

Faculdade de Tecnologia do Estado de São Paulo
FATEC-SP

DANILO LANGELLOTTI
GUSTAVO ROBERTO DE SOUSA ROSA
RAFAEL SILVA BEGA

SISTEMA DE AUTENTICAÇÃO VEICULAR POR RFID

SÃO PAULO

2016

Danilo Langellotti;
Gustavo Roberto de Sousa Rosa; e
Rafael Silva Bega.

SISTEMA DE AUTENTICAÇÃO VEICULAR POR RFID

Trabalho de conclusão de curso
apresentado a Faculdade de
Tecnologia do Estado de São Paulo
/ FATEC-SP para obtenção do título
de tecnólogo em Eletrônica
Industrial.

Orientador: Professor Me. Ricardo
Cardoso Rangel

SÃO PAULO

2016

DANILO LANGELLOTTI
GUSTAVO ROBERTO ROSA
RAFAEL SILVA BEGA

SISTEMA DE AUTENTICAÇÃO VEICULAR POR RFID

APROVADO EM ___/___/___

BANCA EXAMINADORA

Ricardo Cardoso Rangel (Orientador)

Mestre

Faculdade de Tecnologia do Estado de São Paulo

Roberto Katsuhiko Yamamoto

Doutor

Faculdade de Tecnologia do Estado de São Paulo

Aparecido Nicollet

Doutor

Faculdade de Tecnologia do Estado de São Paulo

DEDICATÓRIA

A esta Faculdade de Tecnologia do Estado de São Paulo – FATEC-SP, seu corpo docente, direção e administração.

LISTA DE ILUSTRAÇÕES

Figura 1 - Pinagem do PIC16F877A (encapsulamento <i>DIP</i>).....	11
Figura 2 - Aspecto ID-20LA	13
Figura 3 - Pinagem ID-20LA	13
Figura 4 - TAG RFID.....	15
Figura 5 - Relé Eletromecânico.....	16
Figura 6 - Cristal Oscilador	17
Figura 7 - Buzzer	17
Figura 8 - Capacitor Eletrolítico.....	18
Figura 9 - Capacitor Cerâmico	18
Figura 10 - Banco de <i>LEDs</i>	20
Figura 11 - Acionamento do LED verde (módulo ligado)	21
Figura 12 - <i>LED</i> azul, indica que o cartão mestre foi apresentado.....	21
Figura 13 - <i>LED</i> amarelo, indica que o cartão apresentado esta sendo gravado.....	21
Figura 14 - <i>LED</i> verde, indica sucesso na gravação	21
Figura 15 - Sistema volta ao estado inicial	21
Figura 16 - <i>LED</i> vermelho, indica que o cartão apresentado não esta cadastrado.....	22
Figura 17 - <i>LED</i> verde, indica que o cartão apresentado esta cadastrado.....	22
Figura 18 - <i>LED</i> azul, necessário que este seja ativado 5 vezes	23
Figura 19 - Acionamento de todos os <i>LEDs</i>	23
Figura 20 - Dados transmitidos pelo TAG.....	25
Figura 21 - Conversão DEC -> HEX.....	26
Figura 22 - Chaveiro estudado	26
Figura 23 - Utilização do hyperterminal do software Proteus 8	26
Figura 24 - Tabela ASCII.....	27
Figura 25 - Fluxograma rotina VOID MAIN.....	37
Figura 26 - Fluxograma VOID INTERRUPT	38
Figura 27 - Circuito simulado via Proteus 8.....	40
Figura 28 - Circuito simulado via Proteus 8.....	40
Figura 29 - Inicio da montagem na placa universal.....	41
Figura 30 - Fios soldados realizando a função das trilhas	42
Figura 31 - Aspecto final do circuito 100% montado/soldado	43
Figura 32 - Montagem do ID-20LA	43
Figura 33 - Aspecto final do módulo	44
Figura 34 - Módulo de chaveamento dos circuitos de potência.....	45
Figura 35 - Chave de ignição montada e etiquetada	45
Figura 36 - Posições da chave de ignição	46
Figura 37 - Circuito da chave de ignição.....	47
Figura 38 - Circuito de potência atuante na bomba de combustível.....	48
Figura 39 - Circuito de potência para ativação do painel.....	49

SUMÁRIO

1	RESUMO	6
2	ABSTRACT.....	7
3	INTRODUÇÃO.....	8
3.1	METODOLOGIA E FUNDAMENTAÇÃO TEÓRICA	10
3.1.1	<i>O que é o RFID.....</i>	10
3.2	Material Utilizado	11
3.2.1	<i>Microcontrolador.....</i>	11
3.2.2	<i>Leitor de RFID</i>	12
3.2.3	<i>Etiqueta RFID</i>	14
3.2.4	<i>Relês.....</i>	16
3.2.5	<i>Cristal.....</i>	17
3.2.6	<i>Buzzer.....</i>	17
3.2.7	<i>Capacitores.....</i>	18
3.2.8	<i>Resistores.....</i>	18
4	DESENVOLVIMENTO	19
4.1	Funcionamento	19
4.1.1	<i>Entendimento do módulo de segurança</i>	20
4.1.2	<i>Cadastramento de novo chaveiro</i>	21
4.1.3	<i>Autenticação.....</i>	22
4.1.4	<i>Exclusão de chaveiros já cadastrados.....</i>	23
4.1.5	<i>Bloqueio do veículo</i>	24
4.2	Integração dos Principais Dispositivos.....	25
4.3	Código-fonte	28
4.4	Fluxograma.....	36
4.3	Simulador.....	39
4.4	Montagem.....	41
4.5	Circuitos Auxiliares	44
4.5.1	<i>Simulador da chave de ignição do automóvel</i>	46
4.5.2	<i>Circuito de chaveamento da bomba de combustível</i>	48
4.5.3	<i>Circuito de chaveamento para ligação do painel e indicação de falha</i>	49
5	O PRODUTO NO MERCADO	50
5.1	O produto é destinado a quem?	50
5.2	Quais vantagens oferece?	50
5.3	Já existe produto semelhante?	50
6	CONCLUSÃO	52
7	BIBLIOGRAFIA.....	53

1 RESUMO

Este projeto tem como objetivo desenvolver um sistema de segurança para minimizar a quantidade de carros roubados e/ou furtados.

Atualmente existem dois tipos de sistemas de segurança veiculares já tradicionais:

Os puramente mecânicos, como travas carneiro e travas de câmbio, os quais podem ser facilmente violados, uma vez que basta destruí-los fisicamente para que se tenha acesso ao veículo; e

Os sistemas eletrônicos, como alarmes com transmissão por meio de radiofrequência (RF) a distancia, que podem ser clonados ou inibidos de atuar devido à utilização de aparelhos desenvolvidos com este propósito.

O sistema desenvolvido utiliza tecnologia de identificação por radiofrequência (*RFID*) para validar a permissão necessária para se conduzir o veículo.

Ele inibe qualquer tentativa de ligação do motor do automóvel sem que haja a confirmação de permissão por meio de uma *TAG* (etiqueta de transmissão de dados) predefinida.

Para tanto, ele atua diretamente na bomba de combustível do veículo, mantendo-a desligada até que a permissão seja concedida a partir da *TAG*.

Devido ao método de funcionamento, o dispositivo desenvolvido pode ser utilizado em paralelo aos sistemas de segurança tradicionais, sem que haja interferência de atuação entre eles.

2 ABSTRACT

The aim of this paper is to present a security system to reduce /minimize the amount of stolen cars.

Currently, there are two traditional types of vehicle security systems:

The purely mechanical immobilizer devices such as steering wheel-lock or gearshift lock, these methods can be circumvented easily, since just physically destroy them to gain access to the vehicle; and

Electronic systems such as alarms with RF transmission, which can be cloned or inhibited by devices developed for this purpose.

The developed system uses Radio-frequency identification (RFID) to validate the permission required to drive the vehicle.

It inhibits any attempt to start engine of vehicle without confirmation of permission by a presseted tag (label transmission data).

Therefore, it acts directly on the fuel pump of the vehicle keeping it off until the permission is granted from the TAG.

Due to the operation method, the developed device may be used in parallel with traditional security systems without interference acting between them.

3 INTRODUÇÃO

No Brasil, a quantidade de carros roubados e/ou furtados aumentou em 2015, em relação aos anos anteriores. Segundo dados da Confederação Nacional de Seguros foram roubados ou furtados, em média, 57 carros por hora no Brasil no ano de 2015.

Atualmente já existem diversos tipos de sistemas de segurança no mercado, sejam eles eletrônicos ou unicamente mecânicos. Porém, tais sistemas apresentam limitações na segurança oferecida. Os sistemas eletrônicos somente disparam sinal sonoro indicando a tentativa de adentrar o veículo e os puramente mecânicos são facilmente violáveis fisicamente, com utilização de ferramentas adequadas.

O Sistema de Autenticação Veicular proposto atua diretamente no sistema de ignição do veículo, inibindo o funcionamento do motor quando na tentativa de ser colocado em funcionamento por condutor não autorizado. Devido ao método de atuação, o módulo de segurança pode ser utilizado em paralelo aos sistemas já existentes e/ou já implantados no veículo.

Para a verificação de permissão (ou não) para o funcionamento do veículo, o módulo de segurança utiliza a tecnologia *RFID* para realizar a comunicação com etiquetas (comumente chamadas de *TAGs*) previamente cadastradas na memória interna do próprio módulo.

As *TAGs* são dispositivos que possuem dados únicos, e que quando expostas às condições ideais, transmitem tais dados para o meio externo (através de *radiofrequência*), podendo assim realizar a comunicação com o módulo de segurança sem necessidade de contato físico. Elas portam dados únicos em âmbito mundial, impossibilitando que um usuário indesejado coloque o automóvel em funcionamento.

Quando uma *TAG* previamente cadastrada se comunica com o módulo de segurança, este permite a ligação da bomba de combustível do veículo, até então desligada. Assim o automóvel está pronto para utilização.

Quando da tentativa de partida do veículo sem prévia autorização, o motor não entra em funcionamento (devido à falta de combustível) e um indicador de erro é gerado no painel do veículo.

O módulo permite o cadastro prévio de até 23 *TAGs*, para que cada uma delas possa colocar o automóvel em funcionamento, independente das outras.

O módulo inicialmente não possui nenhuma *TAG* cadastrada, e a inserção de uma nova *TAG* no banco de dados fica por conta do proprietário e/ou condutor do veículo. Para tanto se faz necessária a utilização de uma *masterTAG* (única para cada módulo) que possibilita a gravação de novas *TAGs* ou exclusão das *TAGs* já gravadas no banco de dados.

3.1 METODOLOGIA E FUNDAMENTAÇÃO TEÓRICA

3.1.1 O que é o RFID

Identificação por radiofrequência (ou *RFID* na sigla em inglês) é uma tecnologia que utiliza frequência de rádio para captura de dados. Existem diversos métodos de identificação, sendo que o mais comum é o armazenamento de um número de série em um objeto (cartão, chaveiro, entre outros) de maneira que o identifique perante outros semelhantes.

O RFID é uma tecnologia existente desde a segunda guerra mundial, porém somente agora está se popularizando e a cada dia mais empresas estão considerando utilizar a identificação por radiofrequência para melhorar seu desempenho. A necessidade de acelerar os processos e automatizar tarefas são outros fatores que motivam a utilização de RFID (JUNIOR, Joel Andrade, 2007).

A comunicação ocorre por ondas de rádio que carregam a informação que portam os dados uni ou bidirecionalmente, o que depende da tecnologia utilizada. Quando uma *TAG* entra na zona de leitura, esta captura sua identidade que é passada ao dispositivo de interesse para ação. Fisicamente, o leitor transmite ondas eletromagnéticas excitando a bobina da *TAG*, com esta excitação uma corrente é induzida no transmissor fazendo com que a comunicação RF aconteça.

Embora ambos estejam dentro do escopo do nome *RFID*, sistemas ativos e passivos são, fundamentalmente, tecnologias diferentes. Enquanto os dois empregam ondas eletromagnéticas para implementar a comunicação entre a etiqueta e o leitor, o método de energização do *TAG* difere. Os *TAGs* ativos utilizam uma fonte interna de energia (bateria) para alimentar continuamente seu circuito radiotransmissor, em contraste com os passivos que contam com a energia da onda eletromagnética incidente para funcionar (PAIS, Júlia Sakamoto, 2009).

Neste trabalho a opção escolhida de *TAG* foi do tipo passiva, pois este tipo de etiqueta possui baixo custo e seu escopo de funcionamento atende integralmente a necessidade proposta, uma vez que este projeto não necessita de uma *TAG* com funcionalidades como memória, temporizadores ou altas distâncias de comunicação.

3.2 Material Utilizado

3.2.1 Microcontrolador

Foi selecionado para uso neste projeto o microcontrolador *PIC 16F877A*, devido principalmente à fácil compreensão e acessibilidade ao componente.

As principais características do dispositivo são conversor analógico/digital (*A/D*) de dez bits e oito canais, memória *FLASH* de 8k linhas com 14 espaços de memória cada, memória *RAM* de 368 bytes, memória *E²PROM* de 256 bytes, 33 portas de *I/O*, dois canais com Modulação por Largura de Pulso (*PWM*), conexão *USART*, três temporizadores/contadores sendo dois (*Timer0* e *Timer2*) de oito bits e um (*Timer1*) de 16 bits e 15 interrupções.

Possui também tecnologia *CMOS* (*Complementary Metal Oxide Semiconductor*) proporcionando baixa potência consumida pelas memórias *Flash* e *E²PROM*, faixa de tensão de operação de (2.0V a 5.5V) e baixo consumo de potência.

Na figura abaixo é apresentada a pinagem do PIC 16F877A:

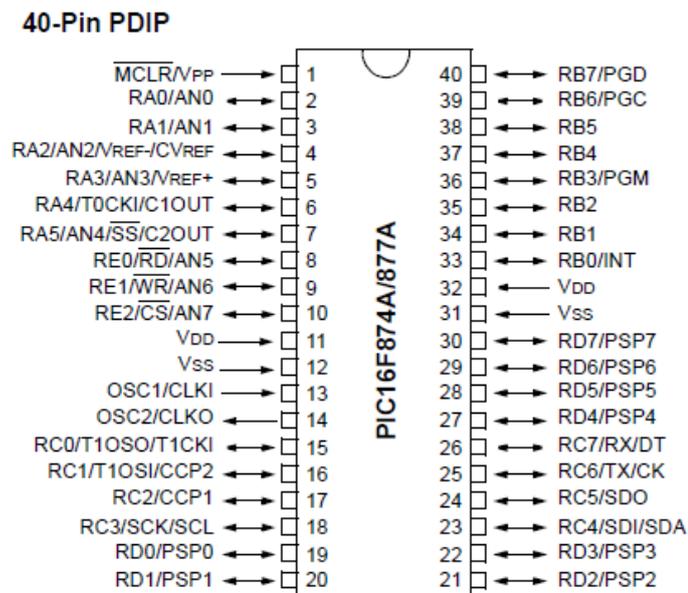


Figura 1 - Pinagem do PIC16F877A (encapsulamento *DIP*)

3.2.2 Leitor de RFID

O leitor escolhido foi o modelo *ID-20LA*, trata-se da camada intermediária do protótipo, tendo a função de intermediar entre as *TAGs* portadoras dos dados a serem tratados e o microcontrolador no qual tratará estes dados.

Para realizar a leitura, o dispositivo possui uma antena geradora de sinal de radiofrequência. Este sinal excita a antena da *TAG* e gera uma corrente elétrica por ela, alimentando o *microship* interno e fazendo com que este transmita os dados de identificação, esta transmissão também é realizada pela antena da *TAG* para o leitor.

O sucesso na leitura dos dados das *TAGs* depende de alguns fatores, como a posição da *TAG* em relação ao leitor (distância, ângulo de inclinação, entre outros), a degradação do sinal provocada pelo meio, compatibilidade entre *TAG* e leitor (frequência de trabalho) e interferências eletromagnéticas.

Uma onda eletromagnética consiste em um enlace de oscilações elétricas e magnéticas que formam um ângulo de 90° entre si. Essas oscilações ocorrem em direções determinadas pela antena geradora (oriunda do leitor). Quanto mais alinhada a *TAG* estiver com a direção de oscilação do campo elétrico, maior será a corrente induzida em seu circuito fazendo assim que haja uma maior eficiência na leitura da informação.

O meio influencia na qualidade de comunicação do sinal. Dependendo do modelo e frequência de operação da etiqueta ela pode tornar-se completamente inoperante quando próxima de uma superfície metálica (DOBKIN, Daniel M., WANDINGER, Titus, 2005, p. 32-42).

Como ainda não é adotado um padrão de comunicação, cada classe de *TAG* opera de uma forma, há diferenças nos protocolos de comunicação, na codificação, na modulação e no modo de operação, isso considerando apenas uma mesma banda de operação.

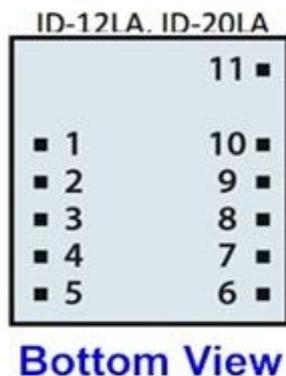
Quando mais de uma onda se propaga através do mesmo meio ocorre interferência entre elas, efeito que é especialmente grave quando estão todas na mesma frequência. Ao fazer a leitura simultânea de várias etiquetas semelhantes, suas transmissões se embaralham no meio, impedindo que qualquer uma seja compreendida, caracterizando colisão de dados. Como o raio de leitura de uma *TAG*

é limitado, pode-se fazer uma separação espacial da etiqueta lida, mas isso nem sempre é possível. É necessário, então, que seja implementado um protocolo anti-colisão, que faça com que elas transmitam cada uma ao seu tempo.

Algumas das características do modelo utilizado: Possui antena interna (geradora), espaçamento entre pinos de 2mm, alimentação de 2,8 à 5 V, frequência de leitura 125kHz, protocolo de comunicação serial *RS232*, velocidade de comunicação serial de 9600bps (bits por segundo), protocolos de informação dos dados de saída podem ser *ASCII*, *Wiegand26* e *Magnetic ABA Track2*, tais protocolos são selecionados através do pino 7 (DATASHEET, ID-20LA, ID-Innovations).



Figura 2 - Aspecto ID-20LA



- | |
|--|
| <ol style="list-style-type: none"> 1. GND; 2. RESET; 3. NC; 4. NC; 5. CP; 6. TAG em leitura; 7. Seleção do formato; 8. Pino de dados 1; 9. Pino de dados 0; 10. Leitura (LED/Buzina) 11. +2.8V até +5V; |
|--|



Figura 3 - Pinagem ID-20LA

3.2.3 Etiqueta RFID

Como tudo pode sugerir, o elemento principal na tecnologia tratada é o próprio *TAG*, o que o torna alvo preferencial das pesquisas e desenvolvimento. Os principais objetivos envolvem questões comerciais, onde se busca atender aos critérios da indústria: preço, compatibilidade, confiabilidade e eficiência.

Entre os atributos principais de uma etiqueta, pode-se nomear: a forma de alimentação, as características da memória e a frequência de operação.

Os mais sofisticados costumam ter *C/s* que gerenciam as principais funções no dispositivo. Nesse caso, são responsáveis por armazenar a memória, conter o circuito oscilatório, implementar propriedades anti-colisão e oferecer funções de alto nível (registro de eventos, data e hora).

Enquanto são privadas de oferecer tais recursos, as *TAGs* sem chip são consideravelmente mais baratas. Sua operação é mais simples e se baseia na simples reflexão da onda incidente, isto é, na manipulação das propriedades físicas do material para criar um padrão de resposta único.

Entre as etiquetas ativas e passivas, a principal diferença é quanto à presença de bateria para alimentar a emissão da onda de resposta. Cabe frisar que as passivas não estão limitadas a modelos sem *CI*, mas não podem oferecer suporte a funções que requeiram energização contínua, como marcação de tempo. Algumas apresentam bateria, mas que se destina a aplicações auxiliares, como mostradores de cristal líquido. Entre as ativas, faz-se distinção entre as que emitem um sinal a intervalos pré-determinados e as que apenas respondem a interrogações de leitores.

No quesito memória encontra-se grande diversidade de tamanhos, tipos e implementações. Há as que permitem somente leitura, vindo programadas de fábrica com um código único, atribuído aleatoriamente. Estas são predominantemente passivas e sem chip, estão entre as mais baratas e são largamente utilizadas na etiquetagem. Outras permitem que se escreva uma vez, fazendo com que, em uma linha de produção, lhes seja atribuído um número no qual não poderá mais ser apagado. As que implementam total possibilidade de leitura e escrita têm originado aplicações interessantes: dada a capacidade de atualizar as informações sempre que desejado, pode-se armazenar critérios de inspeção, andamento, características físicas e etc.

As faixas de operação se distinguem em termos de características passadas aos TAGs, pelas taxas de transmissão atingidas, pela capacidade de operar próximo a metais e superfícies molhadas, e pelo tamanho do enrolamento necessário em um dispositivo passivo.

Quanto mais baixa a frequência de operação, melhor o desempenho quando próximo de superfícies metálicas, e menor a taxa de transmissão atingida. Por ser uma tecnologia amadurecida, tem a maior base instalada no mercado. Na faixa dos 13,56 MHz encontramos TAGs mais baratos e com raio de leitura de até 1 metro, usados principalmente em cartões “inteligentes”, rastreamento em nível de item por não necessitarem de leituras múltiplas à distância. Entre 868 e 915 MHz encontram-se as etiquetas com potencial para serem as mais baratas em grandes quantidades. Costumam ser utilizadas em cobrança automatizada de pedágio por permitirem leituras até três metros de distância, porém alguns países proíbem ou restringem transmissões nessa banda, por ser reservada. TAGs no campo das microondas permitem um sinal mais direcional e altas taxas de leitura, o que as torna ideais para certas aplicações. Por serem as mais suscetíveis a degradações devidas ao meio, seu raio de leitura é reduzido e está próximo de um metro.

O modelo de TAG utilizado foi o do tipo passiva (Somente Leitura), com frequência de operação de 125 kHz (necessariamente compatível com o leitor *ID-20LA*).

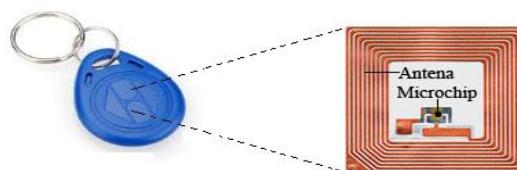


Figura 4 - TAG RFID

3.2.4 Relês

Os relês são dispositivos comutadores eletromecânicos. O que determina a utilização de um relé numa aplicação prática são suas características. O entendimento dessas características é fundamental para a escolha do tipo ideal. A bobina de um relé é enrolada com um fio esmaltado cuja espessura e número de espiras é determinado pelas condições em que se deseja fazer sua energização (SANTOS, Marcelo Diego, 2012). A intensidade do campo magnético produzido e, portanto, a força com que a armadura é atraída depende tanto da intensidade da corrente que circula pela bobina como do número de espiras que contém. O número de contatos e sua disposição vão depender das aplicações a que se destinam os relês. Têm-se então diversas possibilidades:

- Contatos NA ou Normalmente Aberto;
- Contatos NF ou Normalmente Fechado;
- Contatos NA, NF ou Reversíveis;
- Relés aberto, fechados ou selados.

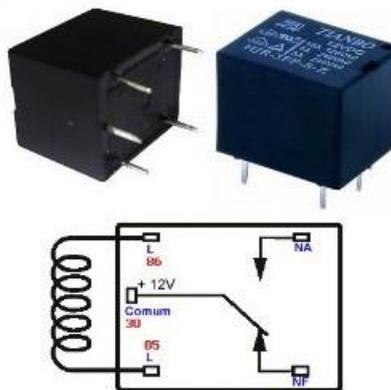


Figura 5 - Relé Eletromecânico

3.2.5 Cristal

Seu funcionamento baseia-se em um efeito físico de contração e relaxamento do cristal de quartzo interno ligado a dois terminais, quando submetido a uma tensão este cristal contrai até certo ponto e logo depois relaxa, esse movimento físico cria uma frequência precisa que é usada como base de tempo do microcontrolador (JONES, Theron, 2012).



Figura 6 - Cristal Oscilador

3.2.6 Buzzer

É um componente eletrônico composto de 2 camadas de metal e uma camada interna de cristal piezoelétrico, ao ser alimentado com uma fonte de sinal vibra com a mesma frequência deste sinal recebido, produzindo um som característico (GUNNAR, Corrêa, 2015)



Figura 7 - Buzzer

3.2.7 Capacitores

Um capacitor é um componente eletrônico que armazena carga elétrica em um campo elétrico, é constituído de duas peças condutoras denominadas armaduras e entre estas armaduras existe um dielétrico, ou seja, um material isolante (SANTOS, Marco Aurélio da Silva, 2012). Os capacitores foram usados em dois circuitos, o *masterclear* do *PIC 16f877A*, e para o circuito oscilador.

Sendo que em cada um dos circuitos acima citados usaram capacitores construídos de formas diferentes, circuito de *masterclear* capacitor Eletrolítico com capacitância de $10\mu\text{F}$ e para o *Crystal* capacitor cerâmico de 22nF .



Figura 8 - Capacitor Eletrolítico



Figura 9 - Capacitor Cerâmico

3.2.8 Resistores

Resistores peliculados de $\frac{1}{4}\text{W}$ com funções diversas, principalmente como limitadores de corrente elétrica para funcionamento dos *LEDs* (220Ω), limitador de corrente elétrica para o Buzina (560Ω), circuito de *MasterClear* responsável por resetar o microcontrolador quando o nível de tensão no pino 1 ficar abaixo de 1.7V ($40\text{K}\Omega$ e $10\text{K}\Omega$).

4 DESENVOLVIMENTO

4.1 Funcionamento

O Sistema está baseado na tecnologia *RFID*. Será utilizado um *TAG RFID* passivo, do tipo *read only* (somente leitura) devido ao menor custo quando comparado a outros tipos e as necessidades básicas do sistema. Cada *TAG* possui o formato de um chaveiro de uso pessoal contendo um código único gravado em seu *chip*, tal código necessita ser gravado previamente no sistema para que possa ser lido pelo mesmo, garantindo segurança. Podem ser cadastrados até 23 chaveiros no sistema, sendo que este número está limitado devido à tecnologia utilizada (capacidade da *E²PROM* do microcontrolador).

O módulo de segurança, ao ser instalado no veículo, atua no sistema de ignição para impedir o funcionamento do automóvel. Cabe ao módulo ler cada chaveiro e verificar se o mesmo permite que o veículo seja colocado em funcionamento.

Como estratégia de segurança, e para que não fique óbvio que o bloqueio do veículo é causado por um sistema de segurança, o módulo também induz uma falsa indicação de falha no painel do automóvel.

O sistema inicialmente não possui nenhum chaveiro cadastrado. O cadastramento é realizado pelo próprio cliente através de um chaveiro-mestre (*MasterTAG*), sem necessidade da utilização de quaisquer botões de comando.

O chaveiro-mestre é utilizado para a gravação de novos cartões e exclusão dos cartões já gravados, conforme necessidade.

Fisicamente o chaveiro-mestre é semelhante aos chaveiros de permissão, com a diferença que o módulo de segurança está configurado para executar outras tarefas quando reconhecer a leitura do chaveiro-mestre.

4.1.1 Entendimento do módulo de segurança

O módulo é totalmente operado a partir do chaveiro-mestre, com ele é possível gravar novos chaveiros ou excluir os chaveiros já gravados na memória do módulo.

Todos os procedimentos são realizados pelo proprietário/conductor do veículo, e para que haja a interação entre o sistema e o cliente foi desenvolvido um código de *LEDs* de fácil entendimento:

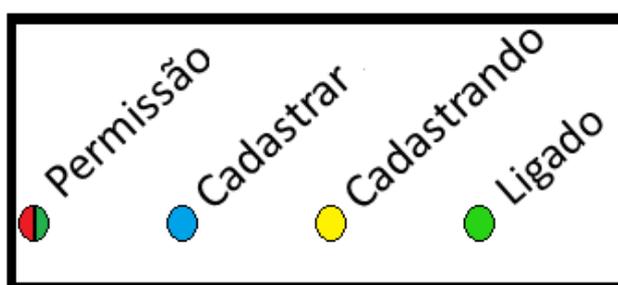


Figura 10 - Banco de *LEDs*

Cada *LED* possui uma ou mais funções específicas e acenderá conforme descrito a seguir:

Permissão: É um *LED* bicolor e acende tanto na cor verde como vermelho. Essencialmente, ele acende sempre que um chaveiro de permissão é lido pelo sistema. Quando **Permissão** acende na cor verde, o chaveiro lido permite o funcionamento do automóvel. Quando acende na cor vermelha, a permissão para funcionamento foi negada.

Cadastrar: É um *LED* de cor azul, acende sempre que o chaveiro-mestre é lido pelo sistema.

Cadastrando: É um *LED* de cor amarelo, acende sempre que o sistema está executando a gravação de um novo chaveiro de permissão.

Ligado: É um *LED* de cor verde, e permanece ligado enquanto o módulo está energizado, indicando funcionamento pleno do sistema.

Portanto, quando inicializado (através da chave de ignição) o módulo apresenta somente o *LED Ligado* aceso.



Figura 11 - Acionamento do LED verde (módulo ligado)

4.1.2 Cadastramento de novo chaveiro

Inicialmente o sistema não possui nenhum chaveiro cadastrado em seu banco de dados.

Para adicionar um chaveiro, basta aproximar o chaveiro-mestre do leitor até que haja o sinal sonoro e aguardar o *LED* azul (**Cadastrar**) acender;



Figura 12 - *LED* azul, indica que o cartão mestre foi apresentado

Após o *LED* **Cadastrar** apagar, o módulo entra em modo de gravação, já sendo possível efetuar o cadastro de um novo chaveiro;

Em seguida, basta aproximar o chaveiro a ser cadastrado e esperar que o *LED* amarelo (**Cadastrando**) acenda, indicando que a gravação está sendo realizada;



Figura 13 - *LED* amarelo, indica que o cartão apresentado esta sendo gravado

Após o *LED* amarelo apagar, o *LED* verde (**Permissão**) indica que o chaveiro foi gravado com sucesso;



Figura 14 - *LED* verde, indica sucesso na gravação

Após o *LED* **Permissão** apagar, o sistema de segurança está pronto para uso.



Figura 15 - Sistema volta ao estado inicial

4.1.3 Autenticação

Sempre que um chaveiro é cadastrado no sistema de segurança, ele permanece salvo mesmo que o módulo seja desligado, para verificar quais chaveiros já estão gravados, basta que, com o módulo ligado, os cartões sejam aproximados do leitor, até que haja o sinal sonoro. O **LED Permissão** indica se o chaveiro está cadastrado ou não.

Caso **não** esteja cadastrado, **Permissão** acende na cor vermelho:



Figura 16 - *LED* vermelho, indica que o cartão apresentado não esta cadastrado

Caso esteja cadastrado, **Permissão** acende na cor verde:



Figura 17 - *LED* verde, indica que o cartão apresentado esta cadastrado

Atenção: Quando **Permissão** acender na cor verde, o veículo já está habilitado para partida do motor.

4.1.4 Exclusão de chaveiros já cadastrados

Caso o proprietário do veículo perca um ou mais chaveiros e deseje apagá-lo(s) do sistema visando otimizar o espaço de memória, o módulo conta com uma etapa de exclusão dos chaveiros já gravados. Porém, nesta etapa todos os chaveiros são apagados, já que o proprietário não sabe em qual espaço de memória os dados dos chaveiros foram armazenados. Logo, faz-se necessária a nova gravação dos chaveiros dos quais ainda se tem posse.

Para realizar a exclusão dos dados da memória, o módulo necessita “entender” a real intenção do cliente. Afim de não excluir dados de maneira indevida, é fundamental uma “confirmação de exclusão” por parte do cliente. Para tanto é necessário que o chaveiro-mestre seja lido cinco vezes consecutivas pelo leitor para entrar em modo de exclusão.

Em cada uma das cinco aproximações, o **LED Cadastrar** deve acender e apagar, para que seja realizada nova aproximação:



Figura 18 - LED azul, necessário que este seja ativado 5 vezes

Após cinco aproximações válidas consecutivas, todos os LEDs acenderão, indicando que toda a memória está apagada.



Figura 19 - Acionamento de todos os LEDs

Em seguida o módulo já está preparado para cadastrar novamente os chaveiros de permissão ainda em posse do proprietário do automóvel, conforme descrito anteriormente.

4.1.5 Bloqueio do veículo

O módulo de segurança é inicializado em paralelo ao painel do automóvel (por meio de chave de ignição) e a partir do momento em que se encontra energizado, começa verificar a aproximação de chaveiros.

Neste momento a bomba de combustível permanece sem energia para funcionamento, porém, mesmo após a aproximação de um chaveiro de permissão cadastrado a bomba de combustível permanece desligada. Somente após a tentativa de ignição a bomba entra em funcionamento, alimentando o sistema de partida do motor.

Quando a tentativa de ignição do veículo ocorre sem autorização prévia por meio de chaveiro cadastrado, a bomba de combustível permanece desligada e uma indicação de falha é gerada no painel no veículo, visando desestimular novas tentativas de ignição sem que haja permissão por meio de chaveiro cadastrado.

Enquanto o sistema não é desligado a indicação de falha permanece. Porém, quando um chaveiro cadastrado é lido, e nova tentativa de ignição acontece, a indicação de falha desaparece e a bomba de combustível é energizada, permitindo o funcionamento pleno do motor.

Quando o sistema é desligado a indicação de falha desaparece, tornando a aparecer caso haja nova tentativa de ignição sem permissão.

4.2 Integração dos Principais Dispositivos

O processo de desenvolvimento do protótipo foi iniciado com base na integração das tecnologias escolhidas de modo a associá-las entre si para que haja comunicação plena, tratamento adequado dos dados transmitidos e tomadas de decisão conforme necessidade.

Inicialmente estudou-se o leitor *ID-20LA* a fim de compreender quais informações são transmitidas ao microcontrolador, quais as características dos protocolos de informação e qual o protocolo mais adequado para tratamento pelo microcontrolador.

Para tanto, montou-se o circuito do leitor *ID-20LA* em uma matriz de contatos conforme configuração desejada e utilizou-se um conversor *Serial RS232 ↔ USB* (modelo *PL2303HX*) para ler por um microcomputador quais dados das *TAGs* eram transmitidos do leitor para o microcontrolador, através do canal serial.

Dentre os protocolos fornecidos, conforme configuração do circuito do leitor, o mais adequado para tratamento é o *ASC II* devido ao vasto material de pesquisa e à facilidade no entendimento dos dados.

A partir do protocolo de informação *ASC II*, uma sequência de 14 *bytes* é transmitida, onde cada *byte* indica na tabela *ASC II* o seu respectivo caractere, conforme mostrado a seguir:

Sequência de *bytes* transmitidos, pertencente ao chaveiro-mestre:

(N° 001348387)

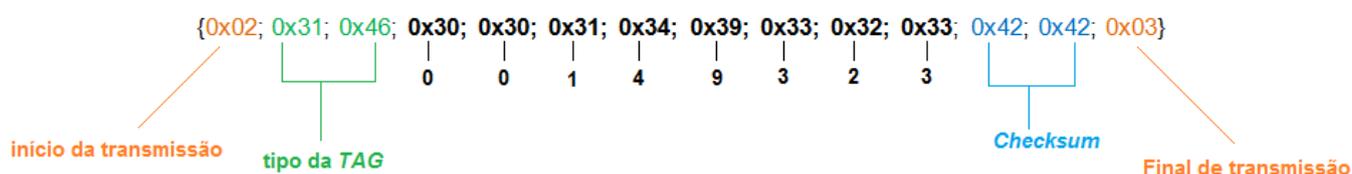


Figura 20 - Dados transmitidos pelo TAG

Forma-se o código em **hexadecimal**: 00149323, que convertendo para decimal obtêm-se: 001348387.

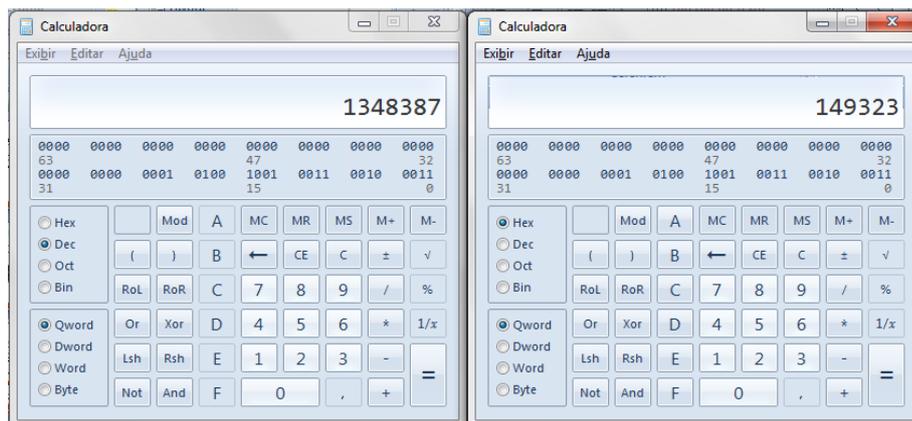


Figura 21 - Conversão DEC -> HEX

A sequência decimal 1348387 pode ser lida no corpo do chaveiro:



Figura 22 - Chaveiro estudado

Enquanto a sequência 149323 é lida no computador, a partir do *hyperterminal* do simulador *Proteus 8*, conforme visto a seguir:

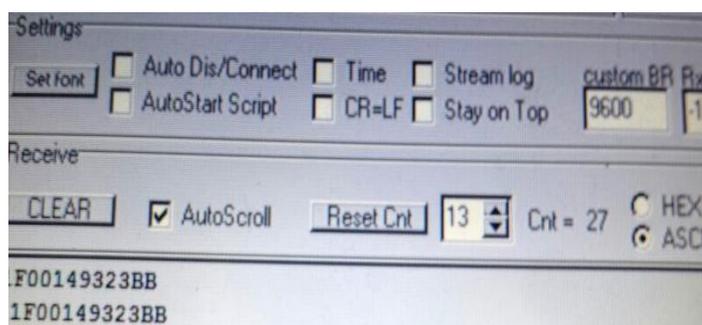


Figura 23 - Utilização do hyperterminal do software Proteus 8

Os dados tratados possuem o mesmo valor, embora em sistemas diferentes de numeração, porém o algoritmo lógico deve obedecer às condições da etapa de transmissão (hexadecimal), visando aperfeiçoar o sistema, minimizando o código-fonte e a memória utilizada para armazenamento.

Os dados do protocolo ASC // podem ser verificados na tabela a seguir:

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	\$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(72	48	H	104	68	h
9	09	Horizontal tab	41	29)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	
29	1D	Group separator	61	3D	=	93	5D]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Figura 24 - Tabela ASCII

4.3 Código-fonte

Com base nas informações obtidas por meio do procedimento descrito anteriormente e, em conjunto com o conhecimento prévio em linguagem de programação, desenvolveu-se o código-fonte em linguagem 'C' de modo a executar as tomadas de decisão, conforme descritas na etapa de funcionamento.

Tal código foi desenvolvido com o auxílio do *software* "MikroC PRO for PIC" produzido e distribuído pela *Microchip*®. A escolha de tal *software* foi principalmente devido à fácil utilização e por ser gratuito.

O código foi feito de maneira estruturada facilitando assim os ajustes e alterações do programador. Como visto a seguir:

```
/*Trabalho de conclusão de curso para graduação de Tecnologia  
em Eletrônica Industrial, FATEC-SP  
Segundo semestre de 2016.
```

```
Grupo: DANILO LANGELLOTTI, GUSTAVO ROBERTO ROSA e RAFAEL SILVA  
BEGA.
```

```
Orientador: Prof. Me. Ricardo Rangel.
```

```
Tema: SISTEMA DE AUTENTICAÇÃO VEICULAR POR RFID */
```

```
clear();
```

```
compara_eeeprom();
```

```
grava_chaveiro();
```

```
limpa_eeeprom();
```

```
char rfid [14]; // Recebe 14 bytes que chegam na UART a cada  
aproximação dos chaveiros.
```

```
char cartao [14] =
```

```
{0x02,0x31,0x46,0x30,0x30,0x31,0x34,0x39,0x33,0x32,0x33,0x42,0  
x42,0x03}; // Referente ao chaveiro mestre 0001348387
```

```

char eeprom [10]; //armazena o conteúdo da rfid, excluindo os
bytes de controle.
int i; //Controle de recepção da UART, cada byte recebido
deixa i=i+1;
int a; //laço para comparação dos bytes recebidos com os
chaveiros cadastrados.
int chaveiro_mestre=2; //Indicação de estágio.
int pos; // Contador dos chaveiros cadastrados na EEPROM.
int adress; //Ponteiro de endereço da EEPROM.
int mc=0; //Controle do Master Clear.
int libera_acesso=0; //Controle de liberação do acesso.
int grava=0; //Indicador do estágio de gravação.
int erro=0b00000010; //Variável referente ao código de erro.

void interrupt() //Interrupção: recebe dados da UART e do
pino RB0.
{
if(PIR1.RCIF==1)
    {
if (i>13) i=0;
rfid[i] = uart1_read();
i++;
PIR1.RCIF == 0;
}
if(INTCON.INTF == 1)
{
if (libera_acesso==1 && grava==0) portd.rd7=1; //Pino que
ativa rele!
    if (libera_acesso==0) // Gerador de erro;

```

```

    {
portd=erro;
erro=erro<<1;
    if (erro==0b00100000) erro=0b00000010;
    }

INTCON.INTF = 0x0;
}
}

void compara_eeprom() //Sub-rotina que faz a comparação do
chaveiro lido com o conteúdo da EEPROM.
{
    int valida;
    int s=0;
for (s=0;s<pos+1;s++)
    {
        valida=1;
for (a=2;a<12;a++)
    {
        adress= 10*s;
        adress=adress+a;
        eeprom[a]= eeprom_read(adress);
        delay_ms(10);

if (rfid[a] != eeprom[a] ) valida=0;
if (a==11 && valida==1) //libera_acesso();
        {
            porta.ra0=1;
            delay_ms(2000) ;
        }
    }
}
}

```

```

        porta.ra0=0;
        if (grava==0) libera_acesso=1;
        goto sai;
    }
}
}
    if (valida==0)
    {
        porta.RA1=1;
        delay_ms(1000);
        porta.RA1=0;
    }
sai:
    porta=0;
    chaveiro_mestre = 1;
}
void clear() //Subrotina para zerar variáveis
{
    int x;
    i=0;
    for (x=0;x<=14;x++) rfid[x] =0;
    for (x=0;x<=14;x++) eeprom[x] =0;
    porta=0;
    chaveiro_mestre=2;
    mc=0;
}

void limpa_eeprom() //Sub-rotina ativada no Master Clear, zera
o conteúdo da EEPROM.

```

```

{
int e;
for (e=0; e<256; e++)
{
    porta=255;
    eeprom_write(e,0x00);
    delay_ms(10);
}
porta=0;
pos=0;
}
void verifica_chaveiro_mestre() //Sub-rotina que compara o
chaveiro lido com a variável "cartao" que possui o código
mestre.
{
    for (a=2;a<12;a++)
    {
        if (rfid[a] != cartao [a] && chaveiro_mestre==2)
compara_eeprom(); //Se houver diferença entre o dado recebido
e a variável cartão, entra em compara eeprom...
        if (a==11 && chaveiro_mestre==2) // Se chaveiro mestre
detectado, faça
    {
        porta.ra2=1;
        delay_ms(2000);
        clear();
chaveiro_mestre=3;
    }
}
}

```

```

}
void grava_chaveiro()
{
    grava=1;

    for (a=2;a<12;a++)          // Laço que verifica se o
chaveiro passado foi o chaveiro mestre...
{
    if (rfid[a] != cartao [a]) break;
        if (a==11)
        {
            mc++;
            if (mc==4)
                {
limpa_eeeprom();
                clear();
                chaveiro_mestre=1;
                porta.ra3 = 0;
                }

            goto sai;
        }
}
adress=0;
for (a=2;a<12;a++)
{
adress=10*pos;
adress=adress+a;
Eeprom_Write(adress,rfid[a]);

```

```

delay_ms(10);
    porta.ra3 = 1;
}
pos++;
eeprom_write(0xff,pos);
delay_ms(1000);
sai:
if (mc!=4)
{
    chaveiro_mestre=2;
    porta.ra3 = 0;
}
    if (mc==4) mc=0;
}
void main()
{
    PIE1.RCIE = 1; //ATIVA INTERRUPTÃO DO RECEBIMENTO DA UART
    INTCON.GIE=1; //habilita interrupção global;
    INTCON.PEIE=1; //habilita interrupção dos perifericos;
    INTCON.INTE=1; //habilita interrupção do pino rb0;
    OPTION_REG.INTEDG = 1; //Interrupt on rising edge

    adcon1=0x07;
    trisb.rb0=1; //define pino rb0 como input;
    trisb.rb7=0;
    trisa=0;
    trisd=0;
    porta=0;
    portd=0;

```

```

    UART1_Init(9600); // initialize UART1 module
Delay_ms(100);

clear();
pos=eeprom_read(0xff);
if (pos==0b11111111) eeprom_write(0xff,0x00); //Verifica se
nã há chaveiros gravados através do valor do primeiro ...
delay_ms(10);
pos=eeprom_read(0xff);
Delay_ms(10); //Pausa obrigatória para gravação na eeprom.

portb.rb7=1; // LED DE CONTROLE DE FUNCIONAMENTO.

while(1) // Loop infinito
{
    if (i==14)
    {
        grava=0;
        if (chaveiro_mestre==3) grava_chaveiro();
        if (chaveiro_mestre==2) verifica_chaveiro_mestre();

        if (chaveiro_mestre==1)
        {
            clear();
            chaveiro_mestre=2;
        }
    }
}
}
}}
```

4.4 Fluxograma

O fluxograma é uma representação gráfica de um processo ou trabalho descrito geralmente com a utilização de figuras geométricas unidas por setas. Pode ser definido como o gráfico em que se representa o percurso ou caminho percorrido por certo elemento. Portanto, a existência de um fluxograma em um trabalho é fundamental para simplificação e racionalização do trabalho.

O fluxograma desenvolvido para o Sistema de Segurança Veicular indica tomadas de decisão conforme os dados recebidos, e foi desenvolvido a partir do *software* “*ClickChart Diagram Flowchart*” e pode ser visto a seguir:

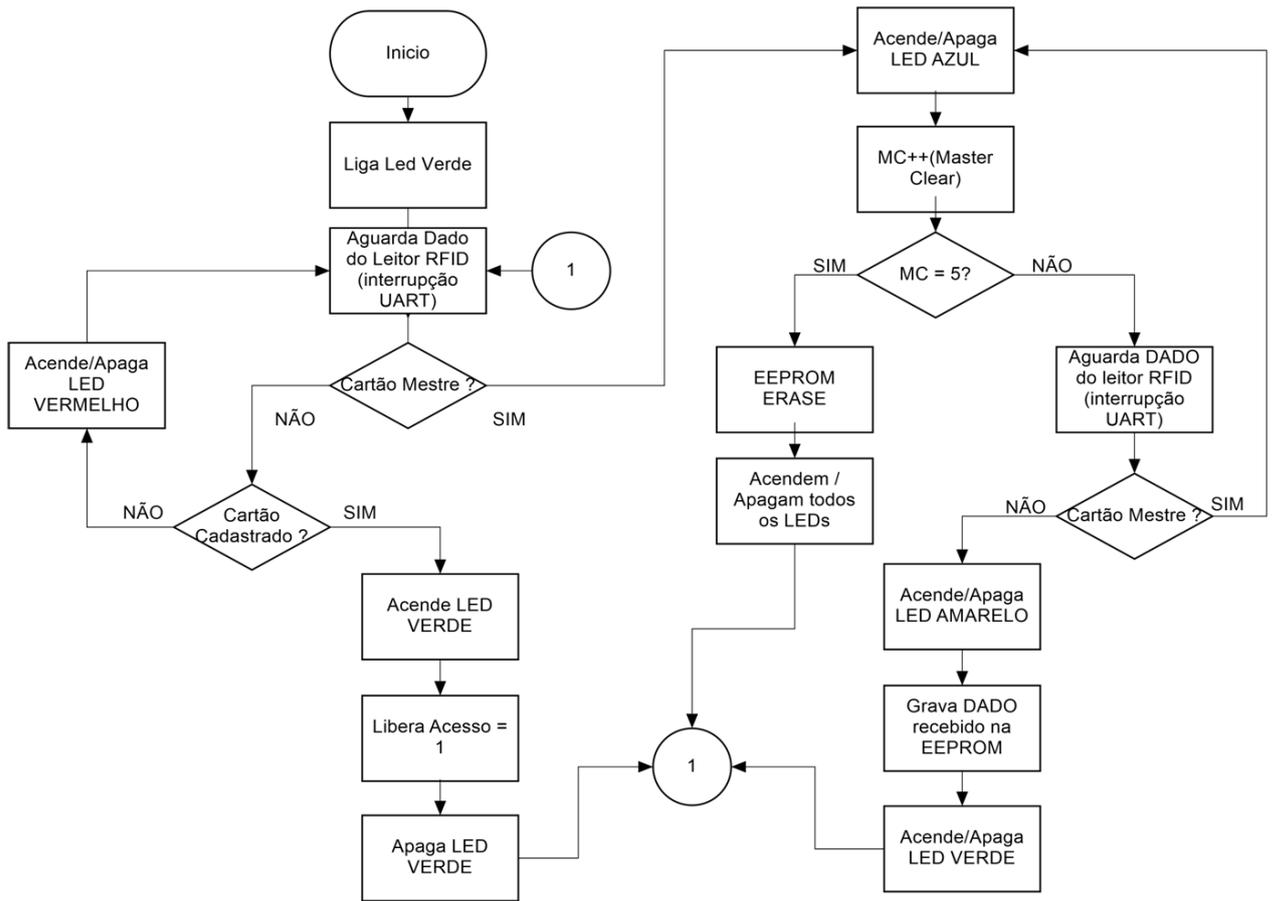


Figura 25 - Fluxograma rotina VOID MAIN

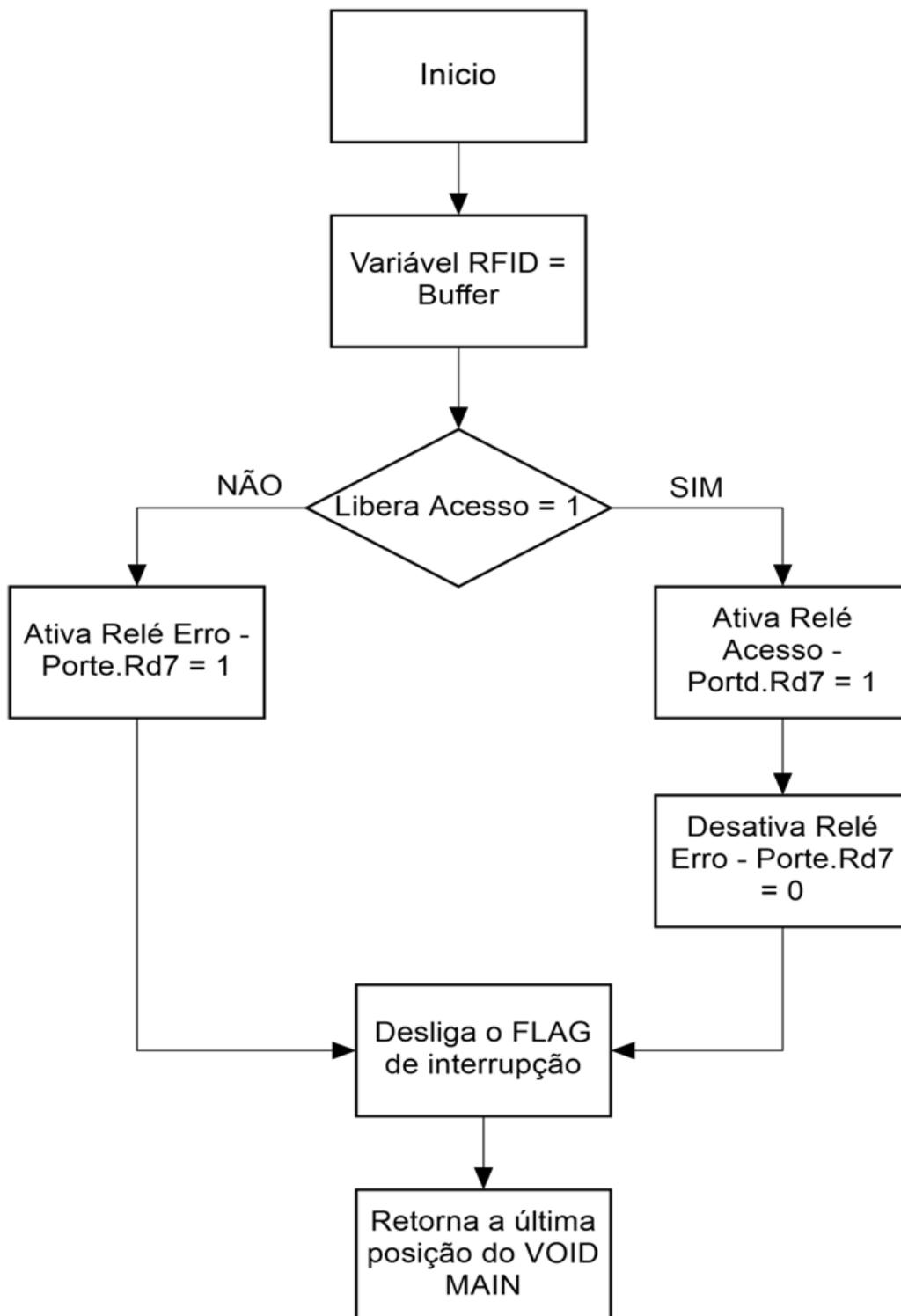


Figura 26 - Fluxograma VOID INTERRUPT

4.3 Simulador

Todo projeto eletrônico necessita sempre ser simulado antes de qualquer tipo de montagem física para já evitar problemas básicos como erros de programação, erros na seleção de componentes.

Para este trabalho foi escolhido o *software* “*Proteus 8 Professional*” devido principalmente ao mesmo ser extremamente poderoso, contendo ferramentas de simulação, visualização em 3D, confecção de arquivo Gerber (esquemático para fabricação da placa de circuito impresso) e vasta biblioteca de componentes.

O *software* é dividido em duas partes, sendo a primeira chamada *ISIS* (onde é possível a construção do esquemático e as simulações) e a segunda chamada *ARES* (responsável pela fabricação da placa de circuito impresso).

Para o desenvolvimento do protótipo utilizou-se somente o *ISIS*, para a construção do circuito elétrico, bem como as simulações necessárias, como de transmissão de dados por meio do canal serial.

O circuito elétrico foi elaborado baseado em pesquisas realizadas e em conjunto aos conhecimentos prévios, de modo a buscar a otimização do resultado, eliminando ruídos elétricos e magnéticos em componentes que poderiam sofrer com tais influências externas. O circuito completo pode ser visto a seguir:

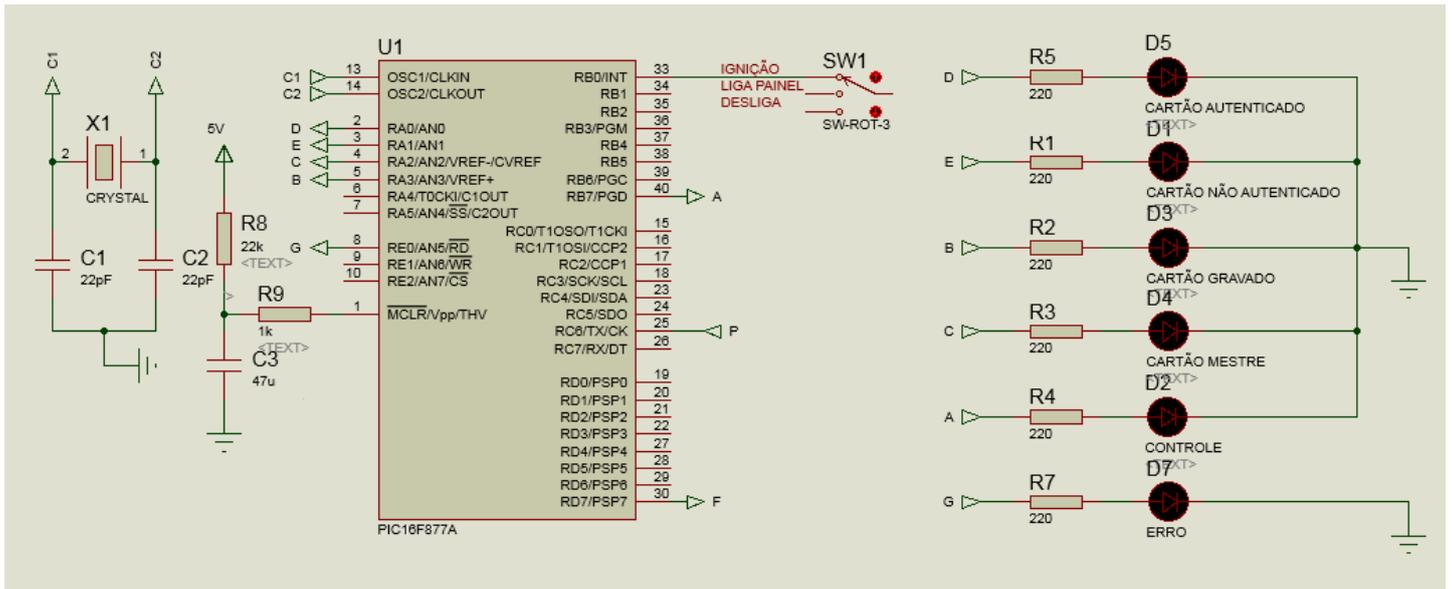


Figura 27 - Circuito simulado via Proteus 8

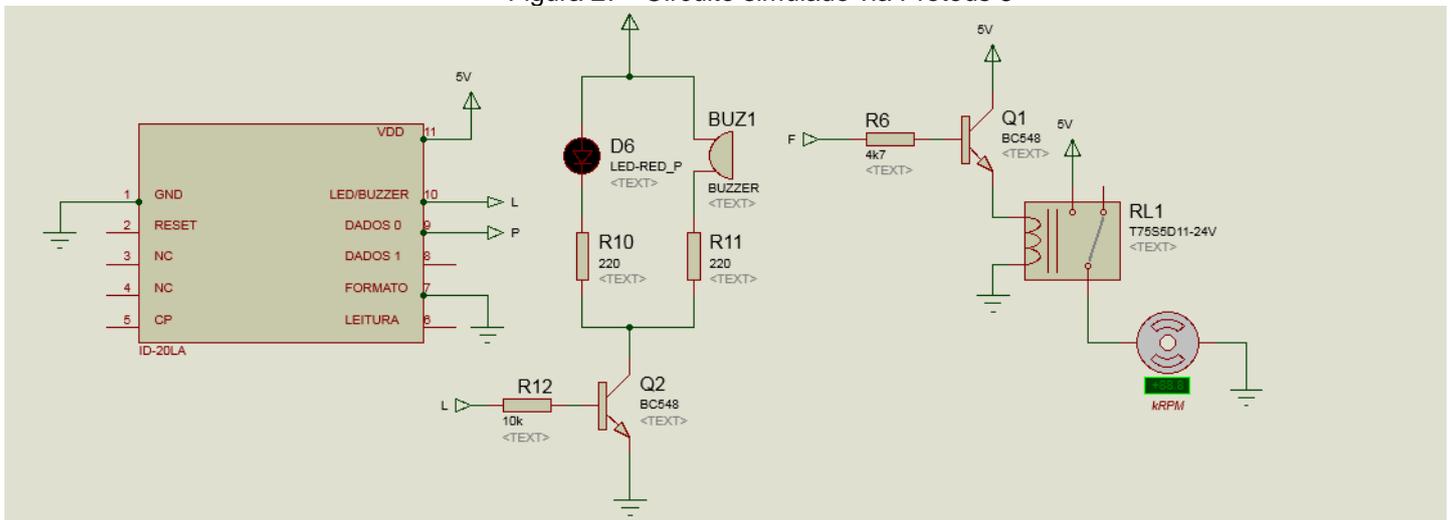


Figura 28 - Circuito simulado via Proteus 8

4.4 Montagem

A montagem do circuito apresentado anteriormente foi executada sobre uma placa perfurada padronizada com distancia entre furos de 2,54 milímetros (mm), visando três características básicas: Facilitar o processo de montagem, evitar problemas de funcionamento do circuito final, e facilitar a operação, visualização e entendimento do sistema, quando finalizado.

Assim sendo, adotaram-se características que buscassem atender cada um dos casos anteriores.

Visando facilitar o processo de montagem, foram inseridos na placa primeiramente os componentes com maior número de conexões, como o leitor *ID-20LA* e o microcontrolador *PIC 16F877A*, com foco em facilitar o processo de distribuição de componentes pela área da placa.

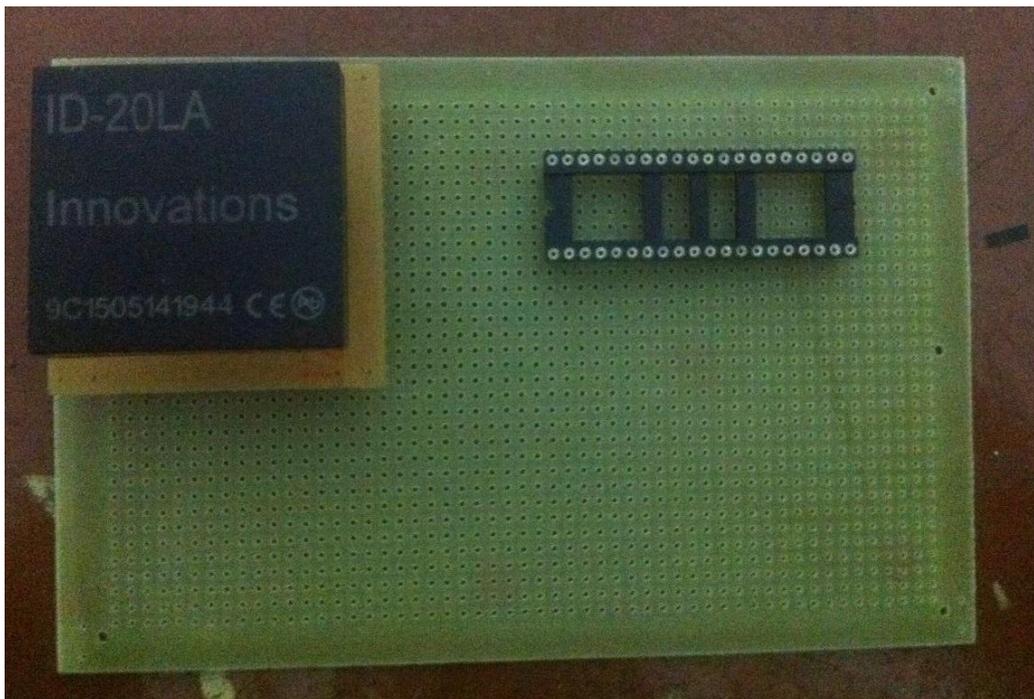


Figura 29 - Início da montagem na placa universal

Ainda visando facilitar a montagem e entendimento do circuito, utilizaram-se fios de cores diferentes para identificação dos diferentes sinais elétricos, como V_{CC} (+), GND (-), sinal serial, entre outros.

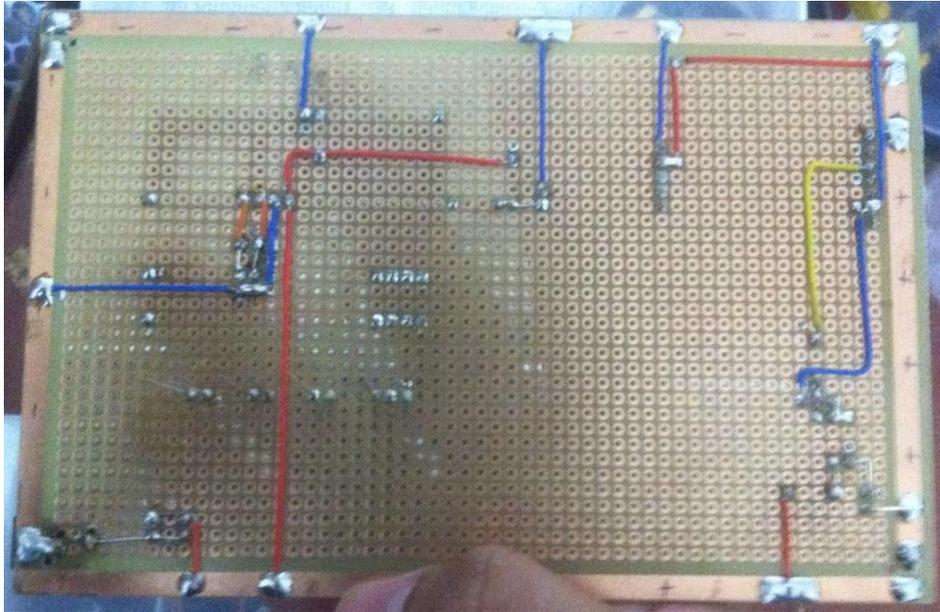


Figura 30 - Fios soldados realizando a função das trilhas

Com o intuito de evitar problemas de funcionamento por meio de ruídos, os componentes foram distribuídos de modo a minimizar a quantidade de conexões sobrepostas na parte inferior da placa:

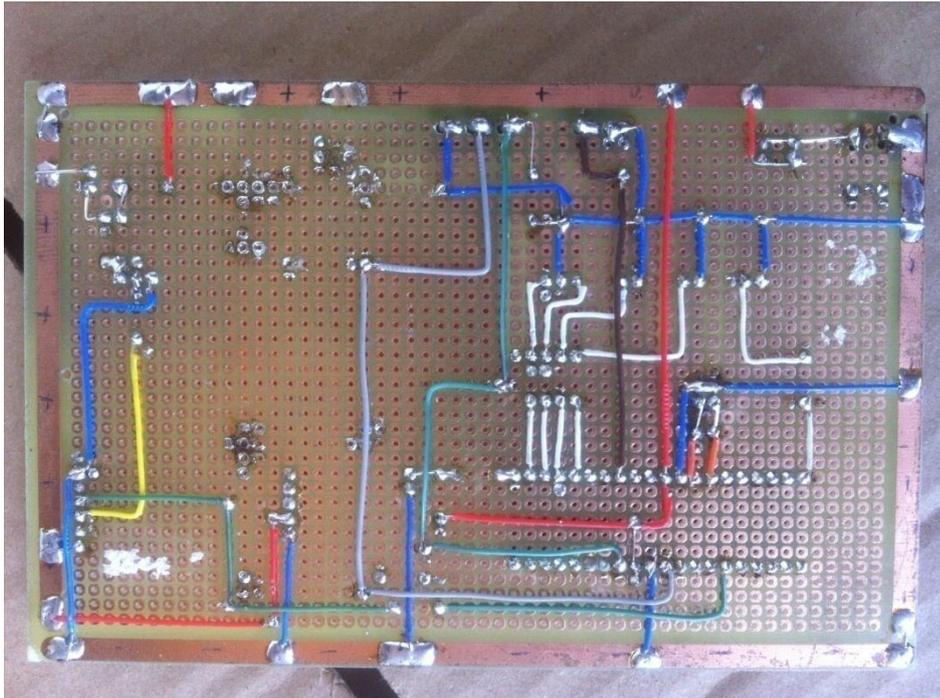


Figura 31 - Aspecto final do circuito 100% montado/soldado

Outra ação visando evitar problemas com funcionamento foi manter o leitor *ID-20LA* a certa distancia dos componentes eletrônicos, evitando que ruídos provenientes de tais componentes pudessem interferir na leitura dos chaveiros. Para tanto, manteve-se o leitor elevado em relação à placa, com as conexões via cabo *flat* e com o leitor permitindo ser conectado ou extraído quando necessário, por meio de receptáculos adaptados.

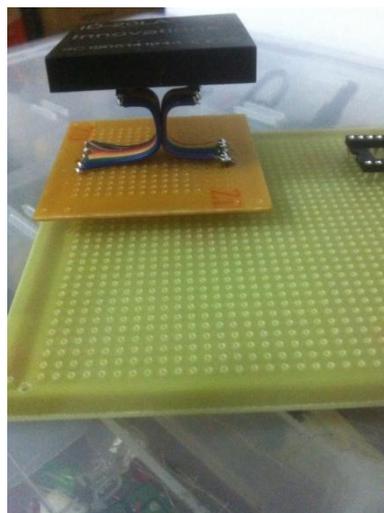


Figura 32 - Montagem do ID-20LA

Por fim, o leiaute do módulo principal foi desenvolvido de modo a facilitar a operação, com algumas características voltadas para isso, como o dispositivo leitor que se encontra na extremidade da placa, facilitando aproximação do chaveiro, ou mesmo o circuito de indicação de leitura (sinal sonoro e luminoso) separados do circuito de comandos, visualmente.

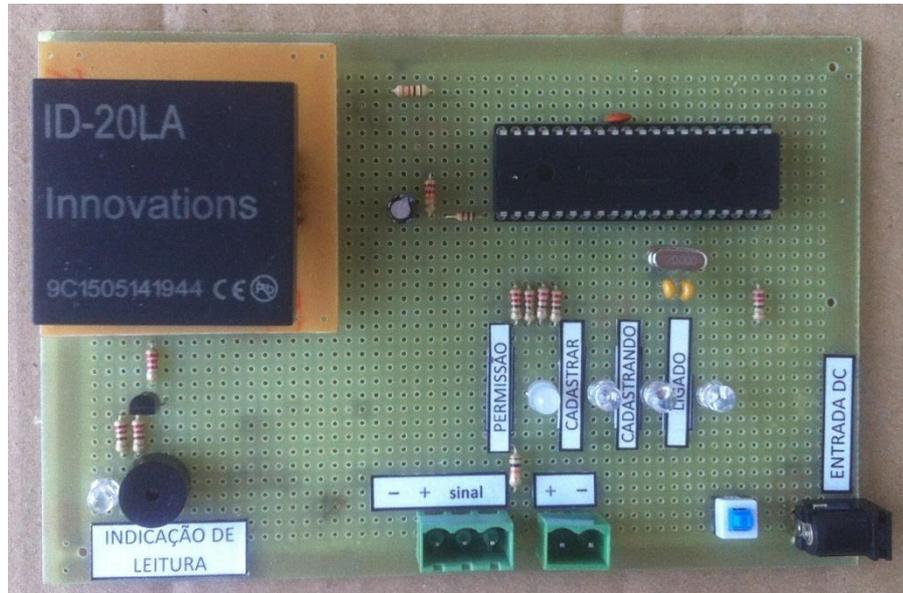


Figura 33 - Aspecto final do módulo

4.5 Circuitos Auxiliares

Foram utilizados, durante a etapa de apresentação, circuitos auxiliares para demonstração do pleno funcionamento do projeto apresentado. Foram ao todo três circuitos auxiliares, sendo eles: circuito simulador da chave de ignição do automóvel, circuito de chaveamento da bomba de combustível e circuito de chaveamento para ligação do painel e indicação de falha.

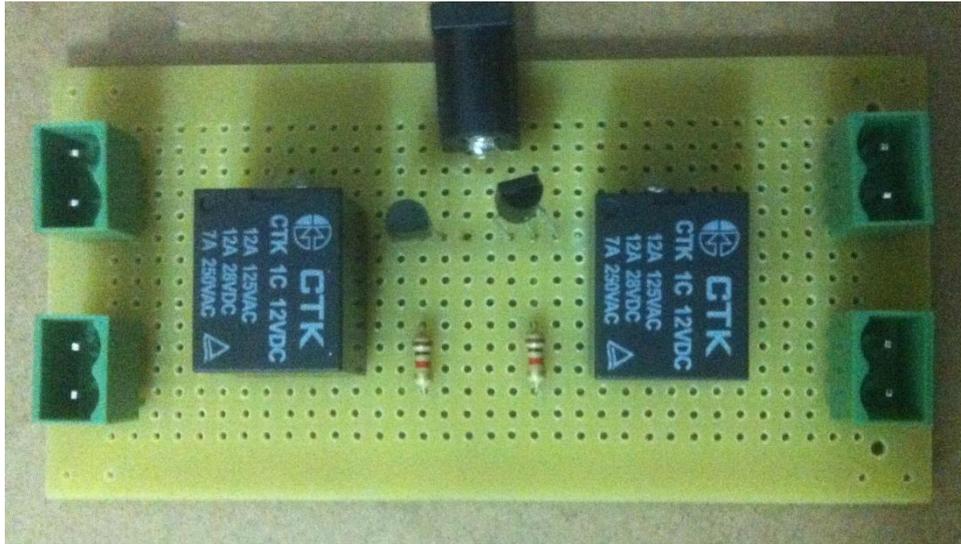


Figura 34 - Módulo de chaveamento dos circuitos de potência



Figura 35 - Chave de Ignição montada e etiquetada

4.5.1 Simulador da chave de ignição do automóvel

Possui uma chave de três posições (0, 1 e 2), onde duas posições (0 e 1) possuem trava e a terceira (2) possui retorno por mola para a posição central (1).

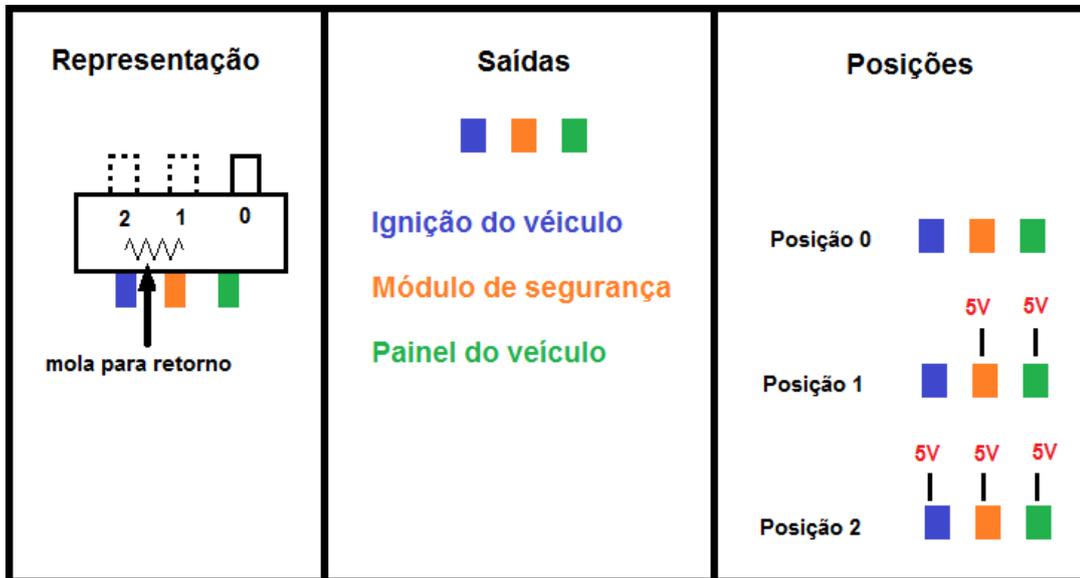


Figura 36 - Posições da chave de ignição

Na posição 0 (zero) todos os circuitos estão desligados;

Na posição 1 (um) o módulo de segurança e o painel estão ligados; e

Na posição 2 (dois) os circuitos do módulo de segurança e do painel do veículo permanecem ligados e um pulso elétrico é enviado ao circuito de ignição e ao microcontrolador do módulo de segurança, para verificar permissão para ligar a bomba de combustível.

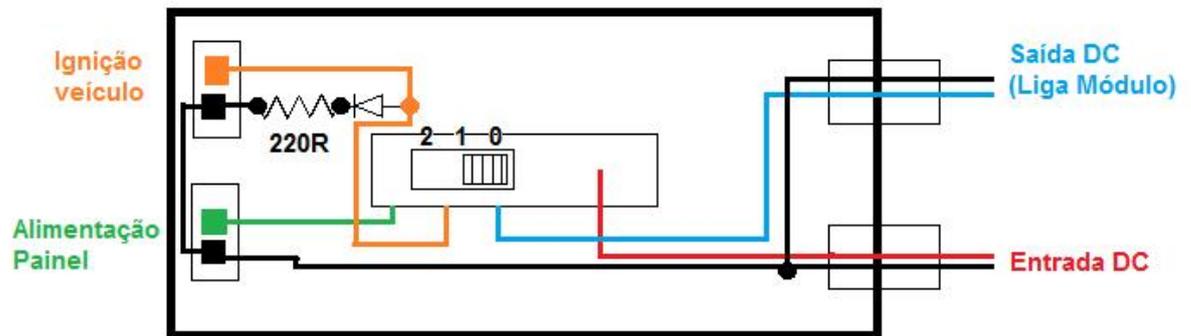


Figura 37 - Circuito da chave de ignição

4.5.2 Circuito de chaveamento da bomba de combustível

A bomba de combustível é um dispositivo de potência. É controlado pelo microcontrolador, um dispositivo de comando, sendo que este é incapaz de ligar ou desligar a bomba de combustível sem auxílio de um equipamento robusto, devido ao elevado nível de corrente exigida para executar tal tarefa.

Para tanto, utilizou-se um relê eletromecânico de 5 V_{CC}, e para representação da bomba de combustível do veículo utilizou-se um motor elétrico com alimentação de 5V_{CC}. O circuito auxiliar foi alimentado por uma bateria de 9V_{CC} em conjunto com um regulador de tensão 7805, conforme representação a seguir:

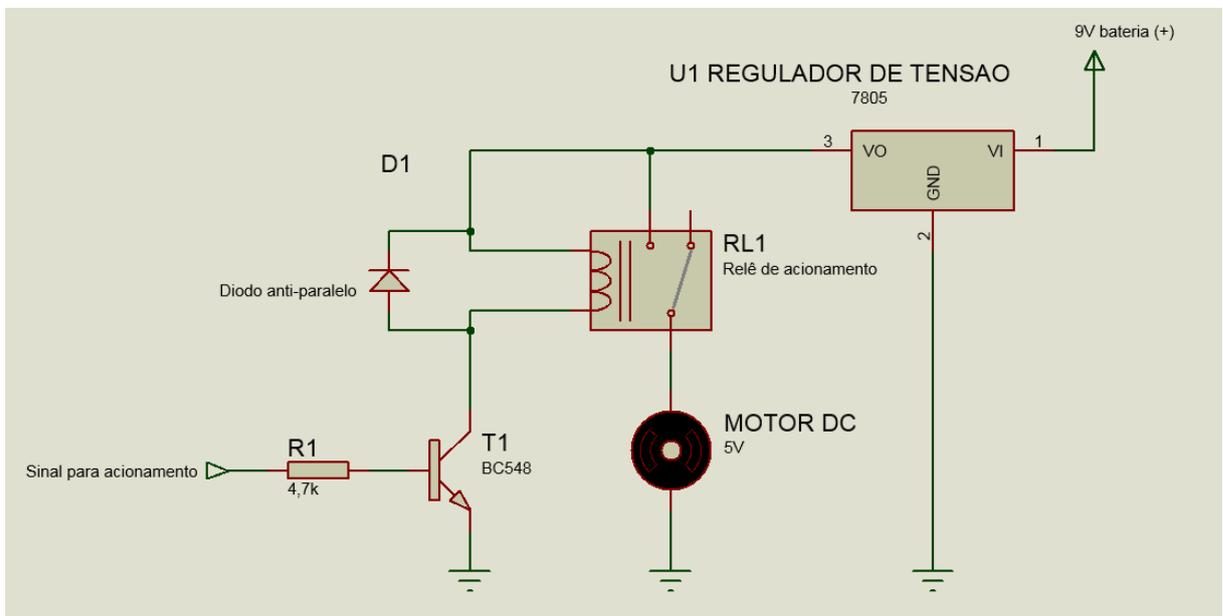


Figura 38 - Circuito de potência atuante na bomba de combustível

4.5.3 Circuito de chaveamento para ligação do painel e indicação de falha

O painel do automóvel é alimentado com tensão de 12 V_{CC}, porém, o comando de ligação é oriundo da chave de ignição. Esta chave, por sua vez, trabalha com tensão de 5 V_{CC}, devido à alimentação do módulo de segurança. Deste modo a tensão na qual a chave fornece não é suficiente para ligar o painel de maneira independente.

Em outra situação, encontra-se a lâmpada de falsa indicação de falha, que opera em 12 V_{CC}, e é controlada pelo microcontrolador, porém este dispositivo não possui capacidade para energizar a lâmpada de maneira autônoma.

Em ambos os casos, utilizaram-se relês eletromecânicos como estratégia de proteção ao circuito eletrônico.

A representação a seguir demonstra como e quais foram os dispositivos utilizados para montagem desta placa auxiliar.

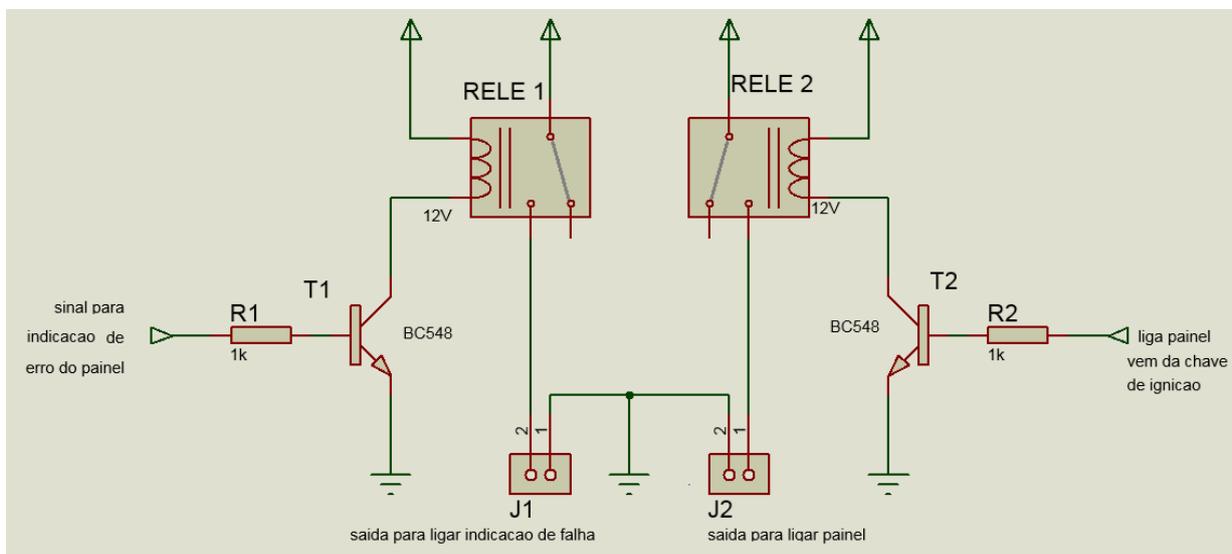


Figura 39 - Circuito de potência para ativação do painel

5 O PRODUTO NO MERCADO

5.1 O produto é destinado a quem?

O Sistema de Autenticação Veicular é um módulo de segurança destinado a veículos automotores, independente de tamanho, utilização e modelo. Suas limitações são mínimas quando se trata de veículos com sistema de ignição convencional, por meio de chave codificada.

Devido à flexibilidade oferecida na quantidade de possíveis condutores, o módulo atende desde veículos particulares até pequenas frotas de empresas ou prestadoras de serviço.

5.2 Quais vantagens oferece?

Além da segurança, tida como item principal, o módulo de segurança pode trazer vantagens como: valorização significativa do veículo no momento de uma possível venda (podendo ultrapassar o próprio valor do produto), amortização de valor do prêmio e/ou franquia do seguro do veículo, desde que constatado pela empresa seguradora a utilização do módulo, entre outros.

5.3 Já existe produto semelhante?

Sim, em *sites* de vendas *online* internacionais pode-se encontrar produtos semelhantes. No entanto, o produto proposto apresenta vantagens significativas quando comparados aos já existentes:

Preço: Em *sites* internacionais os produtos semelhantes variam em torno de US\$ 150,00 a US\$ 250,00 (aproximadamente R\$ 450,00 a R\$ 750,00 conforme câmbio diário), excluindo-se as taxas alfandegárias, que podem elevar significativamente o valor inicial. Já o protótipo proposto, por se tratar de um produto nacional não necessita tais taxas, e teve um orçamento aproximado de R\$ 260,00 (valor de produção), sendo fortemente amenizado caso produzido em larga escala.

Flexibilidade: Quando comparado à outros produtos semelhantes, o proposto possui uma vantagem considerável, em se tratando de flexibilidade, pois os produtos

já oferecidos são comumente limitados a dois chaveiros por veículo, sem opção de acréscimo ou exclusão conforme necessidade.

Discrição: Outro diferencial relevante é o sistema de simulação de defeito, desestimulando novas tentativas de violação por parte do infrator, e impedindo-o de saber que se trata de um sistema de segurança.

Comodidade: O chaveiro-mestre é mais um recurso específico do protótipo apresentado, pois facilita no manuseio e torna o sistema mais compreensível e satisfatório de se operar.

6 CONCLUSÃO

A partir do protótipo desenvolvido, pode-se concluir que dentre as mais diversas tecnologias, a de identificação por radiofrequência é ótima opção quando se trata de segurança e confiabilidade.

Esta tecnologia, quando aplicada à situação proposta pelo Sistema de Segurança Veicular, oferece a capacidade de identificar objetos (chaveiros) de maneira rápida e precisa. Ao ser tratada adequadamente, por meio de sistema microcontrolado, proporciona alto nível de comodidade e facilidade de operação (não se faz necessária a utilização de botões), elevada confiabilidade (TAGs possuem dados únicos em nível mundial), e flexibilidade (a quantidade de condutores de um mesmo veículo é ajustada conforme necessidade).

O dispositivo microcontrolador, por sua vez, quando pesquisado para determinar quais recursos mais se adequavam à necessidade do sistema, ofereceu uma altíssima gama de funções, onde, em alguns casos poder-se-iam utilizar funções distintas para se realizar uma mesma tarefa, ficando a encargo dos idealizadores definirem quais as mais adequadas. Para estas tomadas de decisões alguns fatores foram considerados, como minimização de custos, otimização de memória de armazenamento, diminuição de tempo de processamento e outras características que contribuíram a aperfeiçoar o desempenho do sistema como um todo.

7 BIBLIOGRAFIA

MICROCHIP PIC 16F877A – Datasheet. Disponível em: <<http://www.microchip.com/>>. Acesso em: 29 mar. 2016.

ID-Innovations ID-20LA – Datasheet.
Disponível em: < <http://cdn.sparkfun.com/datasheets/Sensors/ID/ID-2LA,%20ID-12LA,%20ID-20LA2013-4-10.pdf>>. Acesso em: 29 mar. 2016.

CIRIACO, Douglas: Como funciona a RFID?
Disponível em: <<http://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm>>. Acesso em: 02 abr. 2016.

SYSGEN: What is RFID
Disponível em:
<http://www.sysgen.com/inside/inside.php?content=Solutions&topic=What_Is_RFID>. Acesso em: 04 abr. 2016.

LANDT, Jeremy: The History of RFID
Disponível em:< <https://pt.scribd.com/doc/6685529/The-History-of-RFID>>. Acesso em: 04 abr. 2016

DIAS, Renata Rampim de Freitas: Diferenças entre as frequências do sistema RFID passivo.
Disponível em: < <https://brasil.rfidjournal.com/artigos/vision?9591/>>. Acesso em: 08 abr. 2016

SANTOS, Marco Aurélio da Silva: Capacitores
Disponível em: <<http://brasilecola.uol.com.br/fisica/capacitores.htm>>. Acesso em: 16 abr. 2016