para integração.

Pino	Descrição
1	Vcc (3,1 – 3,6 V)
2	Dout – Saída de dados do módulo
3	Din – Entrada de dados do módulo
10	GND -
13	Indicador de status do módulo
15	Indicador de associação. Indica a conexão.

Este módulo durante uma operação de recepção consome 140 mA e durante a transmissão, no máximo, 190 mA. É observado, em sua folha de dados, que deve existir um Ripple máximo de 50 mV para seu correto funcionamento. (Digi, 2012).

3.3.12 MÓDULO DE ALIMENTAÇÃO

Por questões de custo e praticidade, este projeto não teve como um dos objetivos o projeto e construção de uma fonte definitiva para o produto. Sendo assim, o foco deste módulo foi prover o fornecimento dos níveis de tensão, dentro das especificações necessárias, para os demais módulos do sistema.

Em primeiro lugar, a fim de diminuir a interferência entre os módulos, o potencial de terra do projeto foi dividido em potencial de terra analógico e potencial de terra digital como pode ser visto na figura 29.

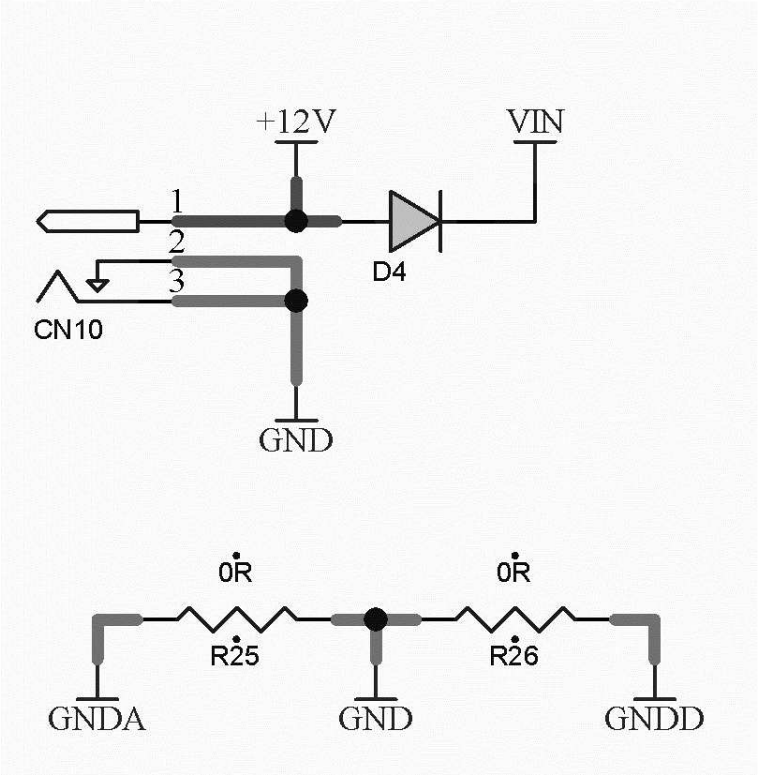


FIGURA 29 - Isolamento dos potenciais de terras analógico e digital.

Esta prática é necessária visto que ruídos provenientes do circuito digital podem ser transmitidos para os circuitos analógicos transformando-se em ruídos.

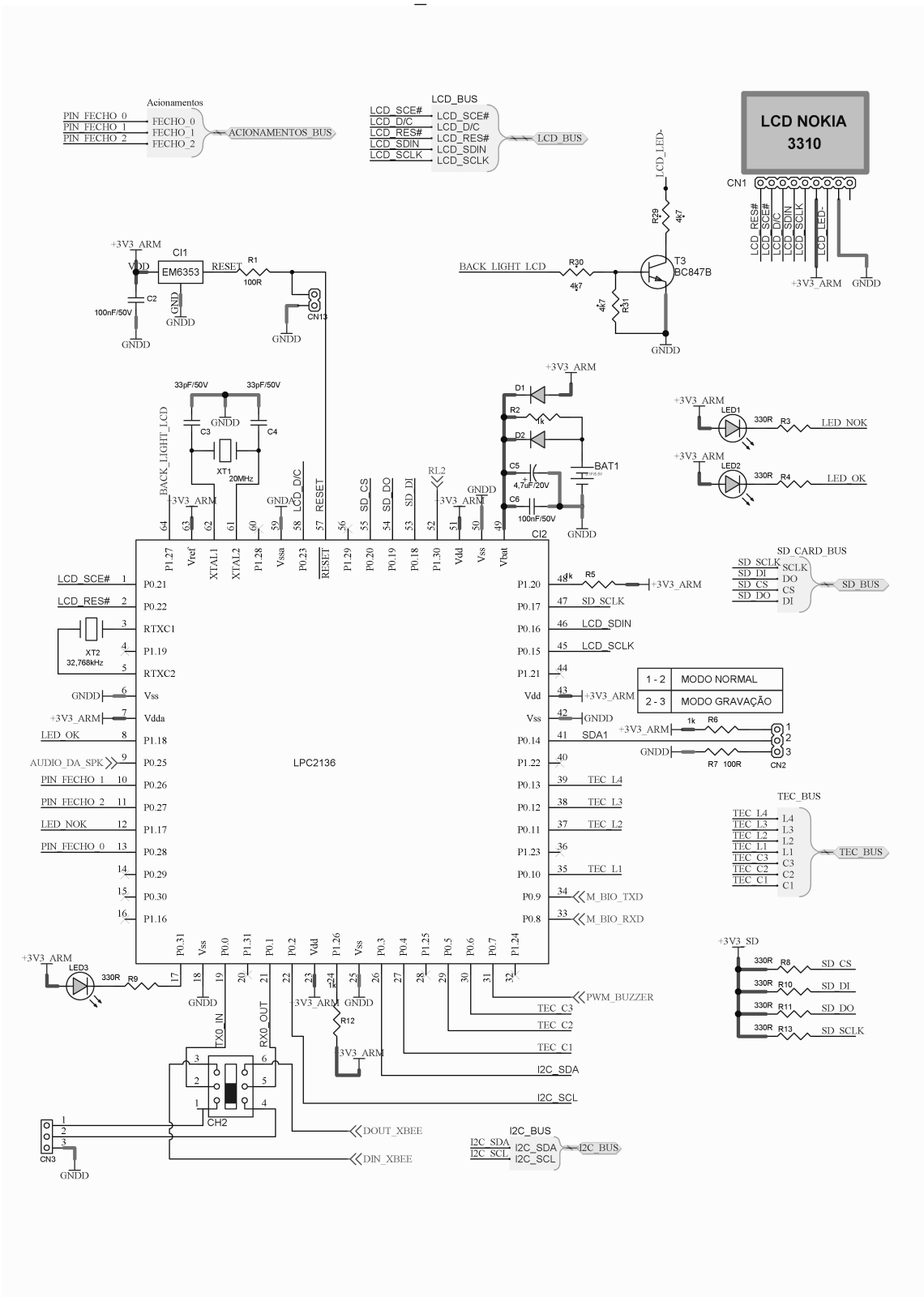
Na prática, os potenciais de terra são interconectados, no entanto, somente em um ponto.

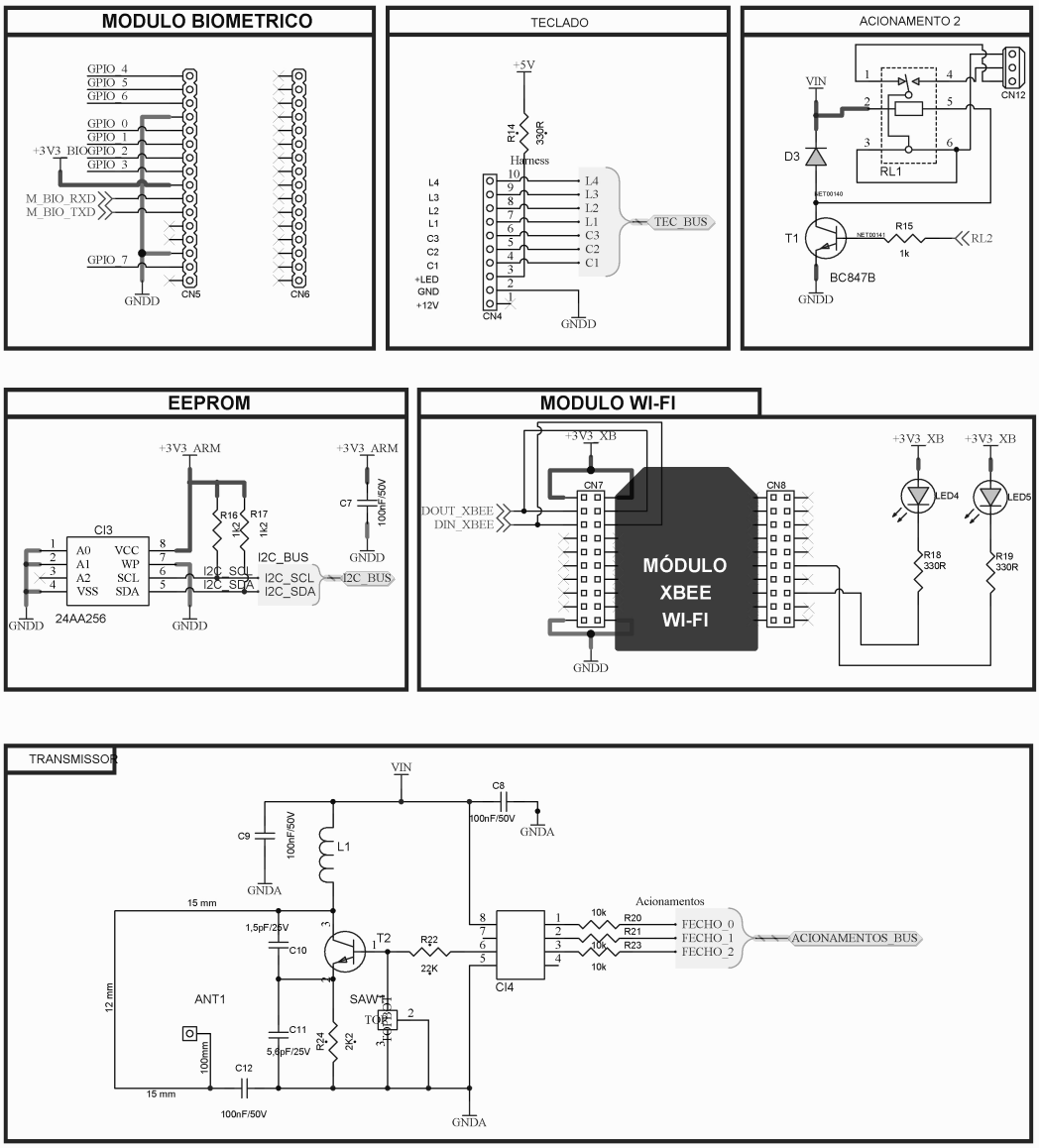
Basicamente, este módulo somente realiza a redução dos níveis de tensão necessários para cada um dos módulos.

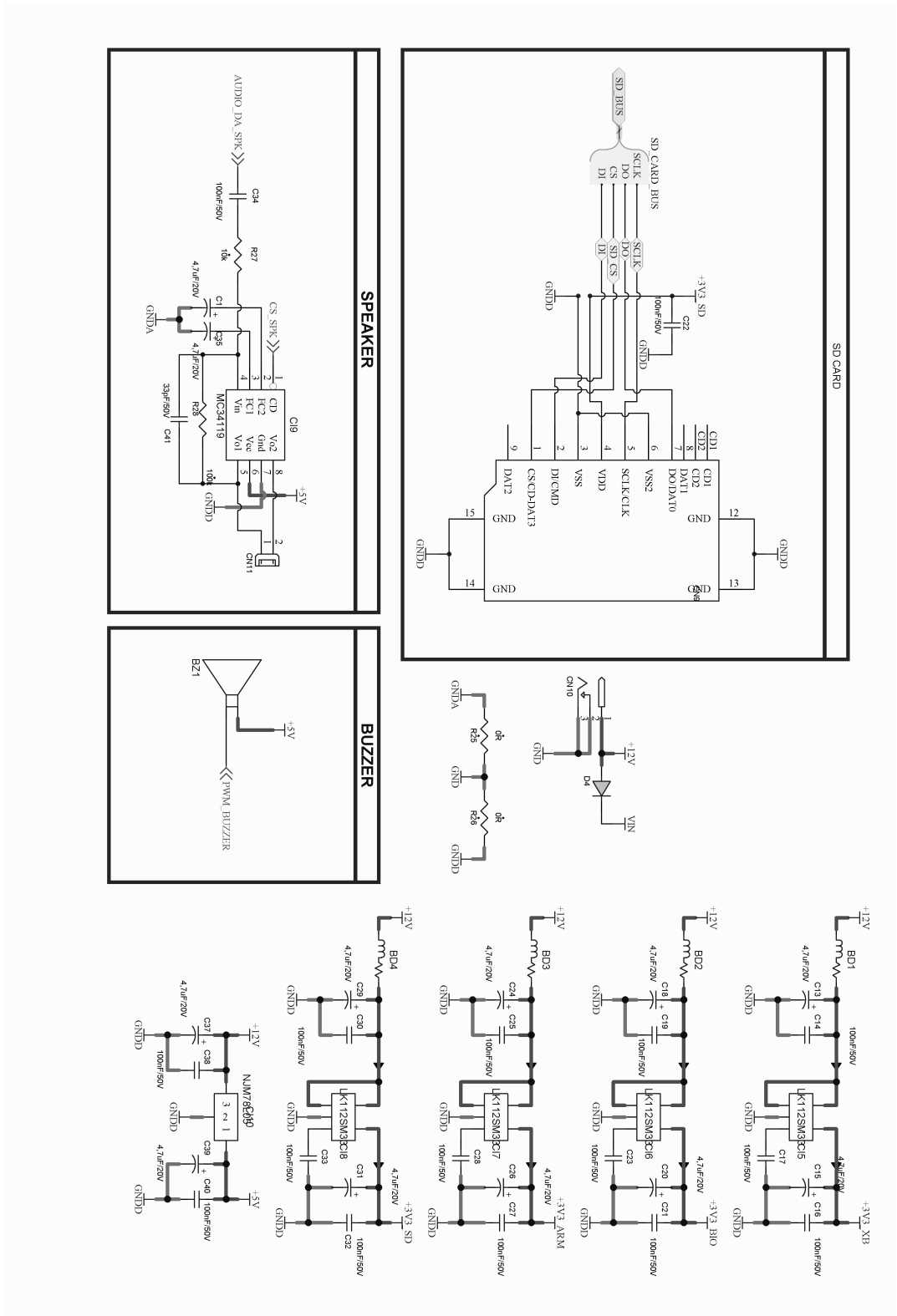
Com o intuito de reduzir as dimensões do circuito, foram utilizados reguladores de tensão de tecnologia SMD nos circuitos alimentados com 3,3 V. Outro grande motivo de sua escolha foi o fácil acesso a estes componentes. Embora de dimensões reduzidas, um componente não seria capaz de fornecer energia para todos os módulos. Sendo assim, os módulos de consumo mais críticos, foram divididos para que os circuitos reguladores tivesse potência suficiente para mantê-lo adequadamente. Além disso, a separação das alimentações contribuiria nos testes iniciais, já que possibilitou ligar os módulos um a um.

Além da alimentação dos módulos de potencial 3,3 V, a fonte necessitou ter uma etapa de redução para 5 V. Esta é necessária para a alimentação do backlight do teclado, circuito de áudio e buzzer.

3.3.13 ESQUEMÁTICO




MODULO BIOMETRICO
GPIO_4
GPIO_5
GPIO_6
GPIO_0
GPIO_1
+3V3_BIO
GPIO_2
GPIO_3
M_BIO_RXD
M_BIO_TXD
GPIO_7
GNDD
CN5
CN6
TECLADO
+5V
R14
330R
Harness
L4
L3
L2
L1
C3
C2
C1
+LED
GND
+12V
CN4
TEC_BUS
GNDD
ACIONAMENTO 2
VIN
CN12
D3
RL1
T1
R15
1k
RL2
BC847B
GNDD
EEPROM
+3V3_ARM
+3V3_ARM
R16
R17
1K2
1K2
C7
100nF/50V
CI3
A0
A1
A2
VSS
VCC
WP
SCL
SDA
I2C_BUS
I2C_SCL
I2C_SDA
I2C_BUS
GNDD
24AA256
GNDD
MODULO WI-FI
+3V3_XB
CN7
CN8
DOUT_XBEE
DIN_XBEE
MÓDULO
XBEE
WI-FI
+3V3_XB
+3V3_XB
LED4
LED5
R18
330R
R19
330R
GNDD
TRANSMISSOR
VIN
C8
100nF/50V
GNDA
C9
100nF/50V
L1
GNDA
15 mm
1,5pF/25V
C10
T2
R22
22K
Acionamentos
10k
R20
10k
R21
10k
R23
10k
FECHO_0
FECHO_1
FECHO_2
ACIONAMENTOS_BUS
CI4
ANT1
SAW1
12 mm
C11
5,6pF/25V
R24
2K2
100mm
C12
15 mm
100nF/50V
GNDA


SD CARD
SD CARD_BUS
SD_BUS
SCLK
DO
CS
DI
+3V3_SD
GNDD
100nF/50V
C22
CD1
CD2
DAT1
DO/DAT0
VSS2
SCLK/CLK
VDD
VSS
DI/CMD
CS/CD-DAT3
DAT2
GND
SPEAKER
AUDIO_DA_SPK
CS_SPK
MC34119
CI9
C34
C35
C41
R27
R28
C1
4,7uF/20V
33pF/50V
10k
GNDA
CN11
+5V
BUZZER
BZ1
PWM_BUZZER
CN10
D4
+12V
VIN
R25
R26
BD1
BD2
BD3
BD4
LK112M33C15
LK112M33C16
LK112M33C17
LK112M33C18
C13
C14
C15
C16
C18
C19
C20
C21
C24
C25
C26
C27
C29
C30
C31
C32
C33
C23
C28
C17
+3V3_XB
+3V3_BIO
+3V3_ARM
NJM78L05
C37
C38
C39
C40
100nF/50V
4,7uF/20V

3.3.14 PROTOTIPAGEM DO HARDWARE

Após ter definido a estrutura dos módulos e por fim a construção do esquemático foi iniciada a etapa de projeto do layout da placa principal. Tanto o esquemático quando o layout da placa principal foi construído na ferramenta Altium Designer Release 10.

Primeiramente, já com o gabinete do produto definido, delimitou-se o tamanho da placa e seus pontos de encaixe e fixação. Para facilitar esta etapa foi importada a base do gabinete que foi escolhida para utilização. Este modelo analítico em 3D auxiliou no posicionamento dos pontos descritos acima. Sendo assim, basicamente, as furações necessárias foram sobrepostas aos existentes no modelo. Evidentemente, a placa possui dimensões inferiores, a área interna do gabinete, para que possa ser encaixada.

Posteriormente, foi realizado o agrupamento dos componentes de comum módulo para evitar a necessidade de rotear trilhas muito longas desnecessariamente. Logo em seguida, realizou-se um trabalho de posicionamento dos grupos de componentes no interior da área limitada à placa. Inquestionavelmente, a utilização do protótipo contribuiu para que os componentes, principalmente os de maior porte, não fossem sobrepostos considerando suas três dimensões. Como exemplo, pode se citar o posicionamento do componente XT1. Inicialmente este seria posicionado entre os conectores CN7 e CN8, figura 30, contudo foi observado, através da angulação da imagem em três dimensões, que o mesmo não permitiria o encaixe adequado do módulo Wi-Fi.

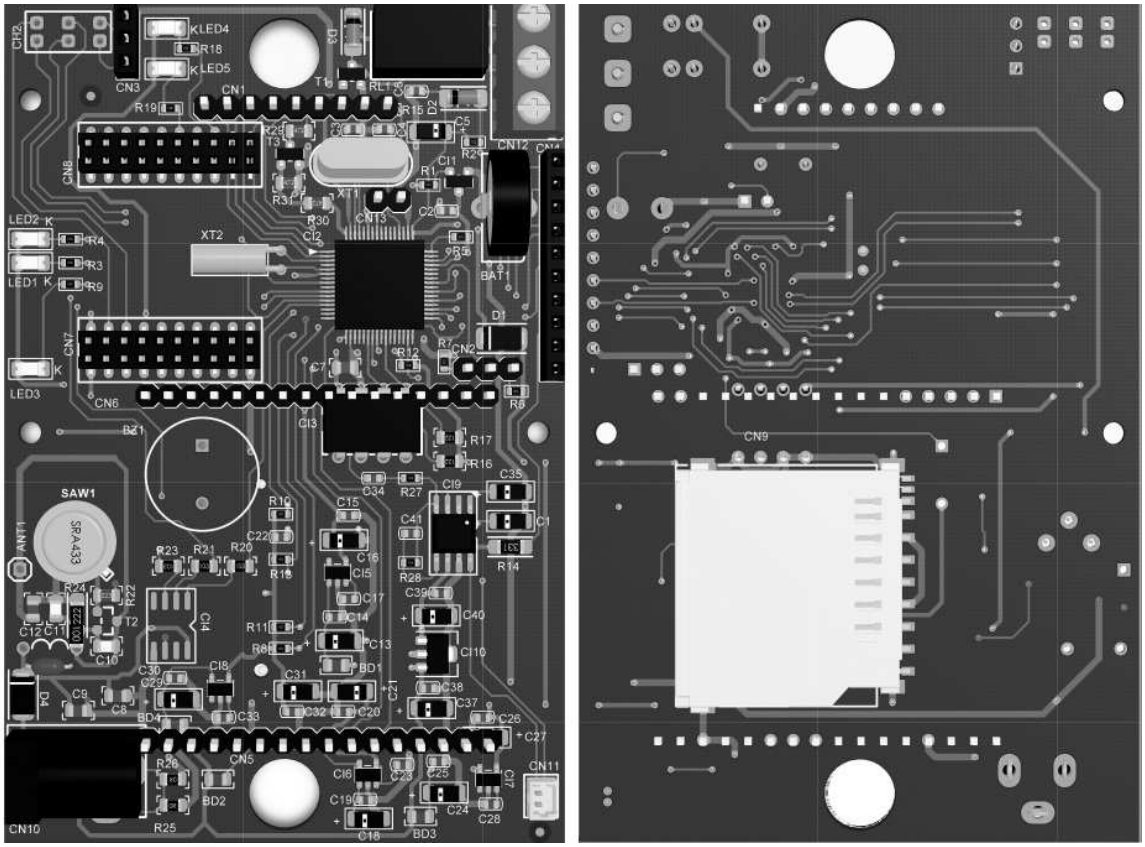


FIGURA 30 - Protótipo analítico da placa principal.

Para auxiliar o trabalho de desenvolvimento das funcionalidades foram previstos alguns componentes no projeto do PCB. Como exemplo há o conector CN10 que foi previsto para a conexão de um plug de alimentação externa. Em um produto final, não seria prudente um conector de alimentação destacável que permite que usuários o manipulem.

Módulo Wi-Fi foi posicionado de forma a exteriorizar a conexão da antena. Como a mecânica escolhida tem uma cobertura em aço inox, esta podia gerar reflexão e em virtude disso reduzir a eficiência da radiação do sinal.

Da mesma forma, para minimizar os efeitos de reflexão, o módulo de acionamento por RF, de frequência 433,92 MHz, também foi posicionado na borda do PCB.

Por fim, com os posicionamentos definidos e as trilhas roteadas se deu início a confecção de um protótipo físico. Através do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina confeccionou-se o protótipo da placa principal

deste projeto. Abaixo, figura 31, se pode visualizar as duas faces a placa montada.

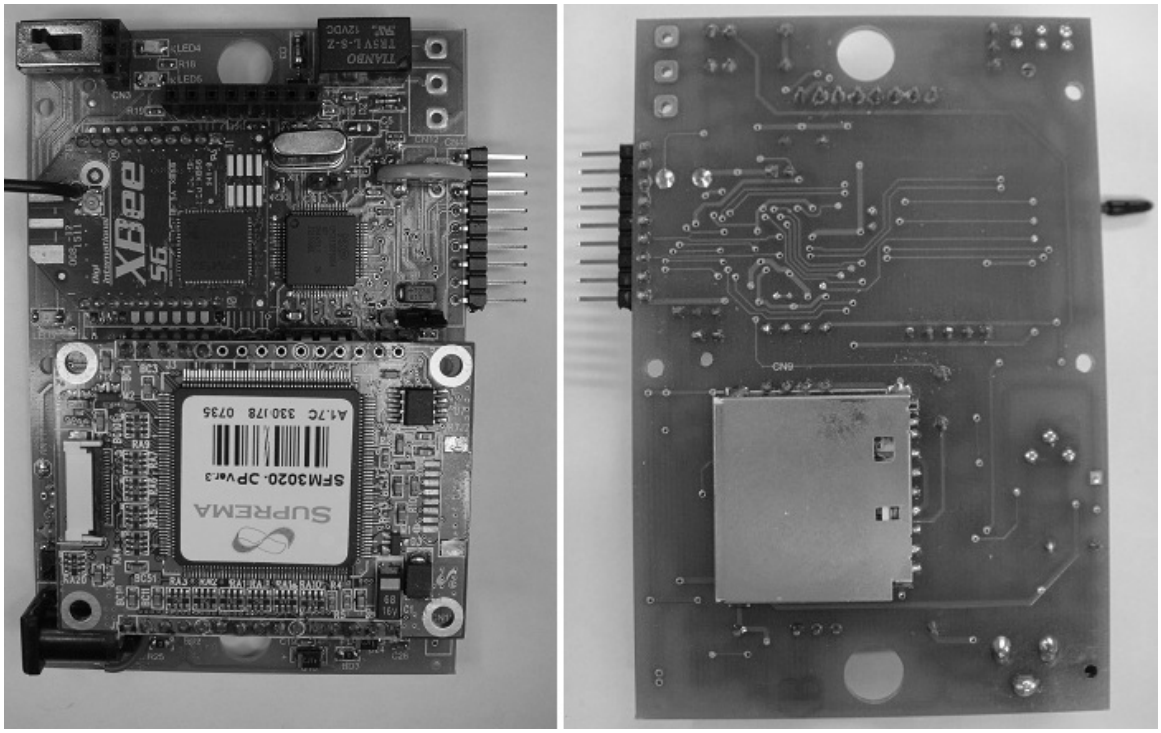


FIGURA 31 - Protótipo físico da placa principal.

Com o protótipo em mãos se deu início a validação dos módulos de forma integrada.

3.4 DESENVOLVIMENTO DO FIRMWARE

3.4.1 PADRONIZAÇÃO DO CÓDIGO FONTE

O projeto do firmware iniciou-se com a criação de um padrão de escrita de código visando à busca pela qualidade. Esta padronização do código pretende auxiliar o desenvolvimento e facilitar futuras manutenções. A adoção desta prática busca passar ao desenvolvedor e sua equipe informações através da simples leitura de seu nome.

Basicamente esta padronização de escrita do código foi dividida e restringida à declaração de funções, variáveis e definições.

Os padrões utilizados foram criados de acordo com as necessidades identificadas, sendo assim, podem não estar previstas e registradas todas as situações existentes.

Nas funções a aplicação da padronização foi adotada na construção dos protótipos. Para isso foram definidas regras que são apresentadas na tabela 12:

Tabela 12 - Padronização adotada em funções.

1	As funções devem ser iniciadas com uma letra ou sequencia de letras, em minúsculo, correspondentes ao tipo de retorno.
2	Caso não haja retorno na função a sua identificação é omitida.
3	Caso haja retorno, a primeira letra da primeira palavra do nome da função deve ser em Maiúsculo. Caso contrário a primeira letra da primeira palavra deve ser em Minúsculo.
4	As letras iniciais das palavras subsequentes, pertencentes ao nome, devem ser em Maiúsculo.
5	Caso a função seja publicado no arquivo .h, esta deve possuir como prefixo o nome do módulo a qual pertence separado do seu nome por um caractere de underscore (_).

Com a adoção do padrão os protótipos devem possuir a seguinte estruturação permitindo as variações previstas nas regras acima:

NomeDoMódulo_tipo+NomeFunção()

Quanto aos argumentos das funções, estes se aplicam as regras voltadas as variáveis que serão apresentadas na sequencia.

A padronização das variáveis, na escrita do código, buscou identificar as variáveis com seu tipo, escopo e sua função. Para isso, foram aplicadas algumas regras.

A composição do nome da variável seguiu a estrutura apresentada abaixo:

Escopo+Tipo+NomeVariável

O nome da variável deve ser precedido pela letra correspondente ao seu escopo e pela contração sigla correspondente ao seu tipo respectivamente. Após este cabeçalho de identificação deve vir o nome da variável iniciado com letra maiúscula. As tabelas 13 e 14 apresentam as variações utilizadas na padronização da declaração das variáveis.

Tabela 13 - Padronização de escopo adotado as variáveis.

Sigla	Significado
G	Variável global (declarada no módulo)
L	Variável local (declarada na função)
M	Variável passada por parâmetro.

Tabela 14 - Padronização de tipo aplicado as variáveis.

Sigla	Significado
C	Char
I	Int
Uc	Unsigned char
Ui	Unsigned int
P	ponteiro

Finalizando, as definições devem ser escritas com letras em maiúsculo. Caso sejam compostas por mais de uma palavra devem ser separadas pelo caractere (_).

3.4.2 MODULARIZAÇÃO DO CÓDIGO

A modularização no projeto do firmware buscou decompor o sistema em parte a fim de entendê-lo separadamente. Nesta atividade, o trabalho também foi direcionado a obter dos módulos alta coesão, ou seja, módulos com objetivos únicos e bem definidos além de baixo grau de acoplamento entre os demais.

Diante das informações obtidas na etapa de domínio da solução se pode obter uma visão mais ampla do sistema e por consequência dividir o sistema em módulos.

Os módulos são arquivos do projeto que constituem o código fonte. Estes arquivos foram subdivididos de acordo com os serviços ou funcionalidades requeridas pelo programa. Na tabela 15 se pode observar os principais módulos do sistema.

TABELA 15 - Descrição dos principais módulos do sistema.

Módulo	Descrição
Ctl_Acesso_Bio	Comporta o software da aplicação. Responsável por gerenciar as funcionalidades do controle de acesso biométrico.
Ap_alarme	Módulo da aplicação responsável por armazenar as funções de tratamento de alarme.
Ap_configuracao	Módulo da aplicação responsável pelas funções relacionadas as configurações do sistema.
Ap_permissões	Módulo da aplicação responsável por prover funções relacionada as permissões de acesso.
Ap_Identificação	Módulo da aplicação responsável pelas funções relacionadas à identificação e liberação
Comunicação	Responsável por gerenciar a comunicação com um host e promover uma interface de comunicação do sistema.
Biometria	Responsável por gerir os processos em andamento no módulo biométrico e promove uma interface transparente para a aplicação.
Sinalização	Gerencia o processo de geração das sinalizações e disponibiliza funcionalidades transparentes para a aplicação.
Acionamento	Gerencia os processos de acionamento abstraindo o módulo e através de uma interface para a aplicação.
Display	Gerencia a comunicação com o LCD e provê métodos de apresentação de telas para a aplicação.

Teclado	Gerencia os processos envolvidos com a leitura e definição das teclas e fornece métodos transparentes para a aplicação
Memória	Gerencia processos de gravação de dados e fornece funções transparentes ao módulo.
Relógio	Responsável por promover uma interface das informações de calendário e hora para a aplicação.
FingerSFM	Biblioteca de funções para o tratamento da comunicação com o módulo biométrico.
CPU	Módulo responsável por funções de inialização da CPU e periféricos.
E2prom	Biblioteca de funções de controle da gravação dos dados na memória E2prom.
Buzzer	Biblioteca de funções de controle e definições de sons para sinalização.
Luzes	Biblioteca de funções de controle das luzes e defines.
Serial	Gerencia a comunicação através das interfaces UART.
Aplicação	
Timer	Biblioteca para inicialização das temporizações
PWM	Biblioteca para inicialização e configuração do PWM.
GPIO	Biblioteca com funções de inicialização das portas, defines.
I2C	Biblioteca para inicialização, leitura e escrita de dados pela interface I2C.
RTC	Biblioteca para inicialização, leitura e configuração do relógio interno do uC.

Este processo de divisão em módulos contribui para que o código tenha a capacidade de reusabilidade e contribui para a portabilidade do software.

Nos módulos também foi aplicada a ideia de encapsulamento. Os módulos foram isolados o máximo possível tomando se o cuidado de não publicar todas as funções existente

e proibindo a manipulação de variáveis de controle de um módulo por outros diretamente. Estas manipulações foram somente permitidas através de funções publicadas.

3.4.3 DESENVOLVIMENTO EM CAMADAS

Visando a provável portabilidade do sistema para outra plataforma foi adotado no desenvolvimento do firmware uma divisão em camadas. Cada uma das camadas disponibiliza serviços à camada imediatamente superior. Ou seja, as camadas inferiores tratam as camadas superiores como clientes.

Neste trabalho foi realizada uma divisão em três camadas:

- Camada de Aplicação;
- Camada de Serviços;
- Camada Física.

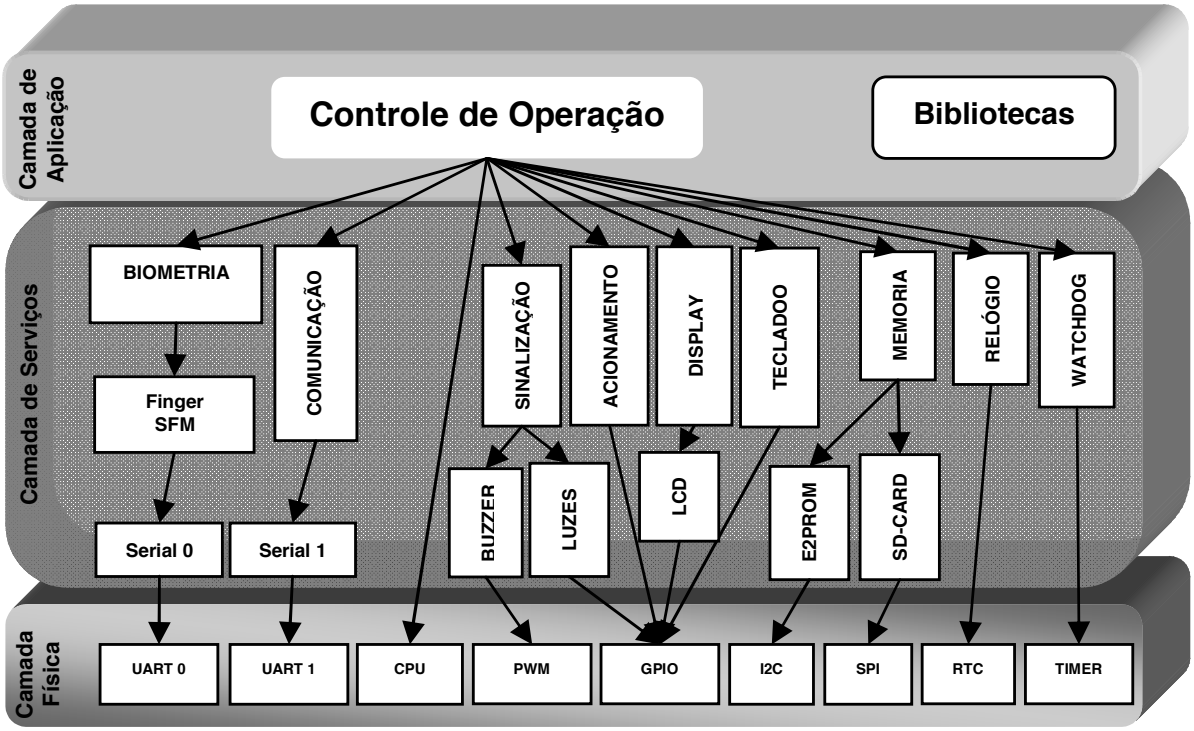


FIGURA 32 - Apresentação do sistema em camadas.

Como apresentado na figura 32, os módulos do sistema estão distribuídos de acordo com a camada que estes pertencem. A definição da camada, a qual um módulo pertence, está associado com as funções que ele deve exercer no firmware.

A camada física está diretamente ligada ao microcontrolador (uC) e a sua plataforma. Estão contidas aqui definições de registros de leitura e escrita, configurações de características dos periféricos e de funções especiais. Esta camada deve disponibilizar métodos, à camada de serviços, de forma a abstrair as características do hardware.

Foram utilizadas nesta camada bibliotecas disponibilizadas pelo fabricante do uC.

A camada superior à física, como seu próprio nome sugere, disponibiliza serviços à aplicação. Estes serviços são apresentados para a aplicação através das funcionalidades identificadas em seus módulos. As bibliotecas desta camada não devem possui dependências comuns para manter os módulos independentes entre si. Este baixo grau de acoplamento possibilita a rastreabilidade, que consequentemente, permite alterações com mais segurança. Este procedimento também permite que seja realizada a troca de um módulo sem a necessidade de alterações na camada de aplicação. Como exemplo, pode-se citar a troca do fornecedor de um módulo biométrico. Em uma situação destas, basicamente, haveria a necessidade de reescrever código para tratamento do novo módulo, desde que o mesmo disponibilize as mesmas funcionalidades e protótipos anteriormente utilizados na aplicação.

Outra vantagem na estruturação em camadas é que as camadas inferiores não tem dependência com a aplicação, sendo assim, podem ser reaproveitadas. Ou seja, futuramente pode-se expandir o escopo deste projeto para realizar controle de ponto. Para isso acontecer, bastaria reescrever a camada de aplicação utilizando as funcionalidades da camada de serviço, como já acontece.

Já a camada de aplicação é responsável em pôr na prática as regras de negócio. Aqui são utilizadas as funcionalidades

disponibilizadas pela camada de serviço para que a execução dos casos de uso identificados seja possível.

3.4.4 CODIFICAÇÃO

O programa embarcado no dispositivo, ou firmware teve sua camada física desenvolvida para ser gravado no uC LPC2136 da fabricante NXP Semiconductors. Este firmware tem a função de gerenciar o processamento das funcionalidades disponibilizadas no equipamento. Para isso é necessário fazer o gerenciamento dos processos provenientes da camada física, dos módulos de serviço e da aplicação.

A ferramenta utilizada para o desenvolvimento e gravação do firmware foi o Ambiente de Desenvolvimento Integrado (IDE) de código aberto chamado Code Blocks (CODE::BLOCKS, 2012). Esta ferramenta é configurável e pode ser utilizada em diversas plataformas. Todo o código fonte deste trabalho foi escrito em linguagem de programação C.

A explicação na íntegra da codificação dos módulos do sistema não será realizada aqui devido ao grande volume de informações que seriam necessárias descreverem neste tópico. Contudo, as implementações de código realizadas nestas etapa espelham os requisitos necessários do sistema encontrados na etapa de domínio da solução.

3.4.4.1 FLUXOGRAMA PRINCIPAL DO FIRMWARE

Basicamente o fluxo principal do firmware, figura 33, inicia com a inicialização do módulo da CPU. Este é responsável por inicializações relacionadas ao microcontrolador como sua frequência de processamento entre outras. Posteriormente a isso é realizada a inicialização dos módulos do sistema. Primeiramente módulos da camada física, na sequência da camada de serviços e finalmente da camada de aplicação.

Após o término da inicialização do sistema, o fluxo do programa fica voltado ao gerenciamento dos processos. Aqui são gerenciados processos dos módulos da camada de serviços e aplicação. Já os módulos da camada física, depois de iniciados, trabalham paralelamente através de interrupções gerenciando o recebimento e transmissão de dados.

Além dos processamentos, neste laço infinito há um controle de watch dog. Este tem a função de evitar que o software fique travado por motivos desconhecidos.

Outra função existente neste fluxo é o controle de reboot do sistema. Esta funcionalidade permite a reinicialização do sistema sem necessidade do desligamento da energia.

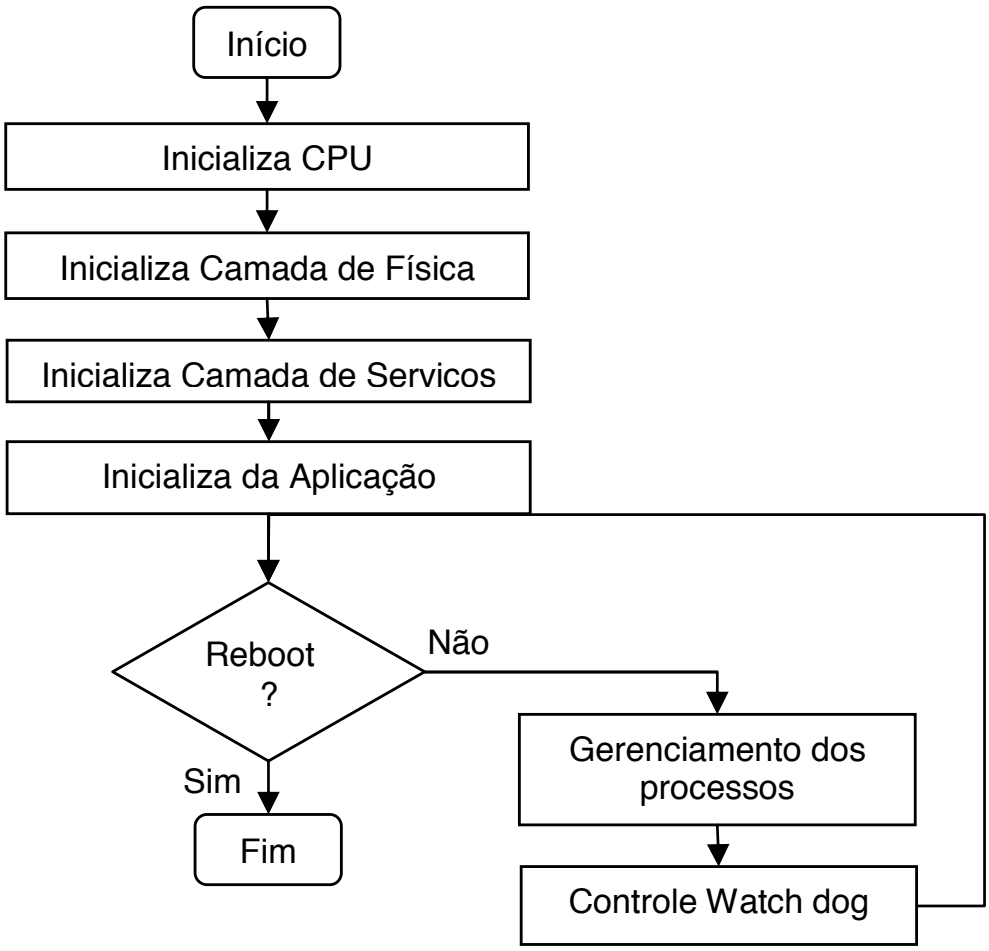


FIGURA 33 - Fluxograma principal do firmware.

Todos os gerenciamentos de processos dos módulos foram implementados com seu controle por máquina de estados. Estas muitas vezes escalonadas em mais de um nível para gerenciar os processos passo a passo e sempre evitando travar o sistema em algum ponto.

3.4.4.2 VALIDAÇÃO DAS FUNÇÕES

Os testes desenvolvidos em funções da camada de aplicação e serviços em sua grande maioria foram realizados através do desenvolvimento de programas para serem executados através do prompt de comandos

Os programas de testes foram desenvolvidos com o auxílio da ferramenta Dev-C++ versão 4.9.9.2. Basicamente, os testes procederam utilizando uma metodologia similar a da *unit testing.* Foram desenvolvidos programas de teste, nos quais, as funções que deveriam ser testadas eram chamadas e se apresentava os resultados através do prompt do dos. Nestes softwares de teste era simulada a inserção dos valores dos parâmetros e observada, quando existente sua saída.

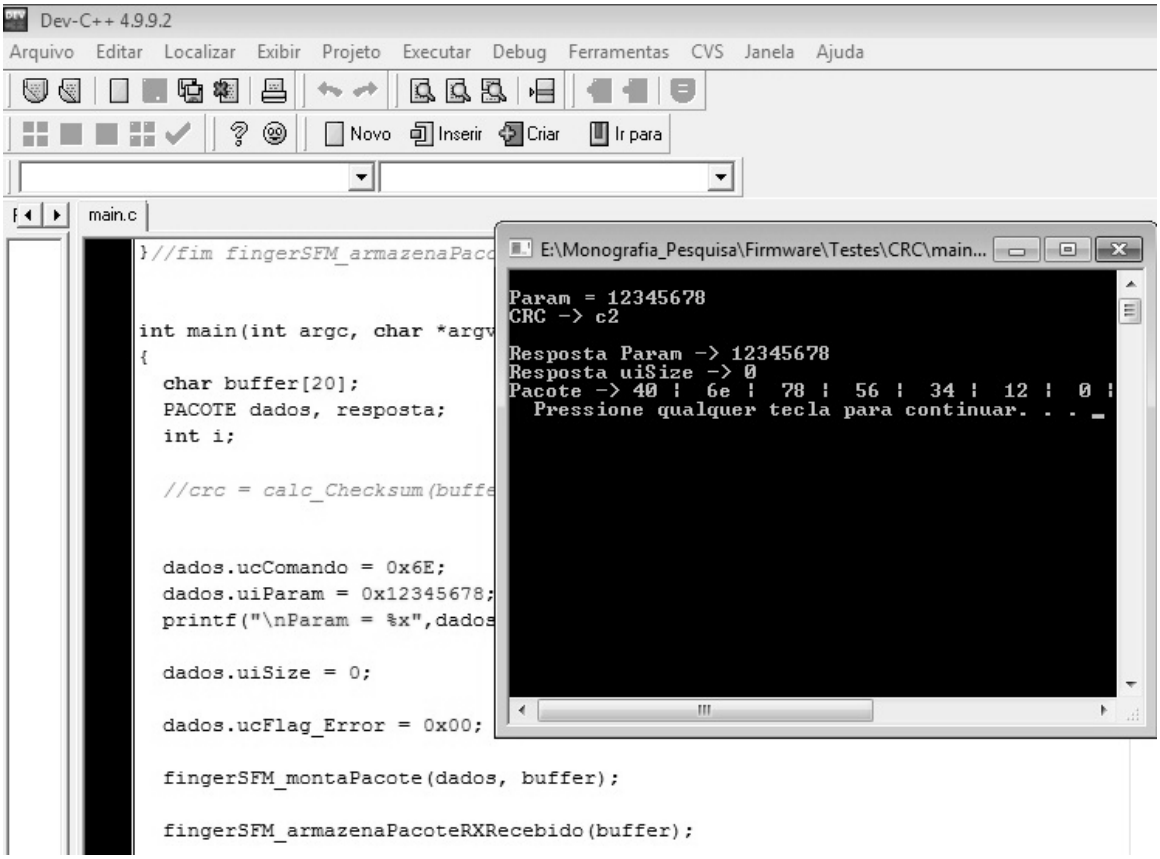


FIGURA 34 - Exemplo de teste de funções.

Na figura 34 é visualizado um programa de teste para validar algumas funções do módulo fingerSFM. Este programa chama as funções publicadas passando parâmetros de teste. Já no lado esquerdo é apresentada a tela do prompt, na qual os resultados foram impressos. O teste em questão pretendia validar se a ordem de posicionamento dos dados no pacote estava correta. O Mesmo procedimento foi adotado para realizar testes de validação do cálculo do CRC do pacote.

4 RESULTADOS E DISCUSSÕES

Como resultado do presente trabalho obteve-se um protótipo de um controle de acesso com reconhecimento por impressão digital.

Os primeiros ensaios realizados foram com o módulo biométrico conectado a placa principal do projeto. Com amostras pré-cadastradas de impressão digital, se pode avaliar a integração do módulo biométrico junto a placa principal já que por intermédio das respostas recebidas do módulo, via protocolo de comunicação, pode-se verificar a correta identificação e rejeição das impressões digitais. Desta forma, se pode validar o funcionamento do protocolo de comunicação com o módulo biométrico.

Para o desenvolvimento do estudo, o trabalho foi dividido em etapas. Primeiramente, procurou-se definir a constituição do produto. Nesta etapa foram utilizadas técnicas de engenharia de software o que auxiliou a definir o problema com maior qualidade. Este estudo contribuiu para ter uma visão mais clara e objetiva do sistema.

A etapa seguinte foi constituída pela definição dos módulos de hardware. Visto que a solução apresentou-se bem definida, esta etapa não apresentou grandes dificuldades. Uma das grandes dificuldades nesta etapa foi definir como integrar no hardware um display proveniente de celular. Esta dúvida foi sanada com a compra do módulo de display utilizado. Entretanto, a mecânica deste módulo, de péssima qualidade, proporcionou diversos problemas de conexão com o display, o que acarretou em problemas de produtividade.

Após a definição do hardware foi dado início a busca por uma mecânica que pudesse atender às necessidades do projeto. Neste ponto, optou-se por adaptar uma mecânica, proveniente de outro produto, as necessidades do projeto.

Deve-se ressaltar que a mudança do escopo inicial que era de utilizar um sensor capacitivo para um sensor óptico acarretou em diversas dificuldades de adaptação. Uma das dificuldades

criadas com essa mudança foi com relação ao comprimento do cabo flat flex utilizado no sensor biométrico. Este não possui um comprimento adequado para a nova posição do sensor. Como consequência disso o cabo sofreu o rompimento de trilhas. A figura 35 apresenta o resultado da montagem do protótipo funcional do controle de acesso.

FIGURA 35 - Protótipo montado do controle de acesso biométrico.

É importante destacar que ficou nítido nesta etapa que um projeto mecânico direcionado as funcionalidades do produto de estudo é importante para garantir o bom funcionamento dos módulos.

Outro importante ponto prejudicado, por não se ter dado o devido valor durante a análise de requisitos foi à definição da saída dos cabos de instalação. A mecânica utilizada prevê a saída na parte traseira, entretanto, este não era um requisito não funcional do produto, desta forma, não foi previsto no PCB a passagem dos cabos.

Por fim, foi desenvolvido o firmware do equipamento. Foram utilizadas técnicas de engenharia de software nesta atividade também com o propósito de aumentar a qualidade do firmware. É notória a maior facilidade na correção de erros, já

que quando definido o problema basta concentrar os esforços de análise no módulo envolvido, já que o código é subdividido em módulos funcionais.

4.1 TESTES DE VALIDAÇÃO

Os testes de validação são sequencias de testes funcionais dos quais avaliam o comportamento externo dos módulos. Dados de entrada são fornecidos ao módulo em teste e seus resultados obtidos são verificados se analisados se dentro do esperado.

4.1.1 TESTE DA FONTE

Durante os testes com o módulo biométrico, o mesmo, apresentou oscilação em seu funcionamento. Após um período de funcionamento, com sensor ligado decorrente de solicitação de leitura biométrica, este desligava não retornando ao funcionar. Após estudo do caso foi constatado que a tensão de 12V aplicada a entrada do regulador de tensão do módulo biométrico somado ao consumo do módulo proporcionou o sobre aquecimento deste componente. Este aquecimento fez com que a proteção térmica do regulador atuasse resultando no corte na corrente de carga e consequentemente no desligamento do módulo. Para solucionar este problema foi reduzida a tensão de entrada dos reguladores de 3,3 V para 5V ao invés de 12V.

4.1.2 TESTE DO MÓDULO BIOMÉTRICO

Este procedimento teve como propósito averiguar a comunicação entre o módulo biométrico e a CPU do equipamento. De forma simplificada, o firmware utilizado durante este procedimento possui o fluxo apresentado abaixo, figura 36.

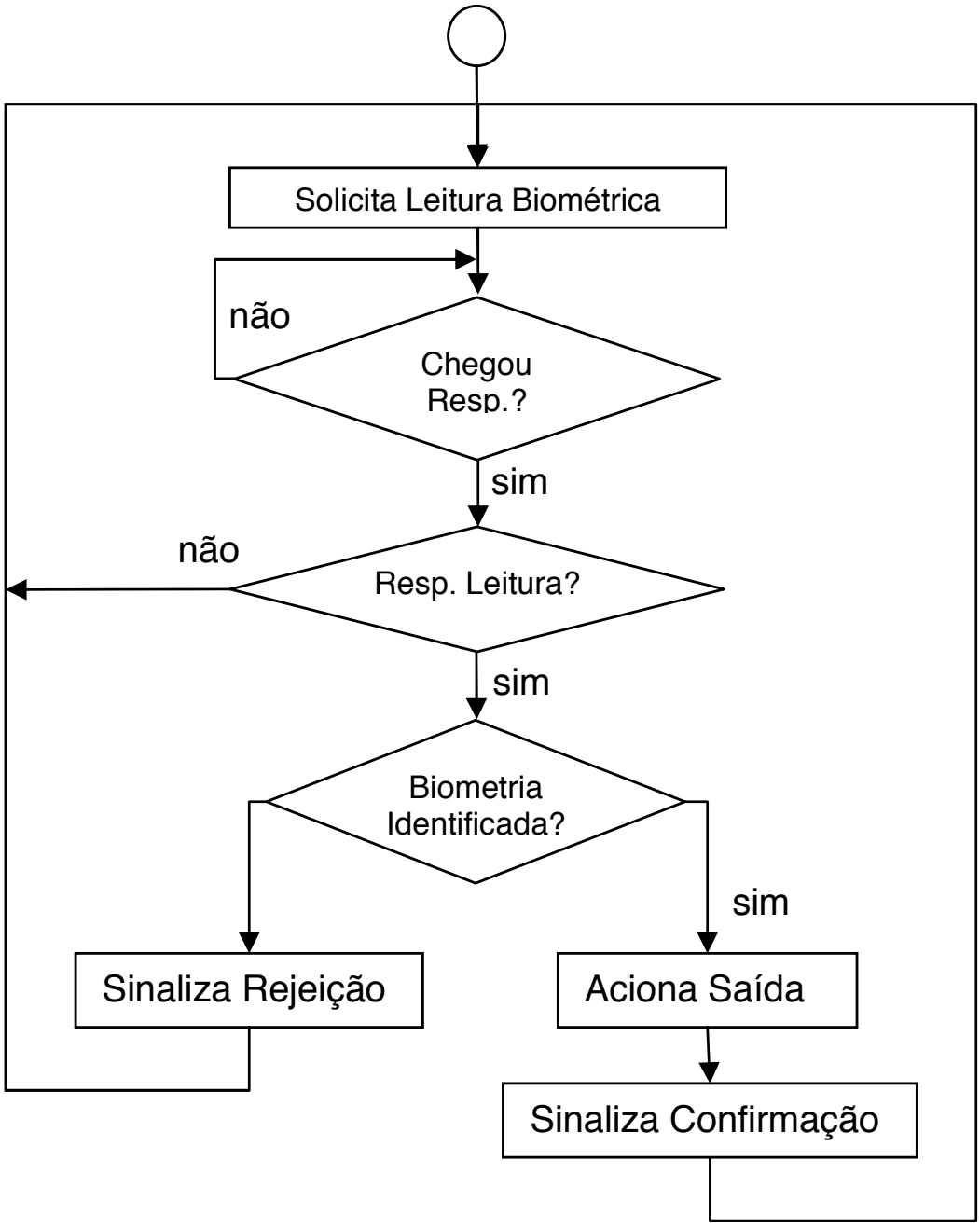


FIGURA 36 - Fluxo simplificado do teste de comunicação com o módulo biométrico.

Neste procedimento, o sinal de rejeição foi configurado com tempo ligado e desligado, ambos com 500 milissegundos e

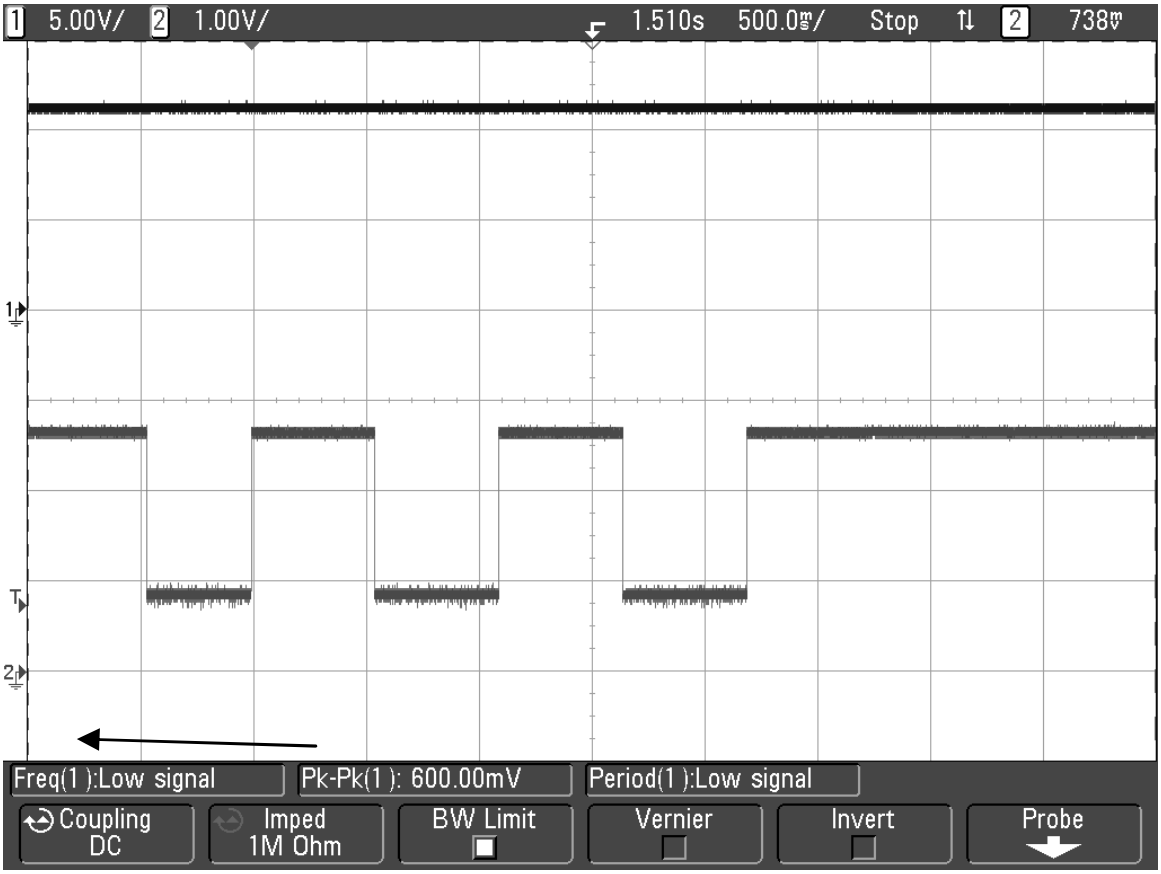


FIGURA 37 - Sinal de rejeição de biometria.

A figura 37 mostra o sinal captura no decorrer do teste. Durante a leitura de uma biometria, foi inserida uma digital que não possuía amostra cadastrada no módulo biométrico. Como esperado, o módulo respondeu que a digital não se apresentava cadastrada e consequentemente a CPU emitiu a sinalização de rejeição através do led de rejeição, sinal apresentado no canal 2.

4.1.3 TESTE DE ACIONAMENTO POR CONTATO SECO

Este procedimento visou avaliar o funcionamento do circuito de acionamento por contato seco presente na placa principal do projeto.

Em um primeiro momento, o teste foi realizado com as seguintes condições: Saída de acionamento configurada em modo contínuo e período de acionamento de três segundos. O

início do ciclo de acionamento foi associado à identificação de um usuário válido.

A imagem da figura 38 representa as formas de ondas capturadas com um osciloscópio do decorrer do teste. O canal um representa o sinal de acionamento gerado pelo uC e aplicado ao circuito de acionamento, já o sinal presente no canal dois corresponde ao acionamento do led de confirmação de identificação.

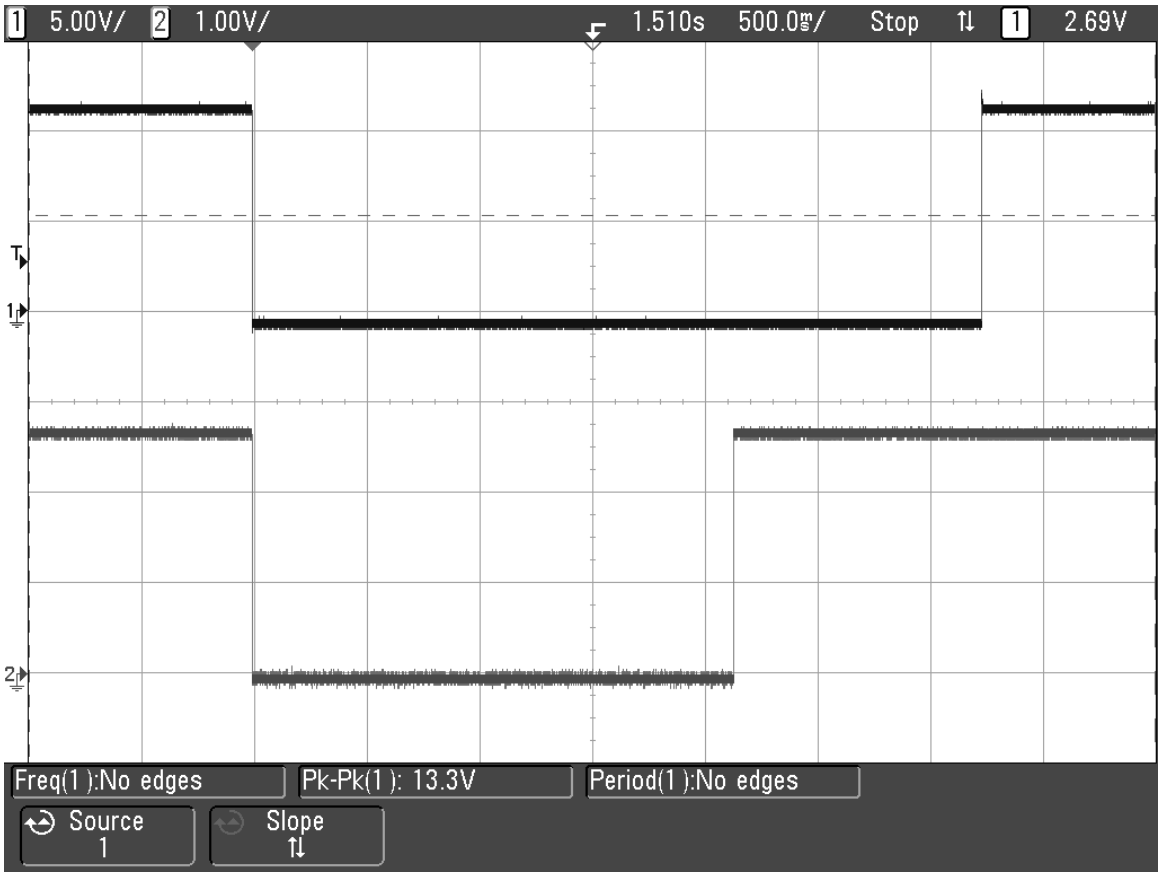


FIGURA 38 - Sinal do acionamento por relé modo contínuo.

Pode-se observar que no mesmo instante que ocorre a sinalização de confirmação da identificação do usuário, nível baixo no canal 2, é iniciado o acionamento da saída à relé, nível baixo no canal 1. De acordo com a configuração o acionamento deveria permanecer por três segundo, entretanto, ocorreu um erro de 200 ms para desacionar. Como este acionamento foi idealizado para fechos elétricos o erro apresentado não se apresenta como um problema.

Em um segundo momento, o teste de acionamento foi realizado no modo pulsado. Neste modo foi definido um período

de um segundo com ciclo ativo de 500 ms para o modo pulsado. Foi definido, como no teste anterior, um acionamento de 3 segundos. O canal 1, da figura 39, representa o sinal de acionamento e o canal 2 o sinal da confirmação de identificação da biometria.

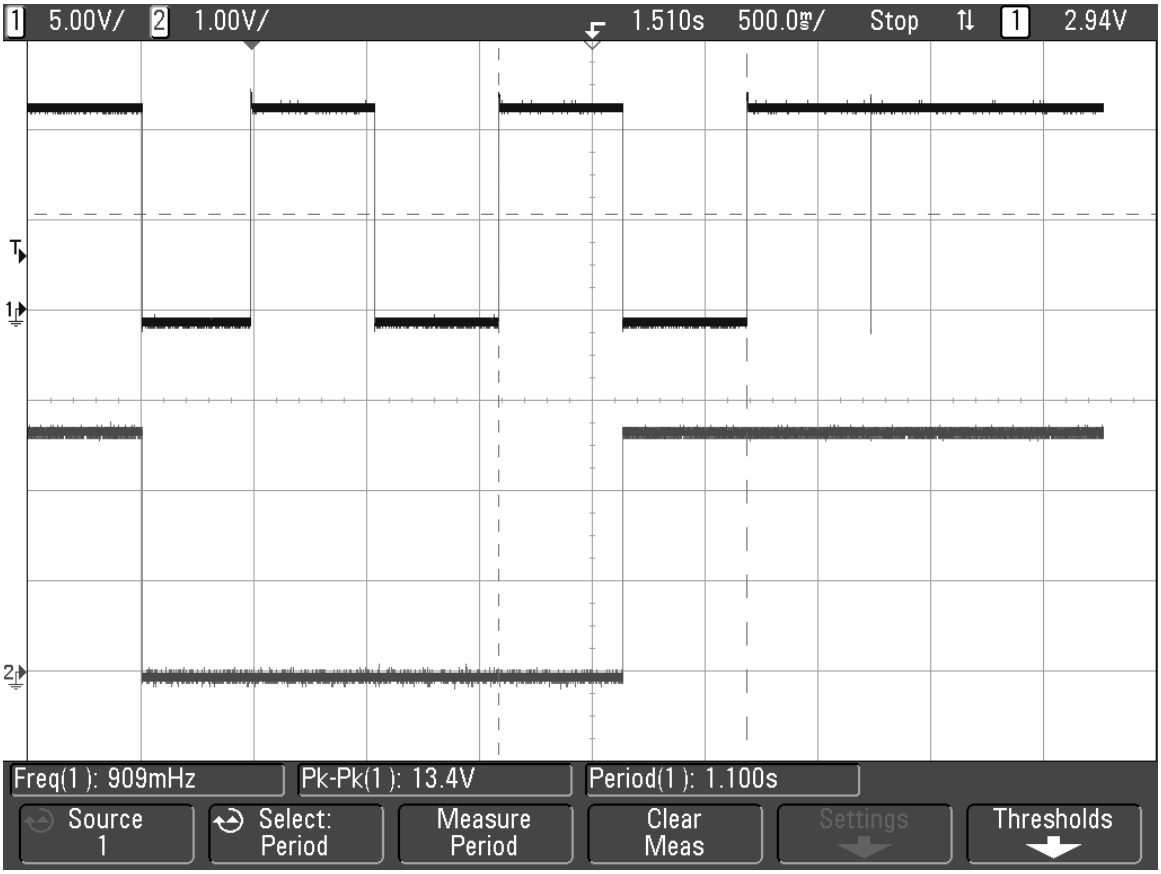


FIGURA 39 - Sinal do acionamento em modo pulsado.

Nota-se novamente que o inicio do acionamento coincide com a confirmação da identificação biométrica. Também se observa na medição do período de acionamento, marcado com as linhas tracejadas, que há um erro de 100 ms em relação ao que foi configurado. Contudo, como mencionado anteriormente, como se trata de acionamento de fecho elétrico o erro observado não se apresenta como um problema.

4.1.4 TESTE DE ACIONAMENTO POR RF

Este teste permitiu validar o funcionamento do circuito de acionamento por RF, circuito transmissor, presente na placa principal do projeto.

Para este procedimento foi utilizado um Receptor Adicional para Controle Remoto HDL, este foi utilizado para receber o sinal de abertura de fecho transmitido pelo controle de acesso.

O programa de controle utilizado foi o mesmo presente no procedimento de teste do módulo biométrico, figura 36, entretanto, a saída de acionamento foi reconfigurada para ser via RF, endereço três. Do lado do módulo receptor, foi configurado o jumper de endereçamento para endereço três de forma a manter a compatibilidade com o sinal transmitido pelo controle de acesso.

Em um primeiro momento foi verificado a transmissão do código pelo circuito transmissor. O código é transmitido mediante a verificação e a respectiva identificação de uma biometria pelo módulo biométrico. O procedimento seguiu os seguintes passos:

1. Pressionado botão de aprendizagem do módulo receptor (Objetiva cadastrar o transmissor);
2. Inserção de uma biometria cadastrada no controle de acesso;
3. Biometria reconhecida: sinal de abertura transmitido;
4. Receptor ao receber transmissão sinaliza cadastro.

A figura 40 mostra o sinal enviado pelo módulo transmissor.

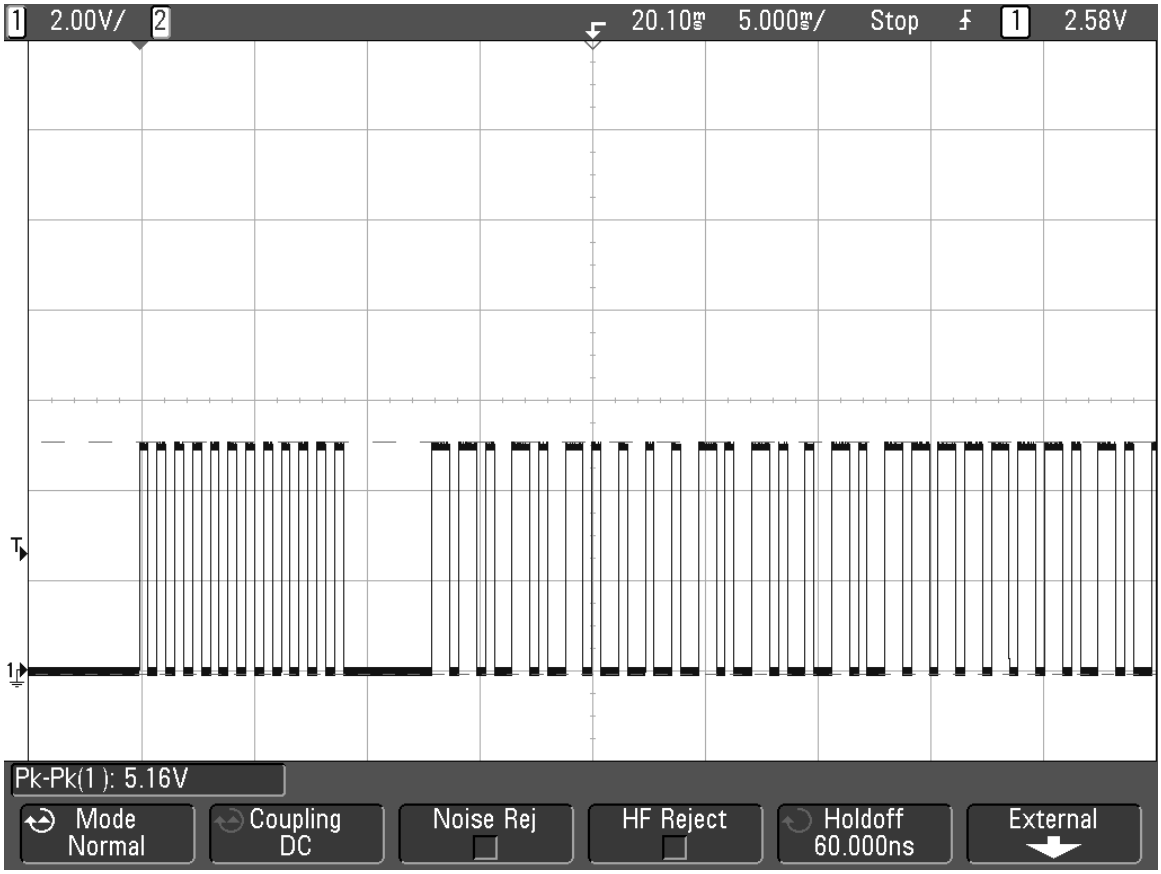


FIGURA 40 - Sinal gerado pelo transmissor de RF.

Através do módulo receptor pode-se constatar que a comunicação foi estabelecida e o mesmo cadastrou o transmissor corretamente.

4.1.5 TESTE DO MÓDULO WI-FI

Este ensaio visou validar o funcionamento do módulo XBee Wi-Fi conectado na placa principal do projeto. Este procedimento se limitou a verificar o funcionamento do módulo no que diz as características e comportamento do hardware O teste seguiu os seguintes passos:

1. Conectar o modo XBee Wi-Fi na placa principal do controle de acesso;
2. Ligar a alimentação da placa principal;

3. Observar o comportamento do led de status do módulo XBee

Com comportamento correto, o módulo XBee Wi-Fi, após alimentado, deve apresentar alguma informação através do led de status do módulo, entretanto, não foi o observado. Após alimentar o dispositivo o mesmo não apresentou nenhum comportamento, ou seja, o led de status do módulo manteve-se desligado.

Já que as ligações do hardware estavam validadas, foi feita uma análise da qualidade da tensão de alimentação fornecida ao módulo XBee Wi-Fi. Nesta análise foi observado que o nível de tensão exigido estava adequado, mas apresentava um ripple de superior a 600 mV como apresentado na figura 41.

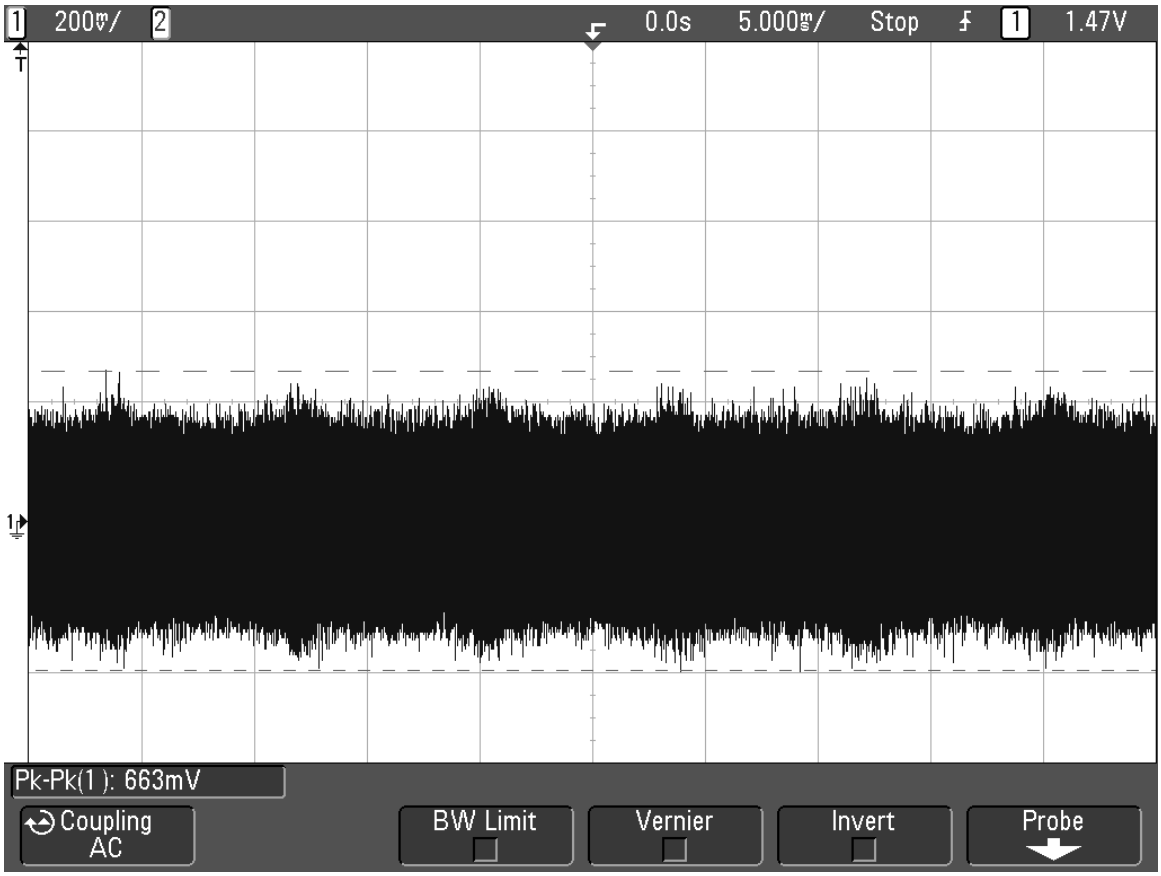


FIGURA 41 - Ripple presente na alimentação do módulo Wi-Fi.

A folha de dados do módulo XBee Wi-Fi especifica que para o funcionamento correto do módulo é necessário um ripple máximo de 50 mV presente na tensão de alimentação.

Considerou-se que nível do ripple encontrado é gerado pelo microcontrolador, foi inserido no circuito, próximos a entrada de alimentação do microcontrolador, dois capacitores em paralelo com os respectivos valores 4,7 uF e 100nF. Com estas alterações pode-se constatar, através da figura 42, que o nível do ripple presente na alimentação do módulo apresentou uma queda considerável para 44 mV. Sendo assim, o ripple presente na alimentação entrou em uma faixa adequada com as características exigidas pelo módulo XBee Wi-Fi.

Após a alteração o teste foi refeito e desta vez o led de status do módulo apresentou-se piscando. Este comportamento indica que o módulo conseguiu iniciar corretamente.

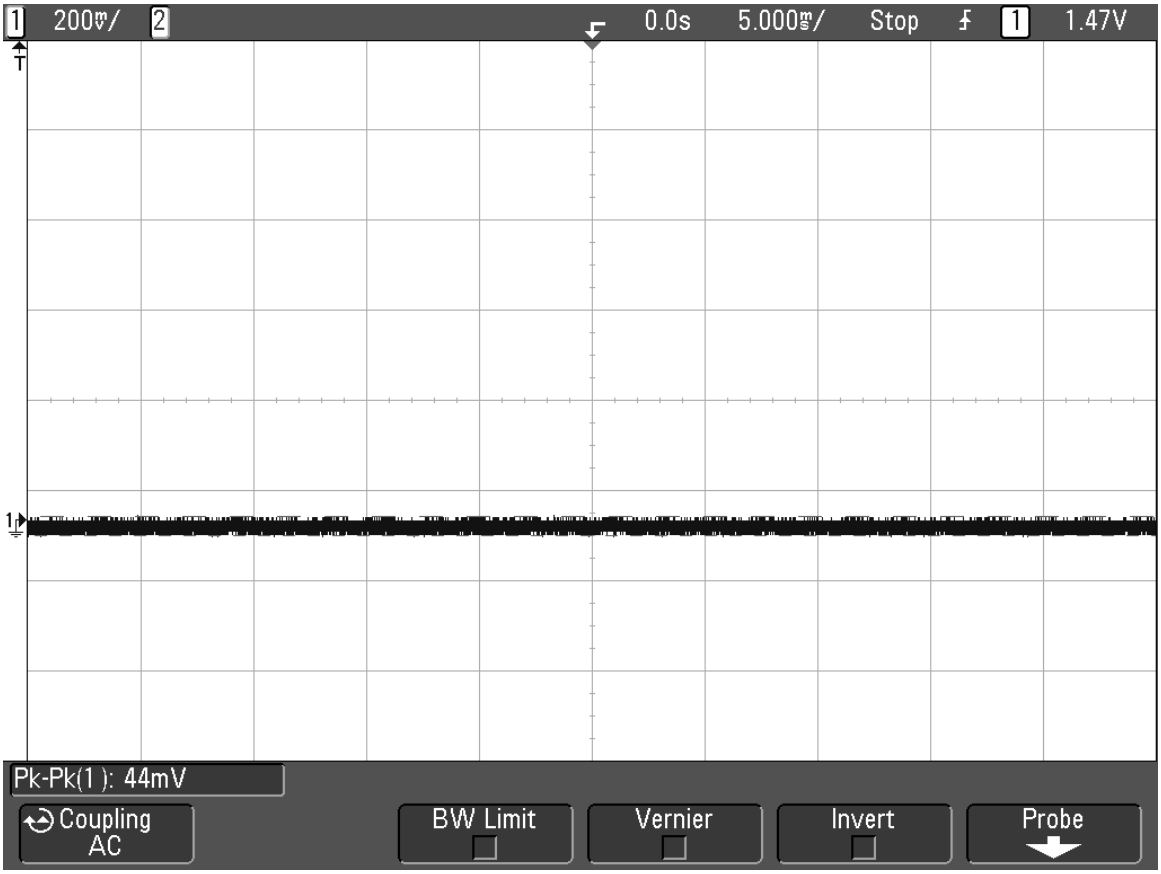


FIGURA 42 - Ripple na alimentação do módulo Wi-Fi filtrado.

5 CONCLUSÃO

Este trabalho não tem como finalidade apresentar uma solução final para controle de acesso biométrico. Pretendeu-se com ele dar início a discussões necessárias sobre a modernização e expansão do portfólio levando em consideração os benefícios que podem ser colhidos através das novas tecnologias.

De acordo com os objetivos descritos inicialmente, o dispositivo final atinge seus desígnios culminando em um controlar de acesso através de identificação por tecnologia biométrica.

Este trabalho permitiu, através da compilação dos resultados obtidos, ampliar a visão da solução onde foi possível identificar pontos para melhoria e implementações futuras.

Propostas de implementações futuras e melhorias:

- Substitui da EEprom e armazenamento de configuração na FLASH;
- Inclusão de um módulo de hardware para leitura de sensores de porta;
- Implementação de um módulo de respostas por voz;
- Inclusão de um leitor de catões RFID modular;
- Software para gerenciamento de informações;
- Opera em modo On-line;
- Utilização de um RTOS;
- Substituição do microcontrolador atual por um com ethernet nativa, objetivando reduzir custos;
- Melhorias no layout.

O material deste trabalho pode vir a ser utilizado pelo autor na implementação de um projeto de um controle de acesso mais

avançado tecnologicamente para a empresa HDL da Amazônia Indústria Eletrônica Ltda. visando tornar este, um produto comercial diferenciado no mercado.

6 REFERÊNCIAS BIBLIOGRÁFICAS

FERREIRA, ABIBE. PROPOSTA DE IMPLEMENTAÇÃO DE SISTEMA DE SEGURANÇA UTILIZANDO SISTEMAS BIOMÉTRICOS. 2001. 43. ENGENHARIA. UNIVERSIDADE DA AMAZÔNIA, CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS, BELÉM.

CBA. Disponível em: <http://www.consultoresbiometricos.com.br/05_Obio_aplicacoes.php>. Acessado em 6 de dezembro de 2012.

CODE::BLOCKS. Disponível em: www.codeblocks.org. Acesso em: 10 de setembro de 2012.

DALTRO, Alexandre Brandão Veras. **Biometria.** Reconhecimento de Retina. Disponível em: http://www.gta.ufrj.br/grad/10_1/retina/introducao.html. Acesso em 12 junho. 2012.

JAIN, Anil K. Biometric Authentication based on Keystroke Dynamics. Disponível em: http://www.cse.msu.edu/~cse891/Sect601/KeystrokeRcg.pdf. Acesso em 18 de junho. 2012.

PINTO, Evandro M. Regra de Negócio Não é Requisito de Software. Disponível em: http://wm2info.com.br/blog/2012/01/17/regra-de-negocio-nao-e-requisito-de-software/. Acesso em 10 de dezembro. 2012.

Wikipédia: Papiloscopia. Disponível em: http://pt.wikipedia.org/wiki/Papiloscopia
Acesso em 10 de novembro 2012.

Wikipédia: Papiloscopia. História da identificação e seus personagens. Disponível em http://www.papiloscopia.com.br/historia.html. Acessado em 10 de novembro. 2012.

MICROCHIP: HCS201. Disponível em:< http://ww1.microchip.com/downloads/en/devicedoc/41098c.pdf>. Acesso em: 28 de outubro de 2012.

MICROCHIP: 24AA256. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/21203R.pdf >. Acesso em: 05 de dezembro. 2012.

HDL: Módulo de Acesso com Teclado com Rádio Receptor HRC (sem fio). Disponível em: <http://www.hdl.com.br/produtos/controle-de-acesso/modulos-de-controle-de-acesso/modulo-de-acesso-com-teclado-com-radio>. Acesso em: 11 de outubro. 2012.

HDL: Receptor Adicional para Controle Remoto. Disponível em: < http://www.hdl.com.br/produtos/controle-de-acesso/acessorios/receptor-adicional-para-controle-remoto>. Acesso em 28 de outubro de 2012.

NXP: PCD8544. Disponível em: < http://www.classic.nxp.com/acrobat_download2/datasheets/PCD8544_1.pdf>. Acesso em: 30 de outubro de 2012.

DATASHEETCATALOG: MC34119. Disponível em: < http://www.datasheetcatalog.org/datasheet/motorola/MC34119.pdf>. Acesso em: 30 de outubro de 2012.

INDIA: XBee Wi-fi. Disponível em:< http://www.indiasemiconductorforum.com/showthread.php/2113-Digi-XBee%C2%AE-Wi-Fi-Embedded-module-for-OEMs>. Acesso em: 29 de novembro de 2012.

Digi: XBee Wi-Fi RF Module: Disponível em: < ftp://ftp1.digi.com/support/documentation/90002124_B.pdf> Acessado em: 29 de novembro de 2012.

BIOMETRUS: Passface 1020. Disponível em: < http://www.biometrus.com.br/site/index.php?option=com_content&view=article&id=116:passface-1020-teste&catid=34:controle-de-acesso-blog&Itemid=67>. Acessado em: 09 de dezembro de 2012.

ARAÚJO, Alexandre. **Iridologia**. O que o olho revela. Disponível em : www.senado.gov.br/senado/portaldoservidor/jornal/jornal74/terapia_alternativa_iridologia.aspx. Acessado em: 09 de dezembro de 2012.

RIBEIRO, Carlos Eduardo Calvente. **Biometria**. Leitores de Impressão Manual. Disponível em: www.gta.ufrj.br/grad/07_2/carlos_eduardo/Produtos.html. Acessado em 10 de dezembro de 2012.

DUARTE, Otto Carlos Muniz Bandeira. **Biometria.** Reconhecimento de Retina. Disponível em: www.gta.ufrj.br/grad/10_1/retina/index.html. Acessado em 9 de dezembro de 2012.