

UNIVERSIDADE DE PASSO FUNDO

Esequiel Rovani

SISTEMA PARA CONTROLE DE ACESSO INTEGRADO
COM CENTRAL DE ALARME

Passo Fundo

2019

Esequiel Rovani

SISTEMA PARA CONTROLE DE ACESSO INTEGRADO COM CENTRAL DE ALARME

Trabalho apresentado ao curso de Engenharia Elétrica, da Faculdade de Engenharia e Arquitetura, da Universidade de Passo Fundo, como requisito parcial para obtenção do grau de Engenheiro Eletricista, sob orientação do professor Dr. Adriano Luís Toazza.

Passo Fundo

2019

Esequiel Rovani

Sistema de controle de acesso integrado com central de alarme

Trabalho apresentado ao curso de Engenharia Elétrica, da Faculdade de Engenharia e Arquitetura, da Universidade de Passo Fundo, como requisito parcial para obtenção do grau de Engenheiro Eletricista, sob orientação do professor Dr. Adriano Luís Toazza.

Aprovado em ____ de _____ de ____.

BANCA EXAMINADORA

Prof. Dr. Orientador Adriano Luiz Toazza - UPF

Prof. Dr. Carlos A.R Behaine- UPF

Prof. Dr. Blanca Rosa Moquera Sosa - UPF

RESUMO

O controle de acesso é um sistema utilizado para o gerenciamento de pessoas em um local restrito. O controle é feito através de equipamentos eletrônicos, clausuras e fechaduras, onde o usuário deve estar cadastrado para acessar o ambiente. Esses sistemas são projetados para atender os requisitos de segurança patrimonial. Em condomínios, há uma vulnerabilidade nestes sistemas, pois a maioria fica limitado somente em abrir e fechar portas, não tendo nenhuma integração com um sistema de alarme que gere notificação para uma empresa de monitoramento, caso haja intrusão.

No presente trabalho apresenta-se a integração de dois sistemas de segurança distintos em uma única central (alarme e controle de acesso), visando aumentar a segurança de entradas de condomínios, já que hoje no mercado existem equipamentos que caminham distantes neste quesito. A automação da clausura é feita através de um controle de acesso, o qual irá gerenciar o intertravamento das portas e liberá-las por *tag*, Senha, disparo no sistema de incêndio e liberação autônoma pelo sistema de interfonia predial. O sistema também conta com detecção de intrusão por sensores magnéticos. Tudo isso é gerenciado por uma única central, onde a mesma tem saídas (contato seco) para integração com um dispositivo de transmissão de dados (GPRS ou Internet) que envia os eventos de disparos para uma central de monitoramento.

Palavras Chaves: Segurança Eletrônica, Clausura, Segurança Patrimonial, Dispositivos de transmissão, Controle de Acesso, Alarme.

ABSTRACT

The access control is a system used for managing people in a restricted location. The control is done through electronic equipment, enclosures and locks, where the user must be registered to access the environment. These systems are designed to meet property security requirements. In condominiums, there is a vulnerability in these systems, as most are limited only to opening and closing doors, and have no integration with an alarm system that generates notification to a monitoring company in case of intrusion.

The present work presents the integration of two distinct security systems in a single central (alarm and access control), aiming to increase the security of condominium entrances, since today in the market there are equipments that are distant in this aspect. The enclosure automation is done through an access control, which will manage the interlocking of the doors and release them by tag, Password, fire system firing and autonomous release by the building intercom system. The system also features intrusion detection by magnetic sensors. All of this is managed by a single switchboard, where it has outputs (dry contact) for integration with a data transmission device (GPRS or Internet) that sends trigger events to a monitoring switch.

Keywords: Electronic Security, Clausura, Property Security, Transmission Devices, Access Control, Alarm.

LISTA DE ILUSTRAÇÕES

Quadro 1 - Níveis de segurança física.	10
Gráfico 1 - Projeção de Crescimento do Setor de Segurança Eletrônica.	11
Figura 2 - Detecção Sensor Infravermelho.....	14
Figura 3- Esquema sensor Magnético.	15
Figura 4 - Sensor de fumaça.	16
Figura 5 - Central Paradox Evo e seus componentes.	18
Figura 6- Controladora de acesso Intelbras.	19
Quadro 2 - Frequências dos leitores RFID	20
Figura 8 - Componentes de uma etiqueta RFID.	21
Quadro 3 - Classe de tag RFID.....	22
Figura 9 - Modelos de tag existentes.	22
Figura 11 - Desenho do Protótipo de uma clausura em 2D.....	24
Figura 12 - Projeto maquete	25
Figura 13 - Foto da maquete.....	25
Figura 14 - Diagrama de blocos do hardware do sistema.....	26
Figura 15 - Pinagem da placa central	28
Figura 16 - Circuito de proteção das entradas	29
Figura 17 - Sistema de isolamento	30
Figura 18 - Filtro snubber.....	32
Figura 19 - Tela de acesso Menu.....	32
Figura 20 - Menu	33
Figura 21 – visualização da senha do menu e os tempos do sistema (opção 1).	33
Figura 22 - Alteração de senha (opção 2).	34
Figura 23 - Cadastro de tempos (opção 3).	34
Figura 24 - Tempo de acionamentos das fechaduras (opção 4).	35
Figura 25 - Visualização de senhas e tags (seção 5).	35
Figura 26 - Exclusão de senhas e tags (opção 6).	36
Figura 27 - Cadastramento de senhas (opção 7).	36
Figura 28 - Cadastramento de tag (opção 8).	37
Figura 29 - Esboço do Teclado.....	38
Figura 30 - Pinagem microcontrolador teclados.....	39
Quadro 4 - Organização dos dados enviados pelo leitor RFID.	40

Figura 32 - Redução da tensão para 5V.....	41
Figura 33 - Ligação Leds/buzzer.....	41
Figura 34 - Sensor magnético.....	43
Figura 35 - Sensor DSC LC 100.....	44
Figura 36 - Fechadura eletrônica.....	44
Figura 37 - Modulo de transmissão de eventos.....	45
Figura 38 - Detector de fumaça.....	46
Figura 39 - Fonte de alimentação do projeto.....	47
Figura 40 - Leitor RF ID RDM 6300.....	48
Figura 41 - Launch pad ARM.....	49
Figura 42 - Fluxograma de funcionamento firmware.....	51
Figura 43 – Interface de seleção dos ajustes via UART.....	56
Figura 44 – Funcionamento do firmware que salva os valores ajustados.....	57
Figura 45 – Leitura do tag via interface com o usuário.....	58
Figura 46 - Sistema armado.....	59
Figura 47 - Disparos de alarme da porta 1	59
Figura 48 - Sistema de alarme da maquete ativado.....	60
Figura 49 - Liberação da porta de entrada.....	61
Figura 50 - Mensagem de liberação das portas pela UART.....	61
Figura 51 - Mensagem de não liberação mostrada pela UART.....	62
Figura 52 - Protótipo em funcionamento.....	62
Figura 53 – Liberação da porta de saída.....	63
Figura 54 - Disparos de arrombamento recebidos pelo software de monitoramento.....	64
Figura 55 - Mensagens de alarmes exibidas na UART do protótipo.....	64
Figura 56 - Disparo do sistema de incêndio.....	65
Figura 57 - Mostra os eventos de incêndio gerados pela UART.....	65
Figura 58 - Disparos do sensor de porta aberta.....	66
Figura 59 - Alarme de porta aberta gerados pela UART.....	66
Figura 60 - Alarmes de porta 1 aberta	67
Figura 61 - Rearme do sistema.....	67
Figura 62 - Sistema de incêndio.....	68
Figura 63 - Disparo de sistema de incêndio	68
Figura 64 - Liberação pelo sistema de incêndio	69

LISTA DE TABELAS

Tabela 1 - Comparação dos principais índices de criminalidade no Rio Grande do Sul	6
Tabela 2 - Perspectiva para 2018.....	6
Tabela 3 - Velocidade de comunicação UART.	39

LISTA DE SIGLAS

ARM – *Advanced risc machine*.

CFTV – Circuito fechado de televisão.

GPRS – Serviço de pacotes por rádio.

IR – Infra *Red* ou infravermelho.

NA – Normalmente aberto.

NF – Normalmente fechado.

RFID – Identificação por rádio frequência.

UART – Transmissor/ Receptor universal assíncrono.

UHF – Frequência ultraelevada.

VA – Volt Ampere.

VDC – Tensão em corrente contínua.

Ah – Ampere hora.

RC – Resistivo, capacitivo.

EEPROM - *Electrically-Erasable Programmable Read-Only Memory*.

SUMÁRIO

1 INTRODUÇÃO	1
1.1 OBJETIVO GERAL.....	2
1.2 OBJETIVOS ESPECÍFICOS	2
1.3 JUSTIFICATIVAS	3
2 REVISÃO BIBLIOGRÁFICA	5
2.1 SEGURANÇA.....	5
2.1.1 Segurança Pública	5
2.1.2 Segurança Privada.....	7
2.1.3 Segurança Física	8
2.1.4 Segurança Eletrônica	11
2.1.5 Segurança em Condomínios	13
2.2 SISTEMA DE ALARME.....	13
2.2.1 Sensores para alarmes.....	14
2.3 CONTROLE DE ACESSO	16
2.3.1 Atribuição e funções do controle de acesso:.....	17
2.3.2 Sistemas de Controle de Acesso Paradox	17
2.3.3 Sistemas de Controle de Acesso Intelbras	19
2.4 CLAUSURA.....	19
2.5 LEITOR DE RFID	20
2.6 TAG	21
3 DESENVOLVIMENTO DO PROJETO.....	23
3.1 REQUISITOS DO SISTEMA	23
3.2 PROJETO DE SEGURANÇA DA CLAUSURA.....	24
3.3 PROJETO ELETRÔNICO	26
3.3.1 Placa Central.....	26
3.3.2 Interfaces com os usuários	37

3.4 COMPONENTES DO SISTEMA.....	43
3.4.1 Sensor <i>reed switch</i>	43
3.4.2 Sensor Infravermelho.....	43
3.4.3 Fechadura.....	44
3.4.4 Transmissão de eventos.....	45
3.4.5 Sensor de fumaça	45
3.4.6 Fonte de alimentação.....	46
3.6.7 Leitor de cartão RFID.....	47
3.5 FUNCIONAMENTO DO PROTÓTIPO	49
3.5.1 <i>Firmware</i>	50
3.5.2 Menu de ajuste	54
4 RESULTADOS E DISCUSSÕES.....	58
4.1 LEITURA DE SENHA E TAG PELO TECLADO	58
4.2 TESTE DO ALARME	59
4.3 TESTE DO SISTEMA DE ENTRADA.....	60
4.4 TESTE DO SISTEMA DE SAÍDA.....	62
4.5 TESTE DO SISTEMA DE EVENTOS GERADOS.....	63
4.6 TESTE DO SISTEMA DE DISPARO DE PORTA ABERTA	67
4.7 TESTE DO SISTEMA DE REARME/AUTO ARME	67
4.8 TESTE DO SISTEMA DE INCENDIO.....	68
4.9 IMPACTO NA SEGURANÇA CASO ALGUM COMPONENTE FALHE	69
5 CONSIDERAÇÕES FINAIS.....	71
6 REFERENCIAS BIBLIOGRÁFICAS	72
APÊNDICE A – FIRMWARE DE COMUNICAÇÃO DAS LAUNCH PADS.	74
APÊNDICE B – TRECHO DO FIRMWARE DAS INTERFACES DOS USUÁRIOS. .	76
APÊNDICE C – TRECHO DO FIRMWARE DO CADASTRO DAS SENHAS.....	78
APÊNDICE D – FIRMWARE DE PROTEÇÃO DA INTERFACE DE AJUSTES.....	79

APÊNDICE E – TRECHO DO FIRMWARE DE COMPARAÇÃO DE TAGS, SENHAS.	
.....	81
APÊNDICE F – LIGAÇÃO DOS DISPOSITIVOS NO SISTEMA.....	83

1 INTRODUÇÃO

Desde tempos remotos, a humanidade se preocupa com sua segurança física e patrimonial. Na pré-história, sempre que se tinha uma comunidade, havia aqueles que eram incumbidos de garantir os acessos de pessoas não autorizadas e dar o alarme caso houvesse algum tipo de calamidade ou perigo. Os seres humanos revezavam-se, estabelecendo estratégias para se proteger de situações de risco (ARAÚJO, 2007).

Com o passar dos séculos, em 1853, Augustus Pope criou o primeiro sistema de alarme antifurto. Ele consistia em um simples sistema de contatos e interruptores presos em portas e janelas e ligados a um sino, que ficava no quarto do proprietário, assim, quando o circuito se fechava, o sino soava. Algum tempo depois, um jovem empreendedor chamado Edwin Holmes comprou a invenção de Pope e aperfeiçoou e vendia para bancos, residências e joalherias em Nova York. Através das ligações de cabos telegráficos dos sistemas de alarme até sua empresa, ele estabeleceu a primeira empresa de Monitoramento. Estes clientes também investiam em sistemas de trancas e fechaduras mecânicas para proteger valores e locais onde somente pessoas autorizadas pudessem acessar através de algum tipo de código que era confiado a poucos (ARAÚJO, 2007).

Hoje, além da invenção de Pope e aperfeiçoamento da mesma, surgiram outros sistemas (câmeras, controle de acesso, etc.). O avanço da tecnologia fez com que eles interagissem entre si, dando um conceito amplo sobre segurança.

Estas interações impactaram muito no combate a roubos e furtos em propriedades privadas e os mesmos tiveram uma taxa de redução de 13% no período de 2014 a 2017 no estado do Rio Grande do Sul, segundo dados do site da Secretaria de Segurança Pública, mas para que isso continue, cada vez mais faz-se necessário a implementação da segurança por meio da tecnologia. O avanço rápido das telecomunicações propiciou hoje o surgimento de cidades digitais, onde uma rede inteligente de vídeo monitoramento se ramifica entre bairros e vilas, deixando a polícia muito mais ostensiva, e otimizando o trabalho do seu efetivo. Além disso, centrais de alarmes detectam e notificam intrusões em tempo real e sistemas de câmeras possibilitam aos seus usuários acesso à imagens e gravações em qualquer lugar do mundo. Todas estas tecnologias trabalham em conjunto com a ação humana e são integradas entre si, e associadas a procedimentos para melhor assegurar a proteção do patrimônio humano e material.

Apesar de toda essa tecnologia, em condomínios tem-se muita dificuldade em se fazer segurança, devido aos grandes números de pessoas que circulam neste ambiente.

Um sistema muito utilizado é o controle de acesso, que tem como finalidade gerenciar, restringir e permitir o acesso de pessoas ao hall de entrada de um condomínio, o qual está equipado normalmente por um sistema de clausura (intertravamento de duas portas, ou seja, uma só é liberada após o fechamento da outra). O problema destas controladoras é que a grande maioria falha no quesito segurança, não possuindo um sistema de alarme, ou automação de clausura, que é feita através de reles instalados separadamente.

No mercado atual existem várias marcas e modelos de equipamentos deste tipo, com características diferentes. Um exemplo é a da marca Paradox que integra à sua central de alarme um sistema de controle de acesso, porém, não faz o controle da clausura, necessitando de dispositivos externos, tais como relés e contactoras para fazer o intertravamento das portas, assim como possui transmissão dos eventos de abertura, fechamento, alarmes etc. O único ponto negativo do sistema Paradox é ser muito modular e ter um alto custo de implementação. Outro exemplo é o da Intelbras que por sua vez controla a clausura, mas não possui sistema de alarme e nenhuma forma de transmissão destes eventos para o monitoramento.

1.1 OBJETIVO GERAL

O presente projeto propõe uma integração das principais características citadas, destes dois sistemas (Paradox e Intelbras), dando origem a um protótipo onde integre em único um sistema, controle de acesso, alarme, controle de clausura e tenha saídas onde possa ser acoplado um módulo transmissor de eventos.

Também contará, com duas *interfaces* para usuários, que serão utilizados para liberar as portas e desativar o alarme automaticamente, usando *launchpads* ARM. O sistema deve controlar uma clausura, verificar acessos de pessoas autorizadas assim como bloquear as não. Caso haja intrusão, deverá gerar disparos, transmitindo esses eventos para um software de monitoramento.

1.2 OBJETIVOS ESPECÍFICOS

Para que os objetivos gerais sejam atingidos, é necessário que se cumpram os seguintes objetivos específicos:

- instalar dois sensores magnéticos nas portas, para que detectem as suas aberturas, fazendo o sistema disparar em caso de arrombamento e não fechamento;

- desenvolver uma entrada para ligação dos sensores magnéticos, que serão utilizados para rearmar o sistema, quando a porta específica fechar;
- desenvolver uma entrada, onde serão ligados os sensores de movimento, fazendo com que o sistema dispare caso haja detecção;
- projetar duas saídas normalmente aberta (NA) e normalmente fechada (NF), para acionamento das fechaduras;
- projetar duas entradas para as comunicações com as *interfaces* dos usuários, onde as mesmas serão ligadas;
- projetar duas entradas que irão intertravar as portas da clausura;
- projetar uma entrada para ligação de um sensor de incêndio, que fará a liberação das portas para evacuação caso o local pegue fogo;
- fazer uma saída para sirene;
- fazer uma entrada para liberação da primeira porta através do interfone e botoeira;
- dimensionar uma saída 12V para ligações de sensores de presença;
- projetar três saídas para ligar o transmissor de eventos, e acioná-lo quando houver: disparo de alarme, alarme porta aberta e disparos de incêndio;
- elaborar duas *interfaces* para os usuários, com avisos sonoros, para rejeição e aceitação de *tag* ou senha, assim como sinalização de *led* vermelho para ativação e verde para desativação;
- desenvolver um *firmware* que gerencie todas as funções da placa, conforme mencionado, e um menu de ajustes, feito através da saída UART da *launchpad*, que possibilite a inclusão ou exclusão de *tag* ou senha, assim como ajustes nos tempos de disparo da sirene, porta deixada aberta e acionamento das fechaduras;

1.3 JUSTIFICATIVAS

Na maioria dos condomínios, o local mais vulnerável é o *hall* de entrada, pois os moradores na maioria das vezes esquecem de fechar portas, ativar o alarme e perdem suas chaves, porque não possuem sistemas que automatizem estas funções, colocando todos os moradores em risco.

No mercado mundial existe somente uma única marca (Paradox), que é capaz de gerenciar estes quesitos de forma autônoma, sem precisar da ação humana, mas por possuir um custo elevado e por ser um equipamento importado, raramente são utilizados. No Brasil, não

existe nenhum equipamento de controle de acesso que tenha estas características reunidas em um só *hardware*. Então para conseguir este nível de funcionalidade, as empresas interligam entre si, dispositivos de várias marcas com características e funções diferentes, visando obter o nível de automação e segurança desejada, o qual raramente é alcançado, pois não são projetados especificamente para esta aplicação.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo são apresentados os conceitos necessários para o desenvolvimento do protótipo, bem como explicações técnicas sobre alguns dispositivos utilizados.

2.1 SEGURANÇA

Segurança é um conjunto de medidas assumidas para se proteger de quaisquer atos de violência, como ataques, roubos, espionagens, sabotagem e etc.

Por outro lado, dizer que alguém ou algo estariam seguros, equivale a dizer, que estariam garantidos contra tudo, o que em tese possa a eles se opor. Infelizmente não à garantia absoluta, portanto não à segurança absoluta. A segurança é uma situação, um estado, qualidade ou condição caracterizado pelo afastamento de risco ou perigo. Não havendo garantia absoluta, o conceito segurança será sempre relativo, resultando no confronto entre ricos prováveis e garantias possíveis [...]” (PORTELLA, 2012, pg.37).

A segurança hoje é dividida em dois setores, Público e Privado.

2.1.1 Segurança Pública

A segurança pública busca, acima de tudo, a manutenção da ordem, a tranquilidade, o respeito às leis e aos costumes, que ajudam a manter adequada à convivência em uma sociedade, com a total preservação dos direitos de seus cidadãos. (SOUZA, 2015)

Em outras palavras é a “atividade exercida para a preservação da ordem, da incolumidade de pessoas e do patrimônio, através dos órgãos estatais dela incumbidos” (CAPUT do Art. 144, da constituição federal, pg.62).

Segundo Tácito (2003, p.107) em uma sociedade em que se exerce democracia plena, a segurança pública garante proteção dos direitos individuais e assegura o pleno exercício da cidadania. Neste sentido, a segurança não se contrapõe à liberdade e é condição para seu exercício. Quanto mais improvável a disfunção da ordem jurídica, maior é o sentimento de segurança entre os cidadãos. (TÁCITO, 2003, p.107)

Segundo o anuário de segurança pública, nos últimos dois anos o Estado do Rio Grande do Sul, atingiu os piores índices de violência, em sua história contemporânea, e Porto Alegre, ingressou no Ranking das 50 capitais mais violentas do mundo, mesmo assim é o sétimo estado menos violento do país. (SECRETARIA DE SEGURANÇA, 2018).

A Tabela 1, demonstra um comparativo dos principais índices de crimes e delitos entre 2016 e 2017, no Rio grande do Sul.

Tabela 1 - Comparação dos principais índices de criminalidade no Rio Grande do Sul

Tipo	Registros em 2016	Registros em 2017	% diminuição
Latrocínio	168	124	- 26 %
Homicídios dolosos	2.646	2.865	8,2 %
Roubo de veículo	19.560	16.893	- 13,6%
Furto	161.155	144.192	- 10,52%
Roubo	88.569	87.170	- 1,57%
Estelionato	17.952	17.580	- 2,07%
Delitos com armas de fogo	7.818	6.868	- 12,15%
Prisões por tráfico de drogas	8.850	9.215	4%
Total de delitos	306.718	284.907	- 7,11%

Fonte: SSP/RS - PROCERGS/SIP (2018).

O gasto em segurança publica pelo estado foi de aproximadamente 3,8 bilhões, que mostra um crescimento de 3,7 % no período de 2014 a 2018 (SECRETARIA DE SEGURANÇA, 2018).

Para 2018, temos uma perspectiva de diminuição da maioria dos índices conforme Tabela 2.

Tabela 2 - Perspectiva para 2018

Tipo	Registros em 2017	Previsão para 2018	% diminuição
Latrocínio	124	99	- 20%
Homicídios dolosos	2.865	2.359	- 17,6%
Roubo de veículo	16.893	16.097	0%
Furto	144.192	136.597	- 5,36%
Roubo	87.170	74.134	- 15%
Estelionato	17.580	19.606	11%
Delitos com armas de fogo	6.868	6.601	- 3,88%
Prisões por tráfico de drogas	9.215	11.473	24%
Total de delitos	284.907	266.966	- 6,29%

Fonte: SSP/RS - PROCERGS/SIP (2018).

Analisando a Tabela 1 e 2 nota-se uma redução na maioria dos delitos. A média foi realizada com dados de janeiro a agosto de 2018, e feita uma estimativa para os meses

subsequentes, porém como estamos em período de eleições, a previsão é um aumento na violência em todos os índices analisados (SECRETARIA DE SEGURANÇA, 2018).

2.1.2 Segurança Privada

Segurança privada é definida como sendo a atividade de proteção de pessoas, áreas ou bens, executadas por empresas privadas, autorizadas pelo Departamento de Polícia Federal, nos termos da legislação em vigor, com a finalidade de garantir a incolumidade física das pessoas e a integridade do patrimônio.

De acordo com a Polícia Federal “as atividades da segurança privada são consideradas complementares as atividades de segurança pública nos termos da legislação específica.” (PORTARIA DA POLICIA FEDERAL Nº 3.233, 2012, Art. 1).

A atividade de segurança privada não substitui nem concorre com a Segurança Pública, apenas à complementa, atuando onde a pública não possa operar normalmente e apresente deficiência, ou quando sua ação não seja conveniente. (MANDARINI, 2005).

Atividades desenvolvidas pelas empresas de segurança privada tem como objetivo, a prestação de serviços, com a finalidade de proceder à vigilância patrimonial das instituições financeiras e de outros estabelecimentos públicos ou privados, bem como a segurança de pessoas físicas, realizar os transportes de valores, ou garantir o transporte de qualquer tipo de carga. (LEI Nº 7.102, 1983, Art. 10)

2.1.2.1 Atuação da Segurança Privada

Segundo a Portaria (3.233/2012) diz que a atuação das empresas deve respeitar as seguintes notas:

- as atividades de segurança privada têm caráter preventivo e complementar da segurança pública;
- o foco da segurança privada não é descobrir, prender e punir transgressores da lei e sim propiciar uma segurança preventiva;
- a atuação da segurança privada busca regular comportamentos e circunstâncias de modo a evitar ou minimizar as possibilidades de ocorrência criminal, prática conhecida no universo da segurança privada como “Medidas Preventivas”;
- a visão preventiva é claramente expressa na corrente criminológica que, orienta o trabalho da segurança, a “criminologia da prevenção situacional”, que preconiza

a prevenção, a partir da inacessibilidade dos alvos cobiçados pelos delinquentes potenciais;

- a preocupação da segurança não é somente a de repetir ou prevenir ações criminais, mas também perdas e danos decorrentes de sinistros, comportamentos antissociais, sabotagens e outros infortúnios;

2.1.2.2 Atividades da Segurança Privada

A portaria (3.233/2012) diz que a atividade de Segurança Privada se divide em 4 tipos:

Vigilância Patrimonial: é a atividade exercida em eventos sociais e dentro de estabelecimentos, urbanos ou rurais, públicos ou privados, com finalidade de garantir a incolumidade física das pessoas e a integridade do patrimônio.

Transporte de Valores: é a atividade de transporte numerário, bens ou valores, mediante a utilização de veículos, comuns ou especiais (carro forte).

Escolta Armada: é a atividade de transporte de qualquer tipo de carga ou de valor em rodovias ou estradas.

Segurança Pessoal: é a atividade de vigilância exercida com finalidade de garantir a incolumidade física das pessoas.

2.1.3 Segurança Física

“Quando se fala em Segurança Física significa falar em atos, em medidas de segurança, em procedimentos, em elementos de proteção, em técnicas e artefatos para livrar algo ou alguém de riscos ou perigos” (PORTELLA, 2012, pg.37).

Segundo Portella (2012), todo o pensamento visando proteger um determinado local, é fazer um plano de Segurança Física, que tem como objetivo:

- proteger eficazmente a propriedade, o pessoal, os processos e usuários contra todo o tipo de risco.
- resguardar o estabelecimento contra ações ou incidentes que possam ameaçar, impedir, danificar ou destruir suprimentos, processos, produção ou serviços.
- salvaguardar o investimento dos proprietários, as oportunidades de trabalho dos empregados e a incolumidade dos usuários

- evitar comprometimento, mau uso, dano ou destruição de documentos, processos e materiais essenciais e sensíveis.

“A proteção interna de uma instalação é responsabilidade da direção do estabelecimento, enquanto a externa deve ser formal e materialmente fornecida pelo Estado” (PORTELLA, 2012, pg. 46).

Segurança Física é um termo usado para abranger todos os sistemas de proteção, dispositivos, atividades, técnicas e aplicações que possam ser úteis na proteção de pessoal.

2.1.3.1 Corrente de Proteção da Segurança Física e seus Elementos e sistemas

Os elementos de proteção (os elos da corrente) são normalmente agrupados, para fins didáticos, em conjuntos sistêmicos em função de suas afinidades correlações e capacidade de complementação mutua, com emprego bastante definido em termos de sua capacidade de detecção, retardo, controle reposta e reforço. Esses sistemas funcionam em conjunto, se suprimindo e complementando (PORTELLA, 2012, pg. 46).

Segundo Portella (2012), são os seguintes os sistemas de proteção:

- *sistema de proteção de perímetro*: são equipamentos que protegem a área externa de uma empresa contra invasores. Seus elementos são barreiras perimétricas, bem como iluminação de proteção, aplicadas para ação psicológica e de retardo.
- *sistemas de sensores*: são sistemas que protegem áreas restritas, tanto salas como perímetro.
- *sistema de guarda e vigilância*: envolvem pessoas, são os vigilantes, que patrulham o local.
- *sistema de identificação de controle de acesso*: controlam a entrada de saída de pessoas em uma área restrita.
- *sistemas de blindagem*: usados para reforço de estruturas físicas, como paredes gradeadas, clausuras ou vidros à prova de bala.

2.1.3.1 Risco de Segurança

Risco de segurança é um termo utilizado que significa perigo potencial ou possibilidade de perigo. O termo risco também pode ser conceituado como evento capaz de produzir perdas reais.

Mas os riscos podem ser prevenidos através de 3 conceitos como diz Portella (2012):

- *Prevenção primária*: são orientações para as causas dos riscos, objetivando neutralizá-los antes que se manifestem, resolvendo situações perigosas.
- *Prevenção Secundária*: tem seus programas orientados para quando e onde o risco passa manifestar-se ou tornar-se concreto.
- *Prevenção Terciária*: tem seus programas orientados para aquele que protagonizam situações de risco. Exemplo: que não fecham uma janela ao deixar uma janela aberta.

2.1.3.2 Níveis de Segurança Física

Segundo Portella (2012), os níveis de segurança física são definidos em ordem crescente, pelo grau de proteção necessário e recursos disponibilizados conforme Quadro 1.

Segurança mínima (nível 1): consiste em simples barreiras físicas, tais como, portas e janelas, equipados com fechaduras e cadeados simples.

Segurança baixa (nível 2): incorporar sistema de detecção contra intrusão, sinalizando alarme discreto em local onde, na maior parte do dia permaneçam pessoas. Também deve-se iluminar convencionalmente os pontos à frente das portas de acesso externo e os periféricos mais acessíveis ou atraentes para roubo. Deve-se estabelecer barreiras físicas mais resistentes que as convencionais (grades, farpados, portas com trancas, bloqueio a acesso à forros) e utilizar fechaduras mais sofisticadas.

Segurança média (nível 3): sistema projetado para impedir, detectar e avaliar a maior parte das atividades externas, ou seja, as medidas de segurança de nível 2 são acrescidas de dispositivos com possibilidade de detecção e avaliação.

Segurança alta (nível 4): impedir, detectar e avaliar o máximo possível, atividades internas e externas não autorizadas, com sistema de câmeras, alarme monitorado e controle de acesso.

Segurança máxima (nível 5): Sistema projetado para impedir, detectar, avaliar e neutralizar toda e qualquer atividade interna e externa não autorizada, com sistemas redundantes.

Quadro 1 - Níveis de segurança física.

Nível 1	Fechamentos de portas de janelas; Fechamento de portões; Cercas e cancelas;
	Acesso (área livre);

Nível 2	Iluminação simples; Alarmes;
Nível 3	Alambrado; Iluminação de proteção; Sistema de comunicação; Vigilância desarmada; Cães guarda; Controle de acesso; Sistema de circuito fechado de televisão
Nível 4	Vigilância armada; Coordenação com órgãos de segurança elétrica; Sistemas auxiliares de comunicação; Sistema de controle de acesso sofisticado; Sistema auxiliar de energia; Sistema de detecção de alarmes;
Nível 5	Alarmes sofisticados; Força armada reativa;

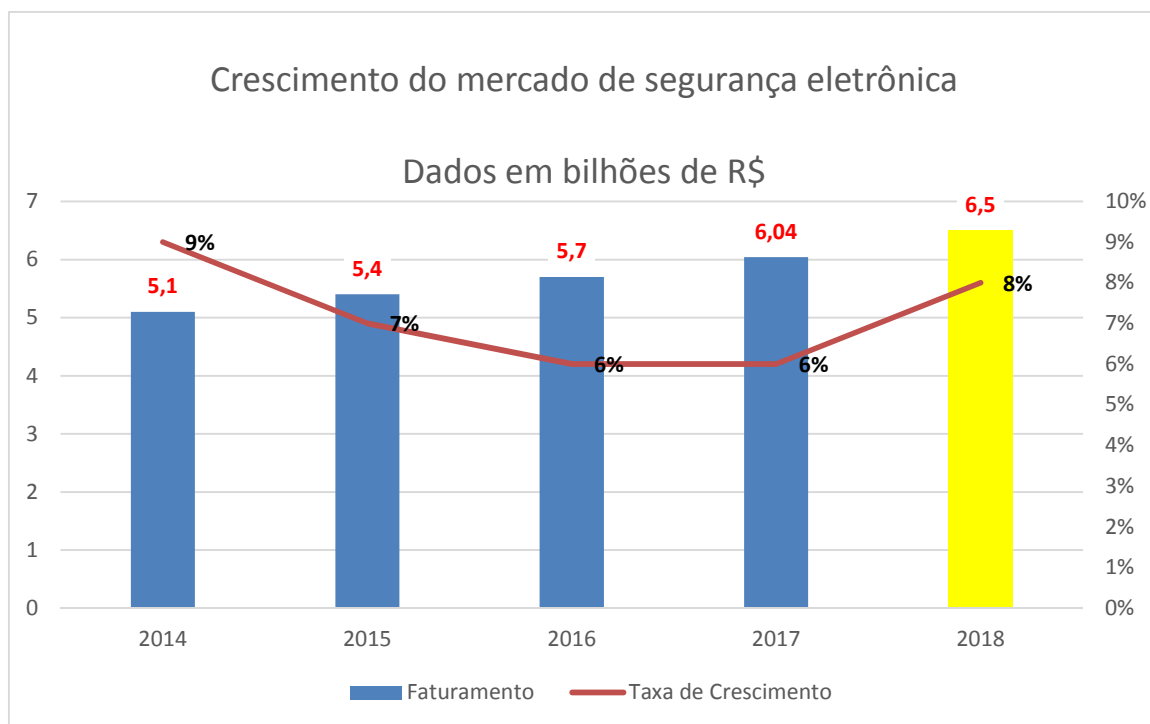
Adaptado: (PORTELLA, 2003, pg. 23)

2.1.4 Segurança Eletrônica

É o serviço que complementa os setores de segurança pública e privada, permite através da tecnologia detectar intrusões, arrombamento, incêndios e outras irregularidades sofridas no local protegido. O setor de Segurança Eletrônica é o que mais cresce anualmente, pois consegue aliar a sua tecnologia para desenvolver os demais setores.

Selma Migliori, presidente da ABESE (Associação Brasileira de Segurança Eletrônica), diz que o setor de segurança eletrônica tem expectativas positivas para o mercado brasileiro em 2018, que projeta crescimento de 8% neste ano. O faturamento do setor em 2017 foi de R\$ 6 bilhões, como mostra o Gráfico 1 (REVISTA SEGURANÇA ELETRÔNICA, 2018,pg. 15).

Gráfico 1 - Projeção de Crescimento do Setor de Segurança Eletrônica.



Adaptado: (REVISTA SEGURANÇA ELETRÔNICA, 2018,pg. 15)

Este setor é constituído por profissionais capacitados na área elétrica ou eletrônica, que executam os projetos de Segurança (alarmes, CFTV, incêndio, etc.), desenvolvidos por empresas ou entidades de segurança.

2.1.4.1 Objetivos da Segurança Eletrônica

Segundo a revista Sevesp (2013), os objetivos de sistemas de segurança eletrônica são:

- detectar presenças não autorizadas, automaticamente, sempre que o sistema de alarme estiver ativo;
- comunicar ocorrências, por meio de aviso sonoro, através do acionamento de sirenes, e silenciosamente por meio de envio de sinais à central de monitoramento remota;
- tratar ocorrências, informando irregularidades aos responsáveis, para que sejam adotadas as devidas providências;
- inibir ocorrências de invasão, depredação ou ameaças, mostrando à comunidade em geral que a área está protegida;

O monitoramento remoto de alarmes e imagens se destina à detecção e tratamento de eventos intrusão, com o consequente acionamento das autoridades competentes.

2.1.5 Segurança em Condomínios

Condomínios são conjuntos habitacionais onde várias famílias residem, e exercem direitos sobre o mesmo bem. Para projetarmos um sistema de segurança eletrônica nestes locais é preciso entender a rotina do condomínio, quantas pessoas o habitam, horários de acessos e seus pontos vulneráveis.

Um fator importante a ser analisado é a proteção do *hall* de entrada, este deve ser protegido por clausura, e com controladoras de acesso em cada porta, para libera-las de forma ágil e fácil.

No perímetro do local devem ser instaladas câmeras de segurança e suas imagens visualizadas pelos moradores, vigilantes e empresas de monitoramento.

Por fim, a segurança em condomínios utiliza também o potencial humano para resguarda-lo, tendo a segurança eletrônica como uma ferramenta de suporte.

2.2 SISTEMA DE ALARME

Desde as épocas mais remotas, a humanidade conhece e utiliza sinais em condições de alarme, num passado distante, o sino, a flecha, a trombeta, a fumaça e outros sinais anunciavam as situações perigosas (ARAÚJO, 2007).

Os alarmes em segurança privada e pública é um sistema de sensores que se limita a detecção, localização e denuncia de presenças e situações indesejáveis através alertas sonoros ou transmissão de eventos a uma empresa de monitoramento. O funcionamento eficaz do sistema requer o pronto comparecimento de pessoal bem treinado e adequadamente equipado. Sem essa pronta resposta tem somente impedimento psicológico (PORTELLA, 2012, p. 108).

Muito se fala de alarme, e alguns até confundem a denominação com a aplicação, porém é de suma importância que se defina a função da tecnologia instalada e a leitura do ambiente mediante a certas condições estáveis, com a posterior transmissão das variações detectadas (ARAÚJO, 2007, pág. 91).

As condições que justificam o sistema de alarme no setor de Segurança, segundo Portella (2012), devem conter as seguintes características:

- áreas que necessitem de controle ou processo crítico;

- locais ou pontos vitais que constituam alvos muito atraentes;
- áreas em que as condições criem vulnerabilidade incomum;
- áreas altamente restritas em que não se queira presença de guardas;
- áreas ou pontos nos quais não se deseja a presença de elementos metálicos;

2.2.1 Sensores para alarmes

Sensor é um dispositivo que tem a função de detectar e responder com eficiência a algum estímulo. Depois que o sensor recebe o estímulo, a sua função é emitir um sinal que seja capaz de ser convertido ou interpretado por outros dispositivos.

Segundo Portella (2012) o sensor em sistema de alarme é limitado a detecção, localização e denuncia de presenças ou situações indesejáveis.

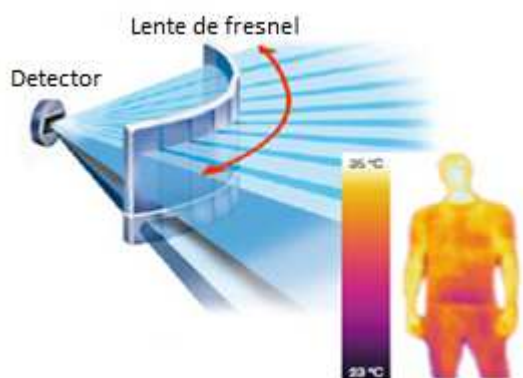
2.2.1.1 Sensor Infravermelho

IR – sensor infravermelho

Os sensores IR, são projetados para detecção de movimento através da mudança de radiação térmica provocado pelos corpos, como mostra a Figura 1 (CESP LEÃO XIII, 2014).

Os componentes básicos que forma este sensor são um detector de luz infravermelha, uma lente chamada Fresnel e um circuito eletrônico. O sensor não emite sinais somente detecta a movimentação de uma luz infravermelha dentro de uma determinada área conforme mostra a Figura 1 (CESP LEÃO XIII, 2014).

Figura 1 - Detecção Sensor Infravermelho

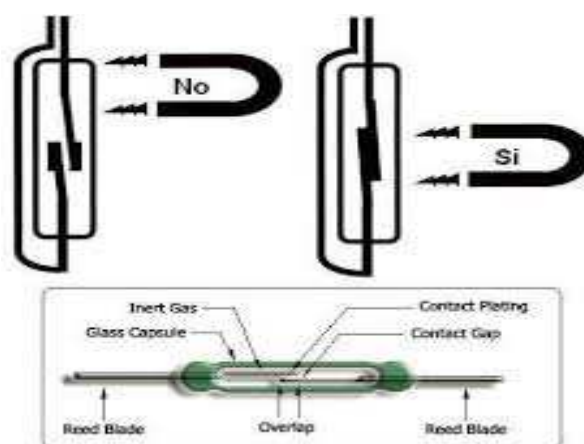


2.2.1.2 Sensor Magnético

Os sensores magnéticos são acionados a partir de um campo magnético geralmente proveniente de um ímã permanente ou de uma bobina. Eles funcionam basicamente como uma chave liga/desliga (CESP LEÃO XIII, 2014).

O sensor magnético é composto por duas lâminas de material ferromagnético, cada uma ligada a um terminal, envoltas por uma ampola de vidro de alta resistividade. A ampola é vedada e dentro dela existe algum gás inerte para impedir a oxidação. Na Figura 2, está representada a estrutura do sensor (CESP LEÃO XIII, 2014, pg.11).

Figura 2- Esquema sensor Magnético.



Fonte: <http://cerev.info/addzthis-interruptor-magnetico.html> (15/10/2017, 14:02)

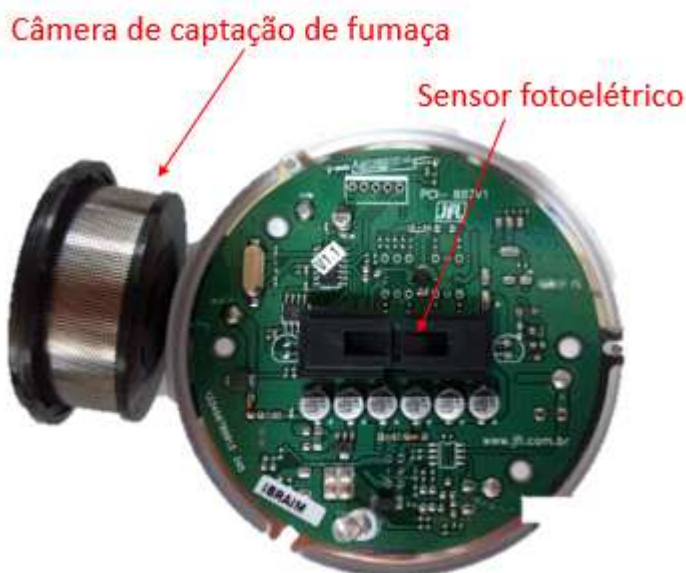
Quando um campo magnético se aproxima do sensor, surge uma força magnética de atração entre as lâminas fazendo com que elas se toquem. Dessa forma os terminais do sensor entram em curto, possibilitando a passagem de uma corrente (CESP LEÃO XIII, 2014).

2.2.1.3 Sensor para detecção de fumaça

A finalidade deste sensor é detectar fumaça emitida através da combustão de algum material, no ambiente protegido. Alguns modelos também detectam o aumento rápido da temperatura. Ele utiliza um sensor fotoelétrico que transforma a luz em eletricidade.

Na ausência de fumaça o feixe sempre segue em linha reta até o sensor. Quando à presença de fumaça a mesma desvia o feixe de luz em 90 graus e o sensor deixa de ficar acionado disparando o alarme, conforme mostra a Figura 3 (CESP LEÃO XIII, 2014).

Figura 3 - Sensor de fumaça.



Fonte: Próprio autor

2.3 CONTROLE DE ACESSO

Controle de acesso é qualquer aplicação usando equipamentos com objetivo de administrar o acesso físico de pessoas, veículos e materiais a um determinado perímetro de segurança ou área delimitada.

O controle de acesso envolve o uso de chaves, trancas, vigilantes, crachás, cercas, sistemas de bloqueio, etc. Além da aplicação de normas e procedimentos utilizados pela organização para operacionalizar o sistema.

A principal função de um controle de acesso físico, é o de gerar um ambiente seguro e livre de acessos não autorizados. Um bom sistema de controle de acesso, deve ser capaz de assegurar a entrada fácil e simplificada das pessoas devidamente autorizadas e impedir o acesso das não.

2.3.1 Atribuição e funções do controle de acesso:

O sistema de controle de acesso tem principais funções e atribuições conforme listado abaixo:

- delimitar e identificar uma área onde o acesso é restrito;
- impedir acesso não autorizado;
- identificar e checar a permissão de acesso;
- liberar o acesso autorizado;
- identificar, alarmar as tentativas de acesso não autorizado;

2.3.2 Sistemas de Controle de Acesso Paradox

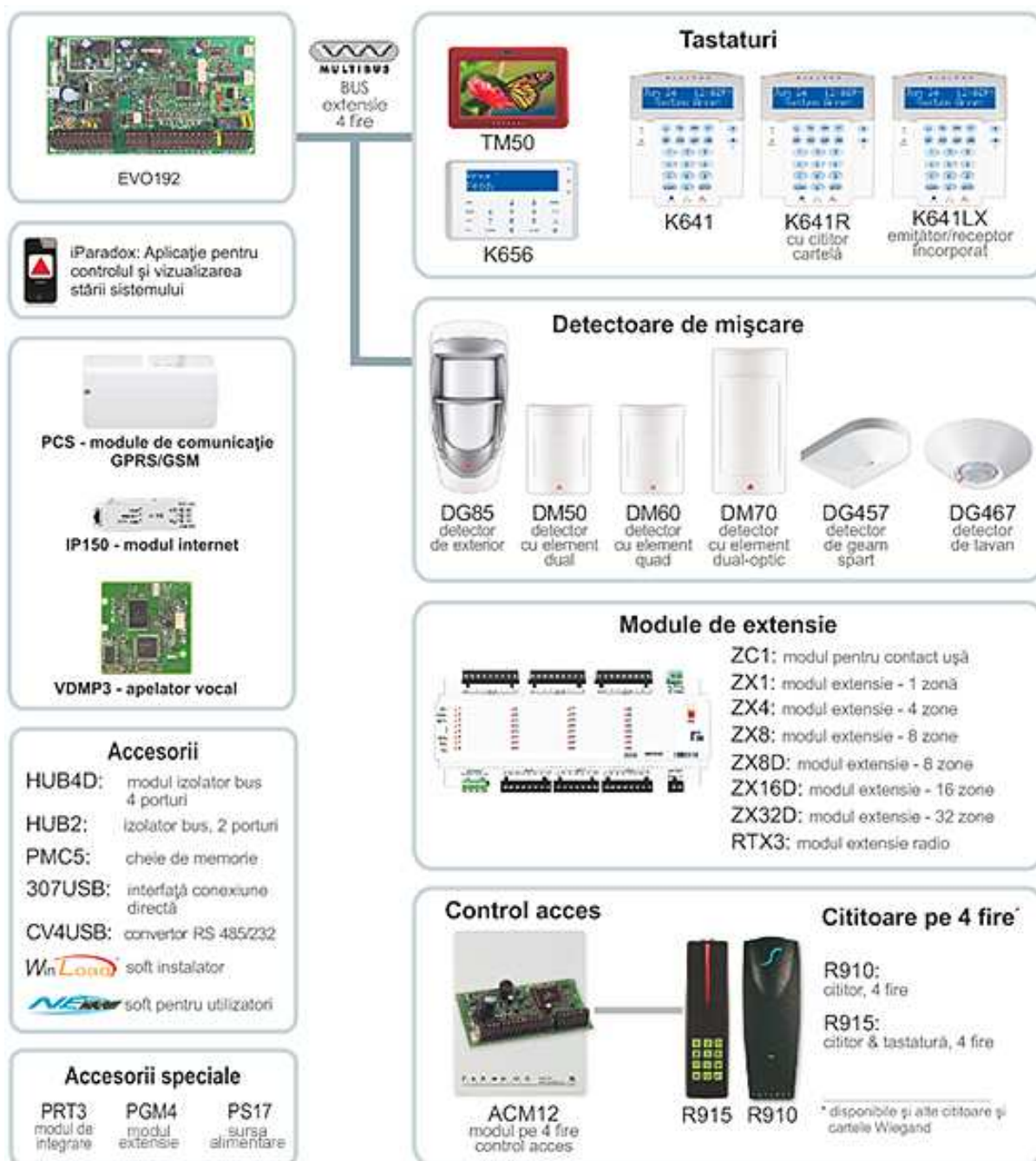
Este sistema é um dos mais completos do mercado usado para proteção de condomínios, ele possui uma poderosa central de alarme que aceita 999 usuários que possibilita o uso de *tag* ou senha e 192 zonas utilizadas para a ligação de sensores.

Sua arquitetura compreende também 15 controladoras de acesso com dois leitores de *tag* cada uma, e transmite todos os eventos gerados. Também é um equipamento modular, o que facilita a manutenção. Seus dispositivos utilizam uma tecnologia, de endereçamento serial, cuja comunicação central-dispositivo é feita através de 4 fios e todos os dispositivos se comunicam com a central usando este barramento.

Seu portfólio também conta com módulos de transmissão de eventos que utiliza Internet e GPRS, e permitem interação remota com o sistema para alteração da programação, ou para visualização do *status* de arme e desarme, que pode ser feita através de aplicativo celular, ou do seu *software* próprio.

A Figura 4, mostra o esquema do sistema de alarme com controle de acesso Paradox.

Figura 4 - Central Paradox Evo e seus componentes.



Fonte: <http://www.paradox.com/Products/default.asp?CATID=7&SUBCATID=68&PRD=158> (15/10/18, 14:27)

2.3.3 Sistemas de Controle de Acesso Intelbras

São sistemas muito simples conforme Figura 5, onde o teclado é a própria controladora, e isso torna o sistema vulnerável, pois se removido as fechaduras se abrem. Ele também funciona com *tag* ou senha, possui um sensor para monitorar caso a porta for deixada aberta. Por ser simples é um sistema barato, mas totalmente inseguro e não possui um sistema de alarme embarcado como o da paradox.

Figura 5- Controladora de acesso Intelbras.



Fonte: <http://www.intelbras.com.br/empresarial/controle-de-acesso/linha-corporativa/controle-de-acesso-stand-alone/sem-software> (15/10/18,14:32)

2.4 CLAUSURA

Clausuras, do ponto de vista da segurança, é um espaço fechado, onde possui portas de entrada e saída, que se abrem de forma alternada sendo controlada por um sistema ou operador, ao qual restringe o acesso a um local específico, caso o usuário não seja autorizado. Elas são usadas para proteger os visitantes, retirando-os da rua e confinando em seu interior.

Após a pessoa entrar, é feita a identificação e a checagem da autorização de acesso, estando aprovada, a porta de entrada é aberta permitindo que a pessoa entre no local.

Se tratando de uma tentativa de invasão, o indivíduo é confinado no interior da clausura, não conseguirá sair do local antes da chegada da polícia.

As clausuras podem ser utilizadas para uma finalidade específica ou um conjunto delas:

- impedir e dificultar que pessoas não autorizadas acessem o local;

- impedir o contato direto de uma pessoa com a segurança antes dela ser identificada;
- evitar a exposição do vigilante a um risco de rendição durante o processo de identificação;
- controlar o acesso através da identificação de crachá, senha ou biometria;
- controle de acesso de veículos e cargas

2.5 LEITOR DE RFID

O leitor de RFID tem a capacidade de criar um campo eletromagnético capaz de absorver as informações geradas pelas etiquetas, usadas para identificar pessoas ou objetos. O leitor é dotado de uma antena, que capta as informações da etiqueta quando ela passa sobre seu campo (CUNHA, 2006).

Os modelos mais avançados são capazes de alterar e processar os dados nelas existentes. Ao passar pela área de cobertura da antena, o *tag* é detectado pelo leitor, decodificando seus dados. Em seguida, o leitor transmite esses dados para um microcontrolador onde serão processados (BERNARDO, 2004).

No Quadro 2 mostra-se as frequências mais utilizadas e suas aplicações.

Quadro 2 - Frequências dos leitores RFID

Frequências	Aplicações
Baixa Frequência (menos que 135KHz)	• Identificação de animais • Automação industrial • Controle de acesso
Alta Frequência (UHF) (433 Mhz e 860 a 930 Mhz)	• Fornecido a cadeia de suprimento logística • Administração de estoque • Localização de itens • Controle de inventario

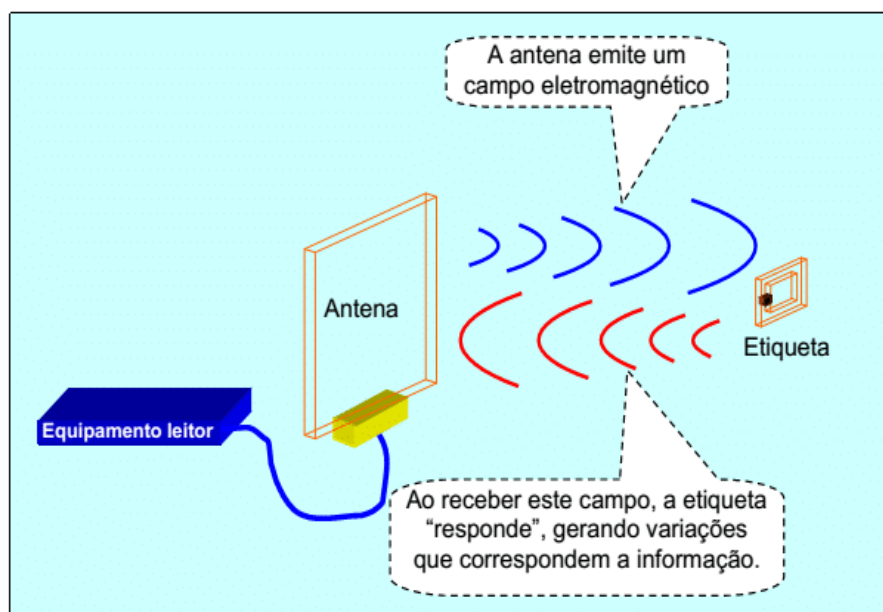
Fonte: (NETO, 2008)

2.6 TAG

Nos sistemas de identificação por radiofrequência, as *tag* devem ser consideradas como elemento principal, uma vez que contêm as informações básicas que permitem a identificação física do objeto a ser rastreado. Quando a leitora RFID recebe o sinal da etiqueta, ela retransmite imediatamente os seus dados (BERNARDO, 2004).

Basicamente o funcionamento de um *tag* é tido através da indução de campos eletromagnéticos em circuitos ressonantes. Uma antena gera um campo eletromagnético e este excita o circuito ressonante LC contido na *tag*. Esta excitação, por sua vez, gera uma corrente que alimenta o seu circuito, ele gera a resposta para o leitor e a envia pela antena. As respostas deste circuito geram alterações no campo eletromagnético, que são medidas novamente pela antena. Estas alterações contêm um sinal modulado que carrega a informação da etiqueta, conforme mostra a Figura 6.

Figura 6 - Componentes de uma etiqueta RFID.



Fonte: (BERNARDO, 2004)

A Figura 7 ilustra as múltiplas formas de *tag* que estão à disposição no mercado.

Figura 7 - Modelos de *tag* existentes.



Fonte: (BERNARDO, 2004)

Em relação às funcionalidades do *tag*, elas são estabelecidas de acordo com uma ordem de classificação, conforme Quadro 3.

Quadro 3 - Classe de tag RFID

Classe do <i>tag</i>	Descrição de funcionalidade
Classe 1:	<i>Tag</i> passivo - leitura
Classe 2:	<i>Tag</i> passivo com memória criptografada
Classe 3:	<i>Tag</i> semi-passivo com suporte de comunicação em banda larga
Classe 4:	<i>Tag</i> ativo, com capacidade de comunicação em banda larga, ponto a ponto com outras etiquetas ativas que operem na mesma frequência e com leitores
Classe 5:	O <i>tag</i> desta classe é essencialmente leitor, pois pode ter <i>tag</i> das classes 1,2 e 3, assim como se comunicar com <i>tag</i> classe 4 e qualquer outro dispositivo <i>wireless</i> .

Fonte: (NETO, 2008)

3 DESENVOLVIMENTO DO PROJETO

Neste capítulo são apresentadas as especificações do projeto, o *layout* da clausura e seu funcionamento, assim como o fluxograma do *firmware* e menu de ajustes. Também, será apresentado um diagrama de blocos do *hardware* do sistema, assim como as especificações dos componentes e cálculos necessários para seu funcionamento.

3.1 REQUISITOS DO SISTEMA

Todo o sistema eletrônico projetado para a área de segurança deve, além de ser robusto e funcional, ter sua arquitetura voltada para inibir e dificultar que seja burlado, gerenciando os riscos de segurança, sem que haja falhas. Como o projeto trata de um sistema de controle de acesso com sistema de alarme, foram levados em consideração as possíveis vulnerabilidades que o sistema enfrentará.

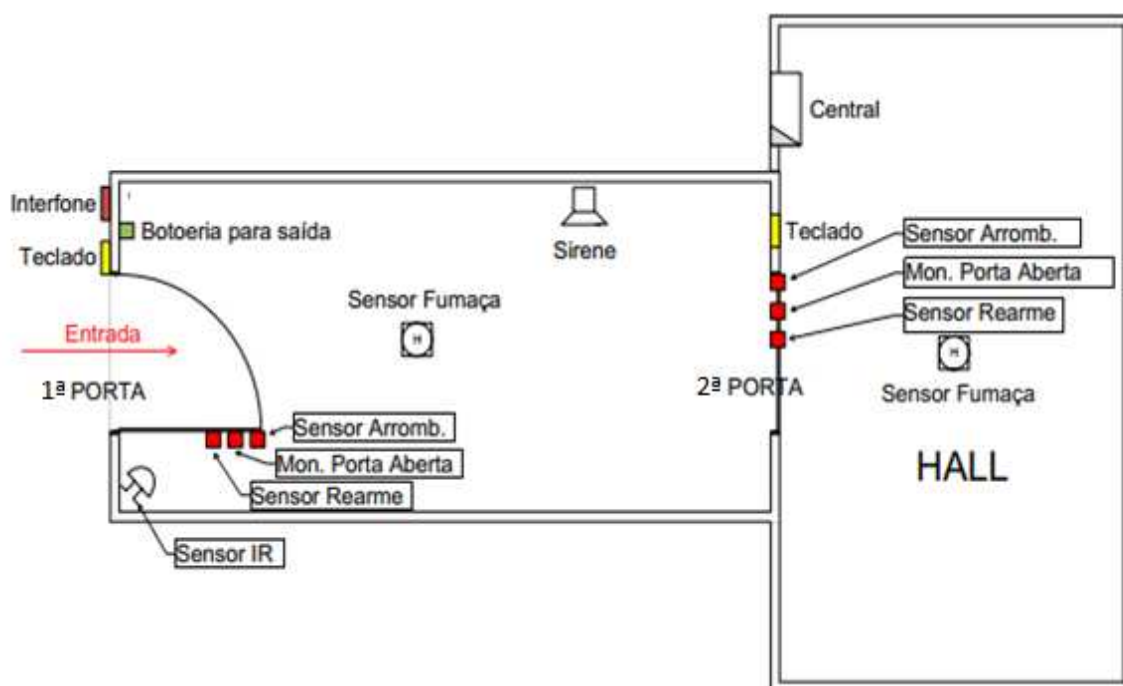
- *falta de energia elétrica*: caso a mesma falte, ou acabe sendo cortada, o sistema ainda assim vai funcionar, ficando ligado pelos menos 7 horas com auxílio de bateria, pois esta alimentação, acaba se desligando as fechaduras e abrindo as portas (caso da magnética). Se estiver utilizando uma fechadura eletromecânica, ela vai ficar trancada, impedindo que o morador entre no condomínio, podendo até ficar preso dentro da clausura ao sair.
- *tentativa de burlar o teclado leitor*: em muitos sistemas, o teclado é quem possui o comando que faz a abertura e o fechamento das portas. No caso de retirada do mesmo, a fechadura desenergiza abrindo a porta (caso da magnética), ou ficará com a fiação exposta, bastando o contato com uma fonte 12 V para liberar (caso da eletromecânica).

3.2 PROJETO DE SEGURANÇA DA CLAUSURA

A clausura, como mostra a Figura 8, tem duas portas intertravadas ou seja (uma só abre mediante o fechamento da outra). Foi utilizado para tal, dois sensores magnéticos, instalados um em cada porta, colocando também uma fechadura em cada uma.

No seu interior foi instalado, um sensor infravermelho e um detector de fumaça, assim como a colocação de uma sirene. Também, conta com mais dois sensores magnéticos nas portas, onde um monitora a porta deixada aberta e o outro, caso a mesma seja arrombada. O sistema central poderá ser instalado em um ambiente protegido dentro do próprio condomínio.

Figura 8 - Desenho do Protótipo de uma clausura em 2D



Fonte: Próprio autor.

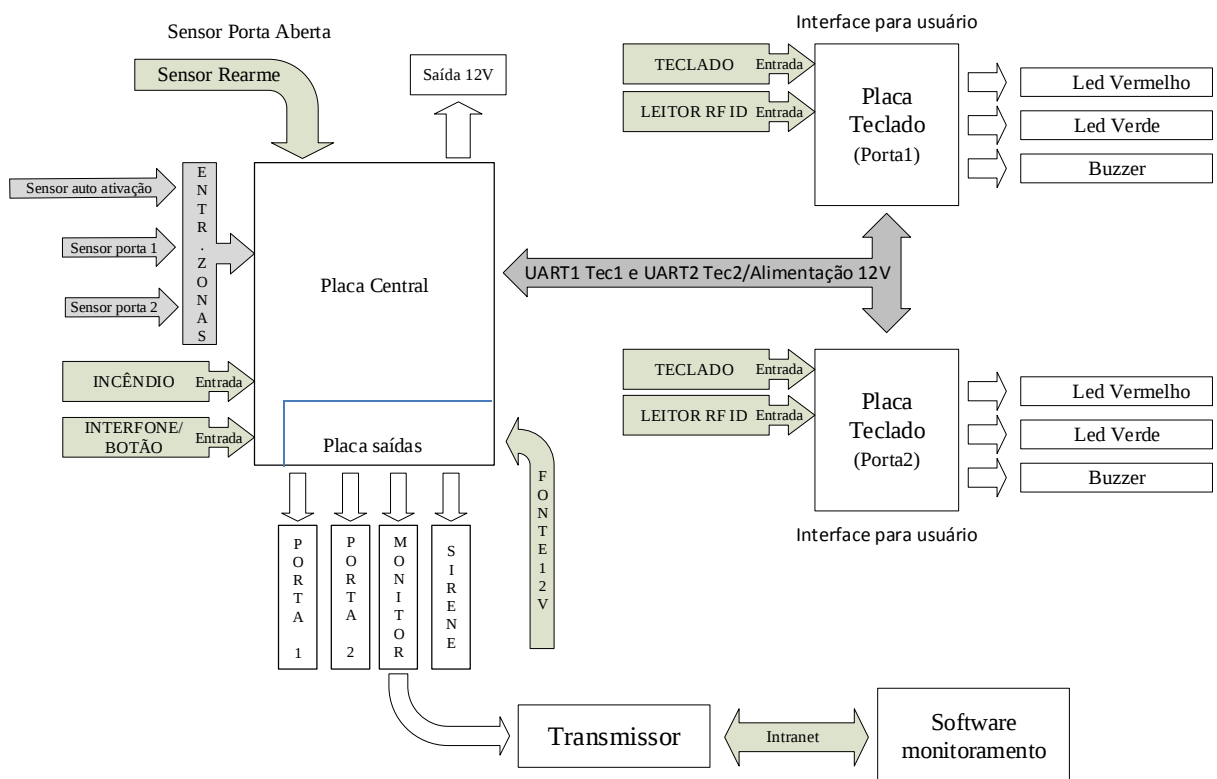
Geralmente, esses projetos contam com uma porta maciça, que protege a entrada da rua (1ª porta) e um gradil interno que protege a entrada do hall (2ª porta), para à qual, foi utilizado somente uma interface de usuário, liberando a entrada e saída. Na primeira porta, para sair, é usada uma botoeira, afim de deixar os visitantes à vontade para fazê-la sem precisar de *tag* ou senha.

Para a apresentação do protótipo foi construída uma maquete, com o objetivo de simular o funcionamento das portas e o ambiente interno de um hall do condomínio com clausura. Na Figura 9, segue o modelo com suas dimensões e na Figura 10, a maquete construída.

3.3 PROJETO ELETRÔNICO

Para o projeto eletrônico foram elaboradas 4 placas conforme o diagrama do bloco da Figura 11. A primeira, é a placa central (onde é feito o processamento, através de uma *launchpad*), a segunda, é a placa de acionamentos das saídas (composta por 6 relés) e as outras duas, são as placas das *interfaces* para os usuários (referente a 1ª porta e a 2ª porta), as quais se comunicam via protocolo UART através de duas *launchpads*.

Figura 11 - Diagrama de blocos do hardware do sistema.



Fonte: Próprio autor.

3.3.1 Placa Central

A placa central é onde está localizado o *firmware* que vai gerenciar o sistema. Ela é composta por uma *launchpad* ARM que conecta os dispositivos. Nela é onde é feito todo o processamento do protótipo, se comunicando com as *interfaces* dos usuários através de duas UARTS distintas. Ela recebe as informações oriundas destas *interfaces*, assim como envia informações para as mesmas, os quais emitem sinais de avisos para o usuário. É nela onde está

localizado o menu de ajustes, o qual, está protegido por uma senha. Ao acessá-lo pode-se cadastrar, excluir, visualizar senhas e *tags* e parametrizar os tempos de acionamento do sistema.

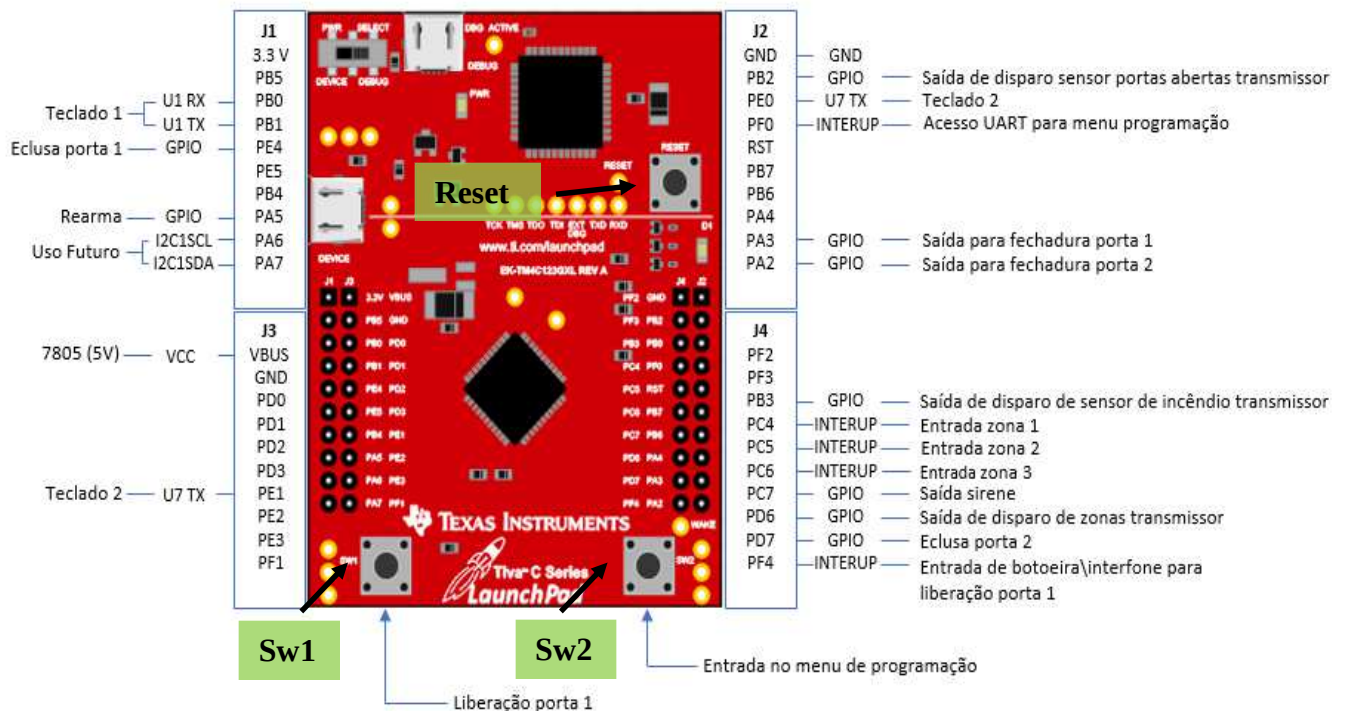
A placa central por sua vez, faz o monitoramento dos sensores *reed switch*, incêndio e infravermelho, fazendo com que saídas sejam acionadas caso o sistema de alarme esteja ativo.

A mesma é composta das seguintes entradas e saídas:

- *entradas de zonas*: composta por 2 entradas, onde foi ligado um sensor infravermelho e na segunda um sensor que vai inibir a auto ativação;
- *entrada de incêndio*: entrada exclusiva onde foi conectado o sensor de fumaça. Também poderia ter sido ligada uma central de incêndio;
- *entrada de interfone*: entrada utilizada para liberação e desativação do sistema de alarme da 1ª porta, pelo interfone ou pela botoeira, caso algum visitante chegue (liberação da porta dá-se interfone do apto) ou queira sair de dentro da clausura (dá-se pelo uso da botoeira).
- *sensor rearme*: entrada utilizada para fazer a reativação do sistema quando uma das portas fechar;
- *sensor porta aberta*: entrada que vai monitorar caso a porta correspondente for deixada aberta emitindo sinais sonoros;
- *saída 12V* – usada exclusivamente para alimentação dos sensores de segurança e outros dispositivos;
- *saída Porta 1* – usada para liberação da 1ª porta;
- *saída Porta 2* – usada para liberação da 2ª porta;
- *saídas para monitoramento* – composto por três saídas, que acionam mediante aos três eventos citados anteriormente. Nelas será ligado o transmissor;
- *sirene*: Saída onde a sirene é ligada, e vai disparar mediante a violação de um dos sensores de segurança, ou quando termine o tempo de porta aberta;
- *entrada alimentação*: onde é ligada a fonte de alimentação;
- *saída UART*– Barramento utilizado para a comunicação da placa central interfaces de usuários;

Após ter definido quais as entradas e saídas que serão necessárias para o funcionamento do protótipo, é hora de definir os pinos que serão utilizados na *launchpad*, para gerenciar os dispositivos. Na Figura 12 segue o esboço desta pinagem:

Figura 12 - Pinagem da placa central



Fonte: Próprio autor.

3.3.1.1 Sistema de Alimentação da placa

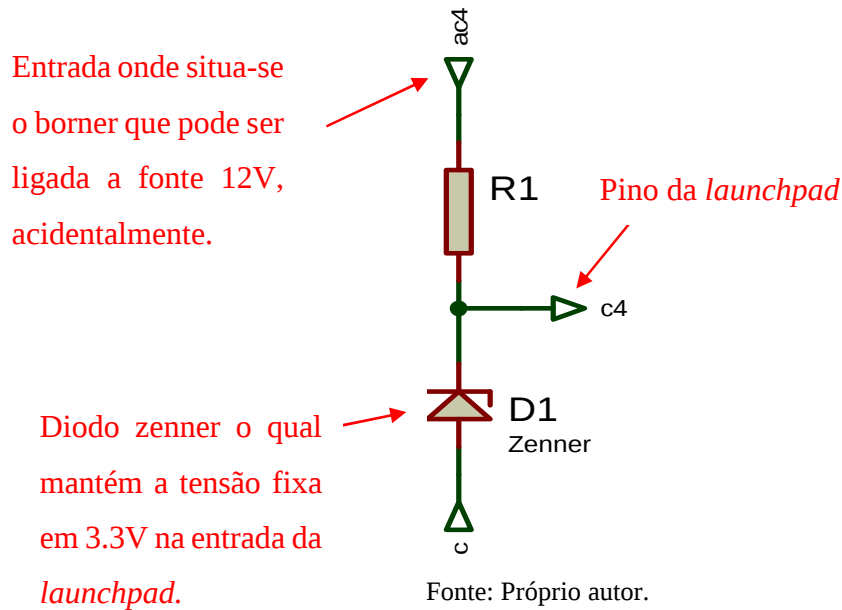
Para o funcionamento do sistema foi utilizado uma fonte de 12V, alimentando os componentes (sensores, teclados e a placa dos relés de saídas). Para a alimentação da *launchpad*, foi utilizado uma fonte de 5V separada.

3.3.1.2 Circuito para a proteção das entradas

Devido ao protótipo utilizar uma fonte 12V para alimentar os circuitos, ela pode ser ligada em qualquer umas das entradas da placa acidentalmente, queimando os componentes. Para evitar esta situação foi desenvolvido um circuito de proteção.

Quando a fonte 12V for ligada acidentalmente na entrada “ac4”, como mostra a Figura 13, sua tensão é drenada pelo zenner de 3.3V, o qual mantém este nível em cima do pino da *launchpad* “c4”, evitando a queima. No total são 8 entradas que serão protegidas pelo circuito.

Figura 13 - Circuito de proteção das entradas



O resistor deste circuito tem como função, limitar a corrente de zenner, fazendo com que o diodo não queime por “sobre corrente”, também mantendo a corrente mínima necessária para o seu funcionamento. Abaixo segue os cálculos para o dimensionamento deste circuito.

$$V_{ac4} = 13V;$$

$$I_{zenner\ max} = 0,276\ A;$$

$$I_{zenner\ min} = 0,1 \times 0,276\ A = 0,0276A$$

$$R = \frac{V_{max} - V_{zenner}}{I_{zenner}} = \quad (1)$$

$$R_{max} = \frac{13 - 3,3}{0,0276} = 360\ ohms;$$

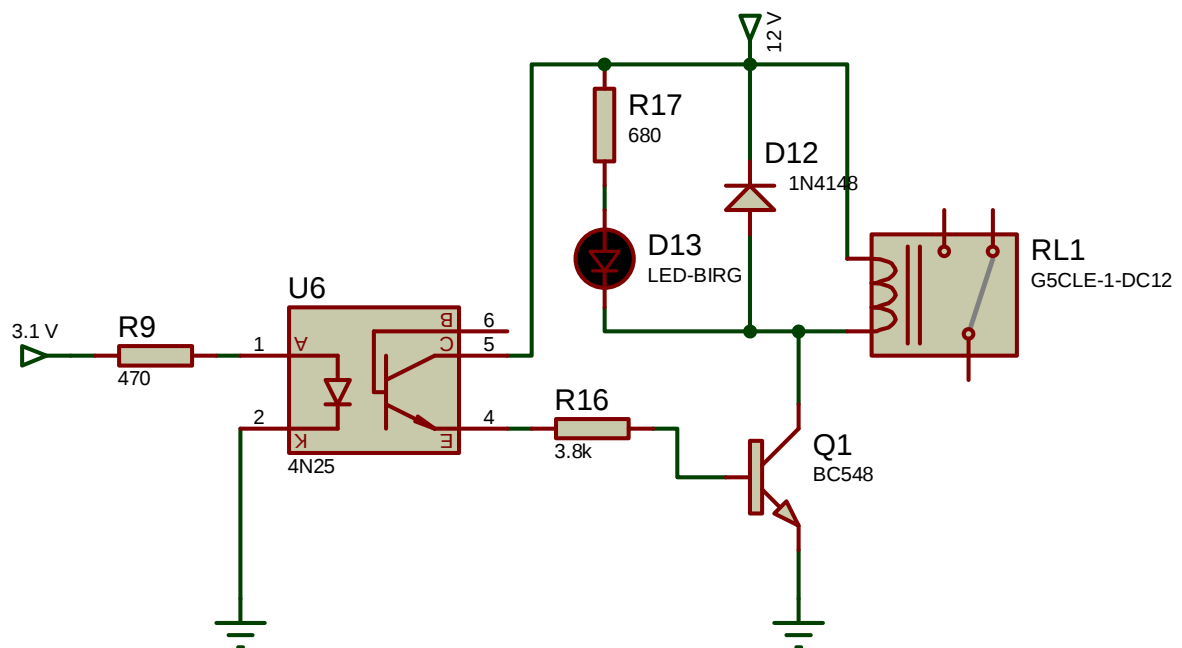
$$R_{min} = \frac{13 - 3,1}{0,276} = 35\ ohms; \text{ Resistor escolhido de } 280\ ohm;$$

O resistor escolhido, ficou entre os limiares de R_{max} e R_{min} , e seu valor é de 280 ohms.

3.3.1.3 Circuito de isolamento das saídas

O sistema possui uma placa com 6 saídas de relés, que tiveram suas entradas isoladas das saídas da *launchpad* com o auxílio de opto-acopladores 4N25, evitando assim indução ou condução reversa geradas pelas cargas instaladas. Os circuitos foram dimensionados para que a corrente nas saídas digitais não ultrapasse o limite de corrente de 25 mA. Na Figura 14 segue o esquema do circuito.

Figura 14 - Sistema de isolamento



Fonte: Próprio autor (2019).

Abaixo seguem os cálculos:

Cálculo resistor R9:

$$V = 3.3 \text{ V};$$

$$V_{4N25} = 1,5 \text{ V};$$

$$I_{4N25} = 4 \text{ mA};$$

$$R_9 = \frac{V_{micro} - V_{4N25}}{I_{4N25}} = \quad (2)$$

$$R_9 = \frac{3.3 - 1,5}{4mA} = 450 \text{ ohms}; \text{ Usado resistor comercial de } 470 \text{ ohms}$$

Para o cálculo de R16 foi considerado que o transistor está em zona de saturação, ou seja, VCE=0. Considerando o Fsat do transistor BC 548 igual a 10.

$$I_{Led} = 2ma;$$

$$I_{rele} = 30 \text{ ma};$$

$$V = 12V;$$

$$IB = \frac{IC}{Fsat} \quad (3)$$

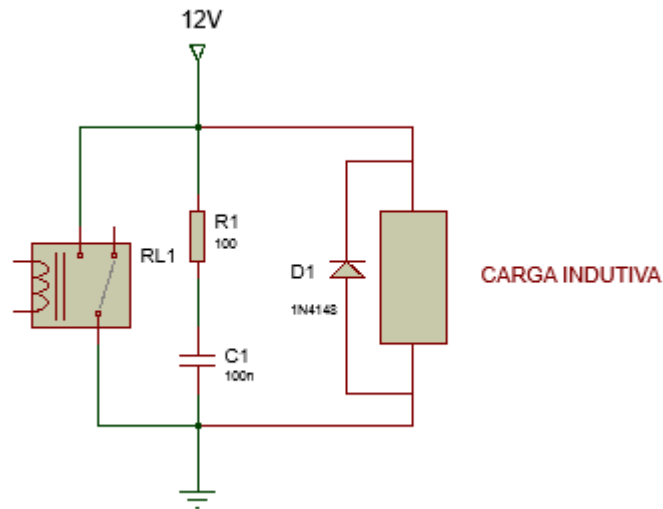
$$IB = \frac{32ma}{10} = 3,2 \text{ mA}$$

$$R_{16} = \frac{Vcc - 0,7}{Ib} \quad (4)$$

$$R_{16} = \frac{12-0,7}{3,2 \text{ mA}} = 3.531 \text{ ohms}; \text{ utilizando resistor comercial de } 3.8k;$$

Devido a indução gerada pela carga, ainda foi acrescentado ao projeto dois diodos de roda livre, fazendo com que as correntes reversas se dissipem em cima das cargas. Também foram adicionados dois filtros *Snubbers* em cima dos contatos dos relés que acionam as cargas, conforme mostra a Figura 15, evitando que os transientes provenientes da comutação destas venham a interferir no circuito. O filtro *snubber* ou RC, é composto por um resistor em serie com um capacitor, que visam eliminar este tipo de ruído.

Para o circuito foi adotado um resistor de 100 ohms e um capacitor de poliéster de 100 nF. Estes foram escolhidos após vários testes.

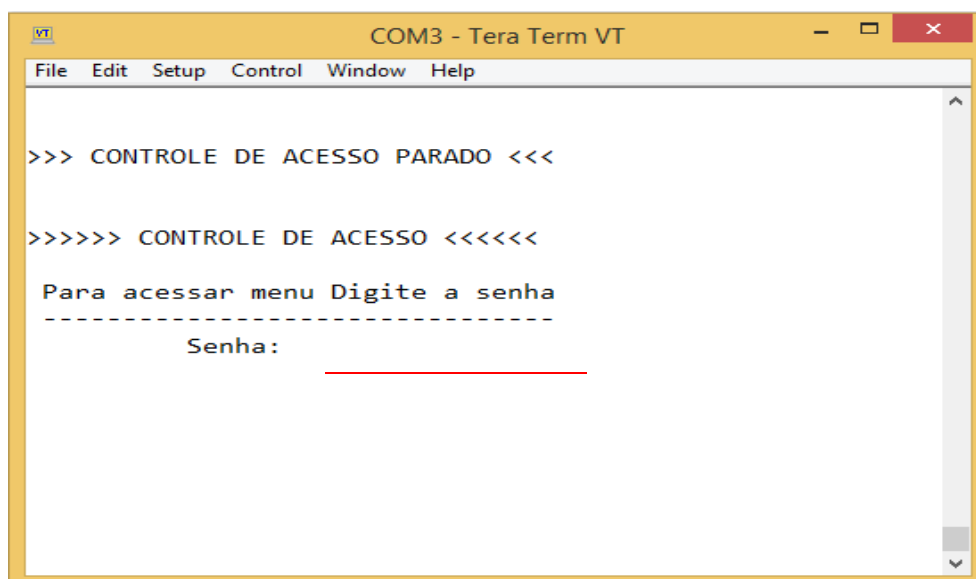
Figura 15 - Filtro *snubber*.

Fonte: Próprio autor.

3.3.1.4 Menu de ajustes

Para o usuário fazer a visualização e cadastramento das senhas, *tags* e tempos, também foi desenvolvido um menu de ajustes, em formato simples e objetivo, utilizando a UART da *launchpad* situada na placa central, onde, para acessar estas configurações, é necessário digitar a senha de acesso correta, conforme mostra a Figura 16. Para acessar o menu basta pressionar a tecla SW2 localizada na *launchpad* conforme mostra a Figura 12.

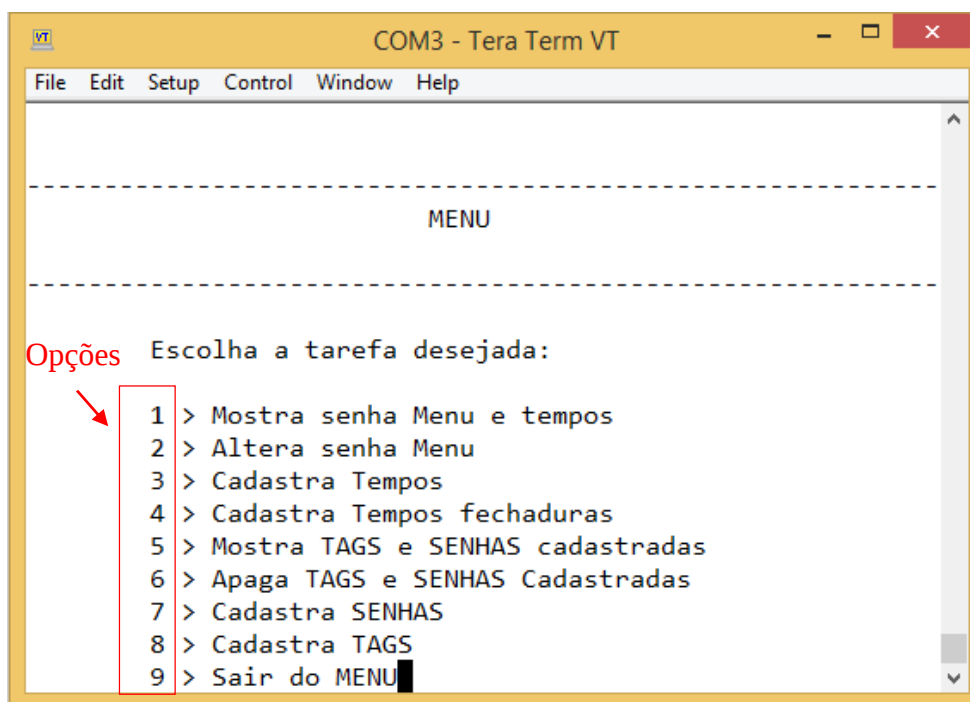
Figura 16 - Tela de acesso Menu



Fonte: Próprio autor.

Após digitar a senha correta, o sistema mostra na tela as opções do menu, conforme mostra a Figura 17, onde o usuário deverá selecionar a opção desejada.

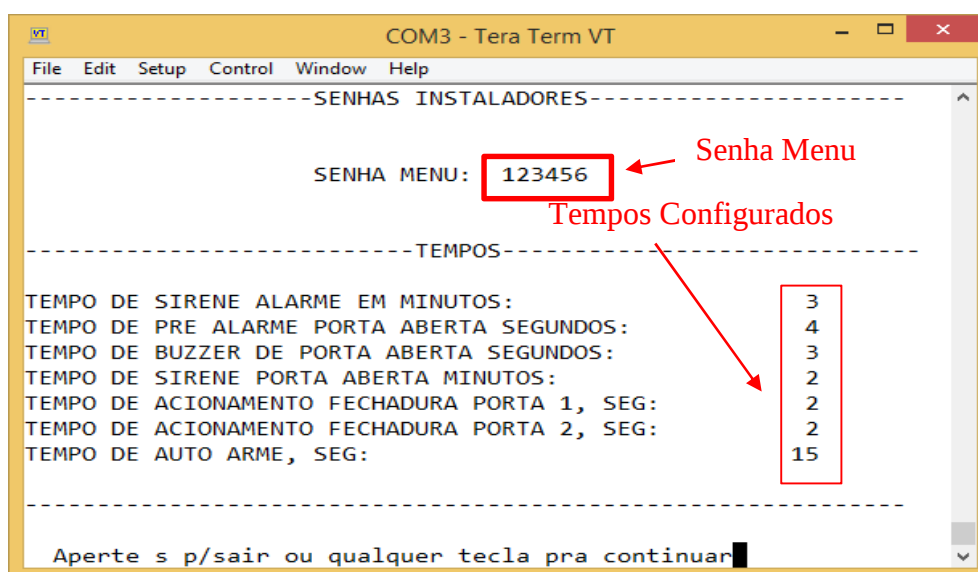
Figura 17 - Menu



Fonte: Próprio autor.

Selecionando a opção 1, o usuário vai visualizar a senha do menu, conforme mostra a Figura 18, e os tempos cadastrados.

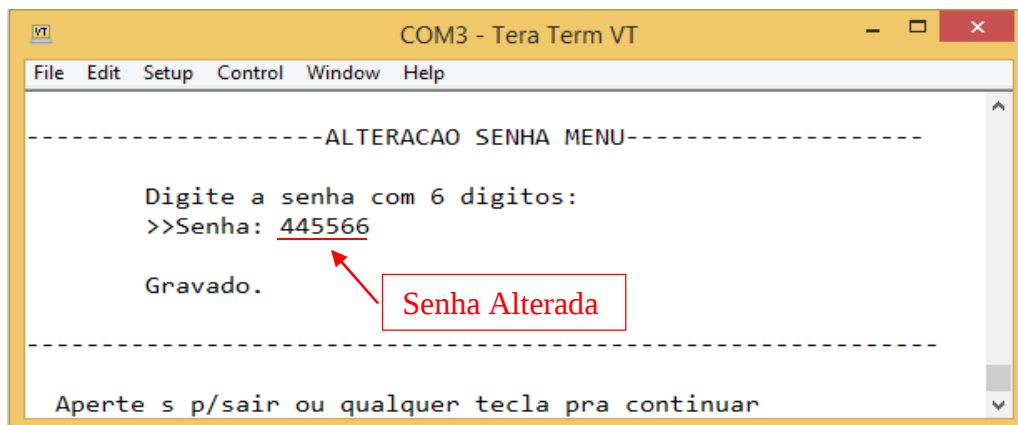
Figura 18 – visualização da senha do menu e os tempos do sistema (opção 1).



Fonte: Próprio autor.

Selecionando a opção 2, o usuário poderá alterar a senha de acesso ao menu de “123456”, para o número desejado, conforme mostra a Figura 19.

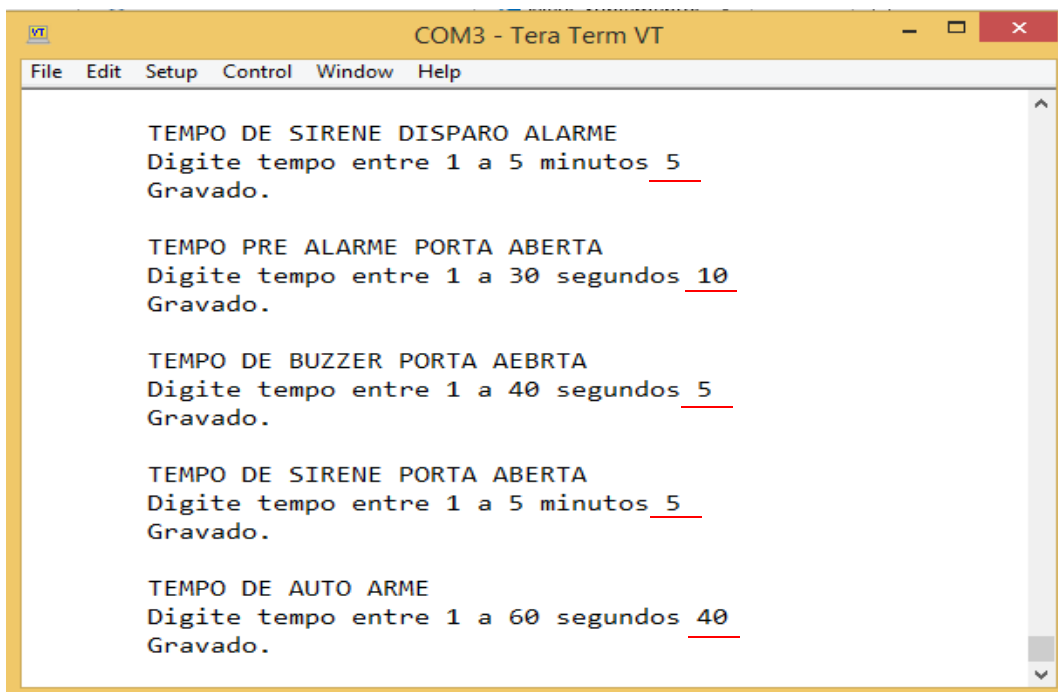
Figura 19 - Alteração de senha (opção 2).



Fonte: Próprio autor.

Selecionando a opção 3, cadastrará os tempos do sistema, conforme mostra a Figura 20.

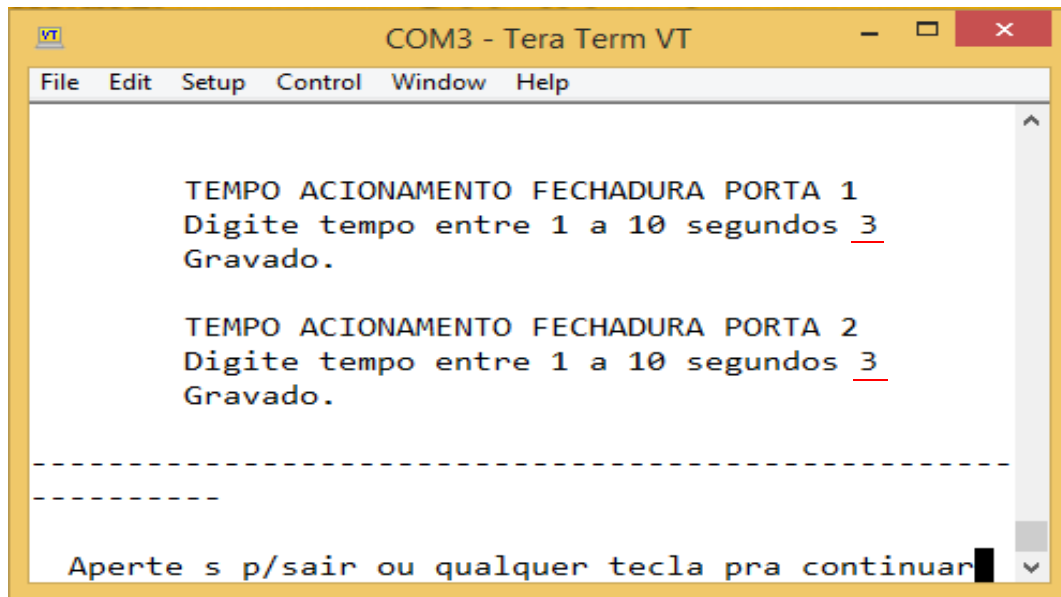
Figura 20 - Cadastro de tempos (opção 3).



Fonte: Próprio autor.

Selecionando a opção 4, o usuário pode cadastrar os tempos de acionamentos das fechaduras, conforme mostra a Figura 21.

Figura 21 - Tempo de acionamentos das fechaduras (opção 4).



Fonte: Próprio autor.

Na opção 5, o sistema mostra as senhas e *tags* cadastrados, conforme já mencionado, sendo 4 de cada tipo, conforme mostra a Figura 22.

Figura 22 - Visualização de senhas e *tags* (seção 5).

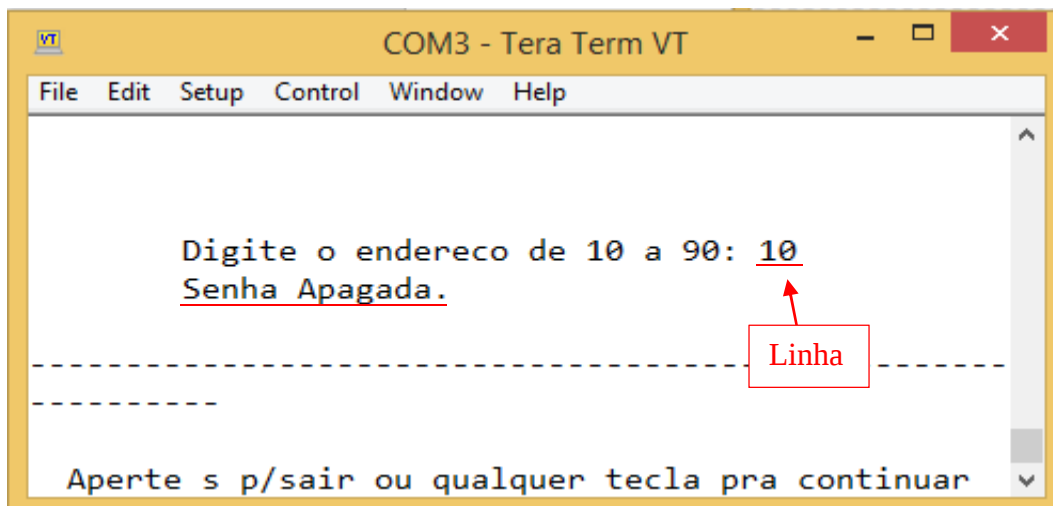


Fonte: Próprio autor.

Na opção 6, apaga-se qualquer uma das senhas ou *tags* cadastrados, para isso basta utilizar o número da linha que está ao lado de cada um deles. Exemplo: para excluir a *senha*

“10” e *tag* “50”, utiliza-se o número da linha, os quais estão cadastrados, no caso, “10” e “50”, conforme mostra a Figura 23.

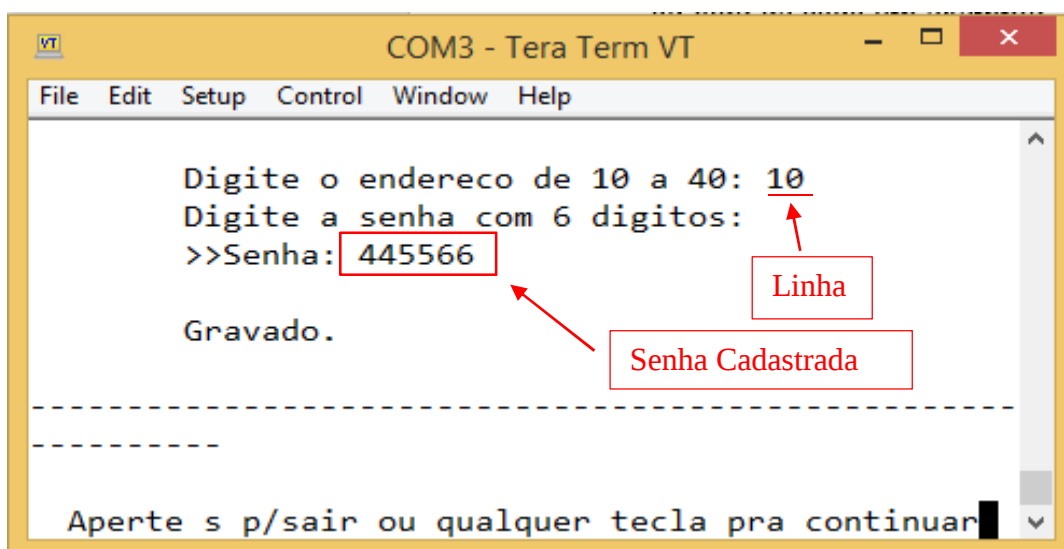
Figura 23 - Exclusão de senhas e *tags* (opção 6).



Fonte: Próprio autor.

Na opção 7, é onde serão cadastradas as senhas, conforme mostra a Figura 24. Elas são utilizadas para acessar o sistema via *interface* com o usuário, desarmando o alarme e liberando as portas.

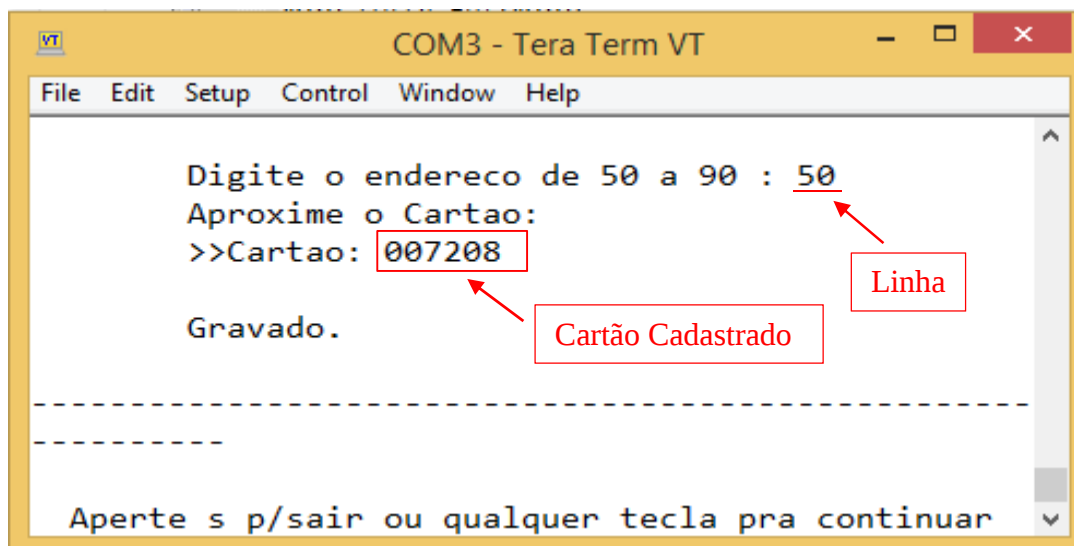
Figura 24 - Cadastramento de senhas (opção 7).



Fonte: Próprio autor.

Na opção 8, é onde serão cadastrados os *tags*, conforme mostra a Figura 25. Eles são utilizados para acessar o sistema via *interface* com o usuário, desarmando o alarme e liberando as portas.

Figura 25 - Cadastramento de tag (opção 8).



Fonte: Próprio autor.

Acessando a opção 9 o usuário sai do menu de ajustes, e o programa volta a ser executado normalmente.

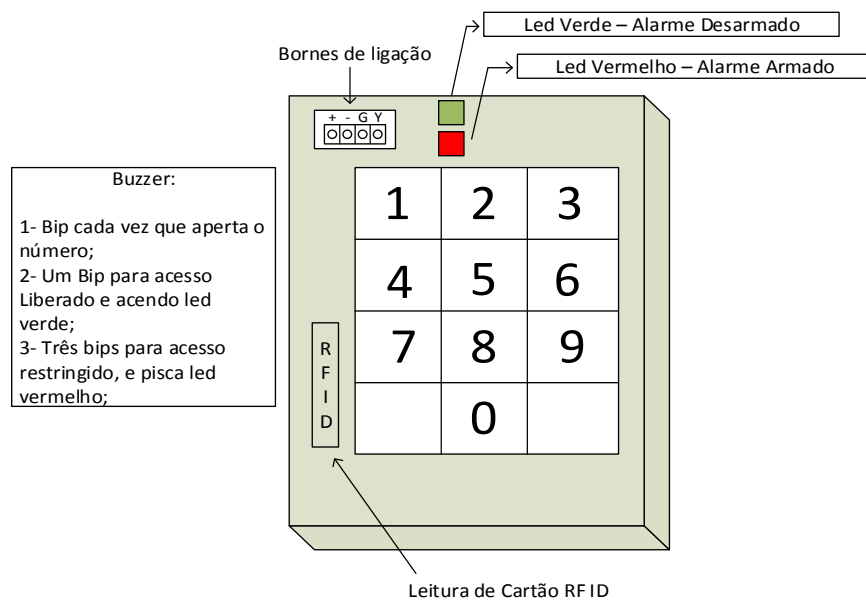
3.3.2 Interfaces com os usuários

O sistema conta com duas destas *interfaces*, conforme o modelo mostrado na Figura 26, estas foram instaladas próximas das portas e utilizam *launchpads*, que fazem o processamento das informações oriundas dos teclados matriciais e dos módulos leitores de *tag*, RDM 6300. As informações são enviadas através do protocolo de comunicação UART, e cada *interface* conta com as saídas e entradas, conforme descritas abaixo:

- *saída para o led vermelho*: quando estiver aceso significa que o alarme está ativado e quando apagar, alarme desativado;
- *saída para led verde*: quando acender significa que o alarme está desligado e o acesso liberado;

- *saída para buzzer*: o mesmo emite um sinal sonoro para cada tecla pressionada, assim como três bips de negação para senha ou *tag* errados, e dois bips para senha correta;
- *entrada para RFID*: onde está ligado o RDM 6300, dispositivo que fará a leitura dos *tags*;
- *saída UART*: saída pela qual a *launchpad* da interface do usuário se comunica com a placa central;
- *entrada do teclado*: local onde é ligado o teclado matricial, pelo qual os usuários digitarão as senhas de acesso;

Figura 26 - Esboço do Teclado.



Fonte: Próprio autor.

Na Figura 27, segue a pinagem da *launchpad*, utilizada para ligar os dispositivos citados nesta seção.

3.3.2.2 Leitor RF ID

Para a leitura dos *tags* foi incorporado ao *layout* da *interface* um módulo RDM 6300, onde o mesmo também se comunica com a *launchpad*, através da UART de forma assíncrona. O Quadro 4 mostra como são recebidos os dados pelo microcontrolador.

Quadro 4 - Organização dos dados enviados pelo leitor RFID.

byte 0	byte 1 - 10	byte 11 - 12	byte 13
.	TAG - Caracteres ASCII	checksum	.

Fonte: Próprio autor.

Nota-se que são recebidos 14 caracteres, onde o primeiro e o último byte recebido são indicadores de início e fim (“.”). Na sequência, os bytes de número 1-10 são a informação contida no cartão, e as informações nos bytes 11 e 12 são o *checksum*.

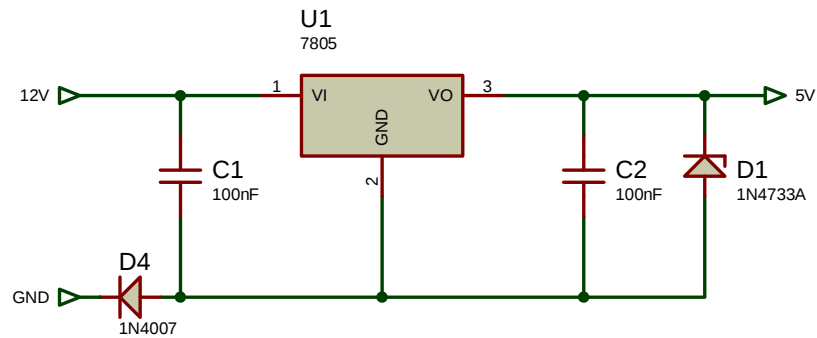
O *checksum* são caracteres que representam a função OU exclusivo da informação recebida pelo microcontrolador, utilizado para fazer a verificação e validação da informação. No código não é utilizado o valor do *checksum*, pois são somente utilizados 6 caracteres do código do *tag* (recebido por um vetor de 6 posições), para uma melhor visualização e armazenamento na memória do microcontrolador central.

A entrada de senha é feita através de um teclado matricial 4x4, onde a quarta coluna que faz referência aos caracteres a,b,c e d (caracteres situados na quarta coluna do teclado matricial) foram desabilitados, pois o sistema utiliza somente caracteres numéricos, onde assim como os *tags*, o valor de entrada será comparado com o valor cadastrado na memória da placa central, fazendo sua validação e abertura das portas.

3.3.2.3 Circuito de redução de tensão da fonte

As alimentações das *interfaces* e de seus componentes foram feitas fisicamente por uma tensão 12V oriunda da placa central. Esta tensão, por sua vez, vai sofrer rebaixamento para 5V através de um 7805, que também fornece 1A de corrente para o circuito, conforme mostra a Figura 28. Para evitar a queima dos componentes do sistema, caso a alimentação for ligada invertida, foi adicionado ao circuito, um diodo reversamente polarizado na entrada negativa da placa.

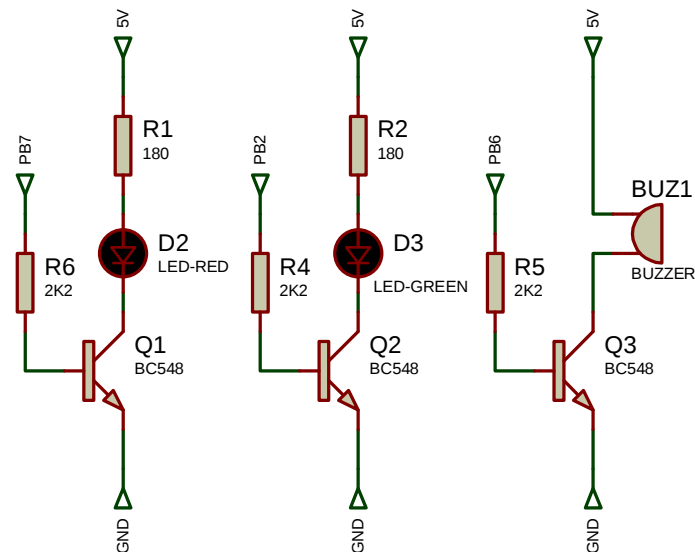
Figura 28 - Redução da tensão para 5V



Fonte: Próprio autor.

Para as sinalizações, foram incorporados ao sistema dois *leds* que mostrarão o status (armado ou desarmado) e um *buzzer* sinalizará quando os números foram digitados no teclado matricial ou quando foi efetuado a leitura do *tag*. Os circuitos foram dimensionados para que a corrente das saídas não ultrapasse 25 mA, como mostra a Figura 29.

Figura 29 - Ligação Leds/buzzer



Fonte: Próprio autor.

Para os cálculos de corrente foi considerado um V_{BE} igual a zero, ou seja, o transistor está em saturação.

$$I_{Coletor} = \frac{VCC - V_{Led}}{180} \quad (5)$$

$$V_{Led} = 1,8V;$$

$$VCC = 5V;$$

$$I_{buzzer} = 28 \text{ mA};$$

$$I_{ColetorLeds} = \frac{5V - 1,8}{180} = 18 \text{ mA}$$

Para a utilização dos transistores, foi calculada a corrente mínima de base para que o modo de operação entre na região de saturação, o que significa que VCE tende a ser igual a zero.

$$I_{Coletor} = hFE \times I_{BaseMin} \tag{6}$$

$$I_{BaseMin} = \frac{28,4}{150} = 0,19 \text{ mA}$$

$$I_{BaseReal} = \frac{3,3 - 0,7}{2200} = 1,18 \text{ mA}$$

3.4 COMPONENTES DO SISTEMA

A seguir são apresentados os componentes utilizados para a elaboração do projeto, com suas características e onde foram aplicados.

3.4.1 Sensor *reed switch*

O sensor magnético, Figura 30, foi utilizado para intertravar as portas, monitorá-las, rearmar o sistema e verificar se foram esquecidas abertas. Suas características são:

- sensor com cabo paralelo 25 mm;
- distância de acionamento 12 mm;
- dimensões C: 25,5 x A:7,4 x L: 9,5 mm;

Figura 30 - Sensor magnético.



Fonte: <http://www.brubeki.com.br/paradox1.html> (15/10/18 às 16:23).

3.4.2 Sensor Infravermelho

O sensor infravermelho, Figura 31, foi usado para detectar pessoas dentro da clausura. Seu modelo é LC 100 da marca DSC. Suas características são:

- sensor IR Quad (4 elementos);
- ângulo de abertura 90°;
- alcance de detecção 10 metros;
- alimentação de 8,2V a 16 V;
- consumo de corrente: ativo 10 mA, repouso 8 mA;

- imunidade a rádio frequência: de 80 MHz a 1 GHz;
- temperatura de operação -10 a 50 graus celsius;

Figura 31 - Sensor DSC LC 100.



Fonte: Próprio autor.

3.4.3 Fechadura

Nas portas foram utilizados 2 fechos eletrônicos da marca Thevear, Figura 32, e acionarão mediante ao comando da placa central, ou pressionando a botoeira de saída, no caso da 1ª porta. Suas características são:

- alimentação 12 V a 15 V;
- corrente de consumo 2A;

Figura 32 - Fechadura eletrônica.



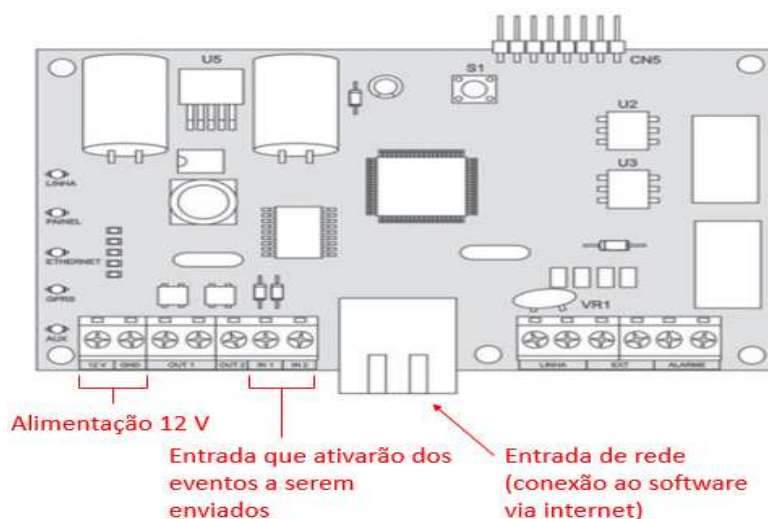
Fonte: <http://www.thevear.com.br/new/VerProdutos.aspx?IDSubCat=143> (15/10/18 às 16:31).

3.4.4 Transmissão de eventos

Os eventos gerados pelo sistema são enviados através da internet, por um módulo de transmissão MONIP, conforme mostra a Figura 33, que está ligado ao protótipo. Quando o sistema gerar os disparos (alarme, porta aberra, ou incêndio), irá acionar as entradas do transmissor, que por sua vez enviará um código de identificação para o *software* de monitoramento o qual será interpretado e identificado. Suas características são:

- consumo de corrente 400 mA;
- transmissão via internet;
- alimentação 12 a 16 V

Figura 33 - Módulo de transmissão de eventos.



Fonte: http://www.softguard.com/71_ppa-compatibilidad-total-ip (15/10/18 às 16:34)

3.4.5 Sensor de fumaça

Este sensor, Figura 34, foi utilizado para realizar a detecção da fumaça, em caso de incêndio, fazendo com que as portas se abram automaticamente. Suas características são:

- alimentação 12 a 26 V;
- consumo 20 mA;
- tipo fotoelétrico;

Figura 34 - Detector de fumaça.



Fonte: Próprio Autor.

3.4.6 Fonte de alimentação

Para alimentar o sistema e foi dimensionada uma fonte que consiga suprir a necessidade de corrente elétrica dos componentes instalados. Ela contém uma bateria para alimentar o sistema, caso energia elétrica venha a falhar e proteção contra curto-circuito.

Consumo de corrente do sistema:

- | | |
|--|--------|
| • 1 sensores Infravermelho | 16 mA |
| • transmissor de eventos MONIP | 400 mA |
| • consumo dos 3 microprocessadores ARM | 100 mA |
| • um sensor de fumaça | 40 mA |

Para dimensionar a fonte, deve ser levado em consideração todas as correntes consumidas pelos dispositivos do projeto, conforme equação 7.

$$IT = I_{\text{infra red}} + I_{\text{fechos eletrônicos}} + I_{\text{monip}} + I_{\text{launchpad}} + I_{\text{fumaça}} \quad (7)$$

$$IT = 16 \text{ mA} + 400 \text{ mA} + 100 \text{ mA} + 40 \text{ mA}$$

$$IT = 556 \text{ mA}$$

Cálculo do tempo de duração da bateria do sistema:

- capacidade de corrente da bateria 7Ah (Ampere hora). Quer dizer que a bateria tem capacidade de fornecer 7A de corrente durante uma hora. Então o pela equação (8) temos:

$$Tempo = \frac{I_{bateria}}{IT} = \quad (8)$$

$$Tempo = \frac{7 Ah}{956 mA} = 12 h 58 min$$

Com base no cálculo da equação 7 a fonte escolhida foi a FAST GOLD 5A, Figura 35, com as características especificadas a seguir e que supre a demanda de corrente do projeto:

- tensão de alimentação 220 V ou 110 v;
- corrente máxima fornecida 5 A;
- tensão de saída 12 VDC;

Figura 35 - Fonte de alimentação do projeto.



Fonte: Próprio autor.

3.6.7 Leitor de cartão RFID

Com o objetivo de identificar o morador, foi utilizado um leitor de RFID para 125kHz, modelo RDM630, o qual está representado pela Figura 36. Esse leitor tem comunicação TTL RS232-UART. As características elétricas são:

- Alimentação: 5VDC;

- Protocolo de comunicação: TTL RS232 UART;
- Corrente máxima: 50mA;
- *Baud Rate*: 9600bps;
- Dado: 8 bits (byte a byte, caractere);
- Paridade: sem paridade;
- Stop bit: 1 bit;
- Frequência de leitura: 125kHz;
- Distância máxima de leitura: 5cm;

Figura 36 - Leitor RF ID RDM 6300.



Fonte: Adaptado de <http://www.rfidhy.com/hy-rdm630-125khz-134-2khz-reader-module-access-control-rfid-reader-writer-module/> (25/11/2019 às 13:23)

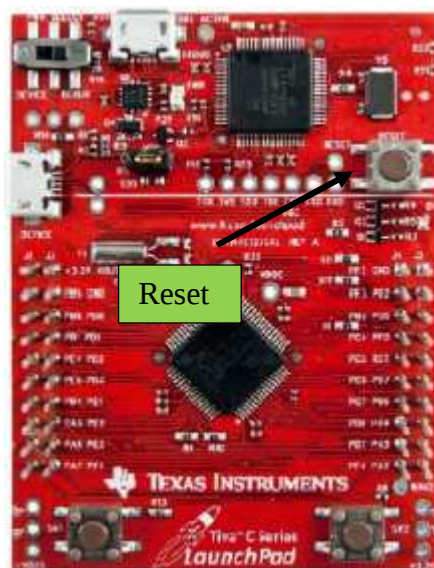
3.5 FUNCIONAMENTO DO PROTÓTIPO

O protótipo desenvolvido fará a liberação de duas portas, através da leitura de um *tag*, ou digitação de uma senha. As *interfaces* com os usuários são equipadas com leitores RFID e foram instaladas nas portas da clausura, conforme mostra a Figura 8.

Para realizar o processamento das informações, assim como a leitura dos sensores e *interfaces* instaladas, foi escolhido um kit de desenvolvimento da família ARM, modelo EK-TM4C123GXL, Figura 37. O kit possui os requisitos necessários para a aplicação, também não precisa de interface física a mais, para sua gravação, pois se pode gravar diretamente do computador usando os seus periféricos externos.

Para o protótipo inteiro, foram utilizados 3 *launchpads*, que se comunicam entre si, via protocolo UART. Esta comunicação é assíncrona, ou seja, os dispositivos não compartilham o mesmo *clock*, e a velocidade entre eles foi setada em 9600 bauds. A sua comunicação de envio e recebimento é *full duplex*, que envia e recebe as informações ao mesmo tempo.

Figura 37 - *Launch pad* ARM.



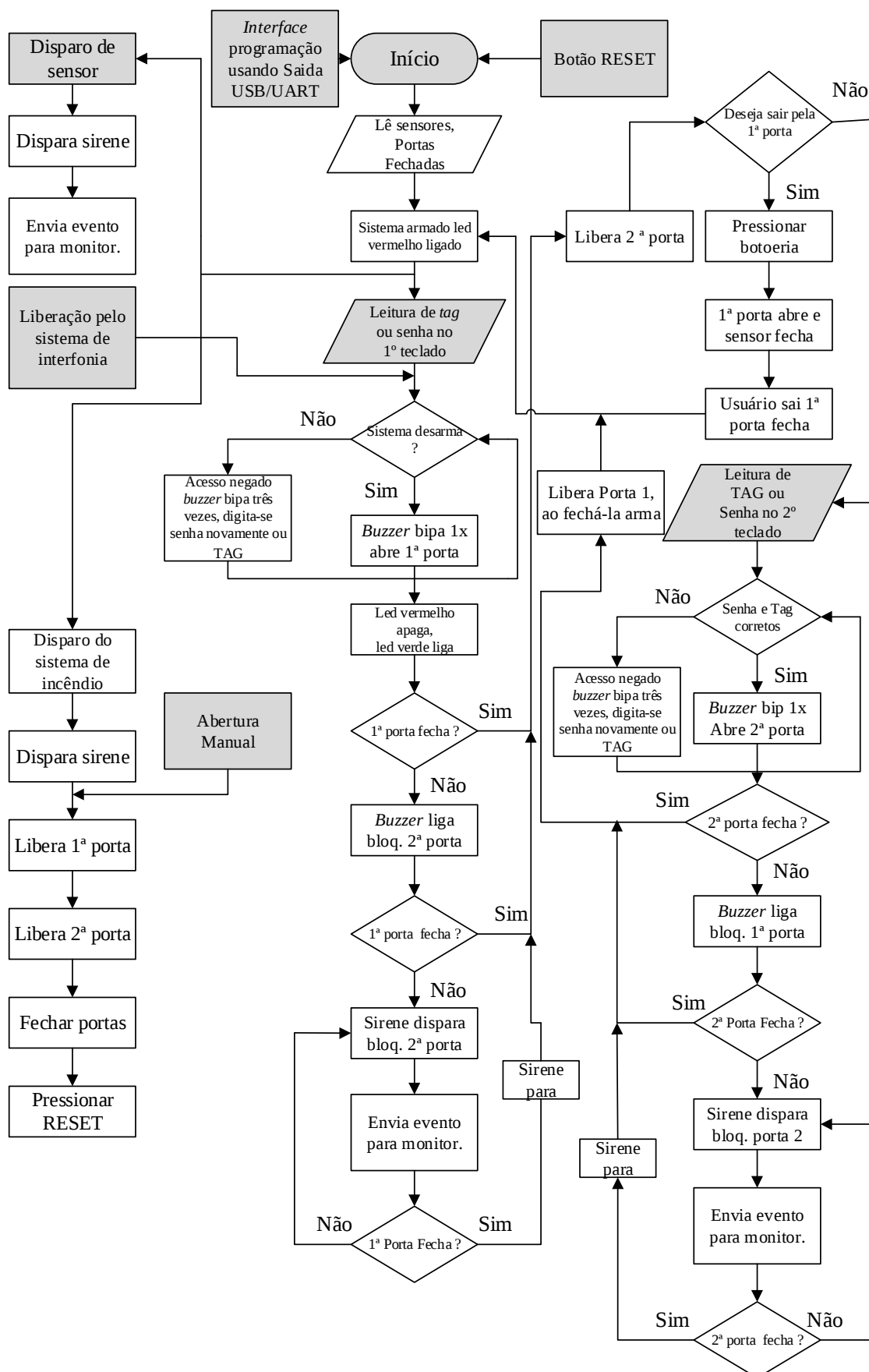
Fonte: Próprio autor.

3.5.1 Firmware

O *firmware* foi desenvolvido em linguagem C, a qual é utilizada no compilador. Para a programação foi escolhido o *IAR Embedded Workbench* para ARM, pois apresenta uma *interface* mais interativa e familiar. Para o desenvolvimento do *firmware* foram analisadas as necessidades de hardware, mas o que mais influenciou foi fazer a comunicação entre a placa central com as duas *interfaces* dos usuários, usando UART.

Para o sistema foram utilizados vários sensores, os quais farão a leitura da abertura e fechamento das portas, levando as informações para o *firmware*, fazendo com que o mesmo execute as tarefas, conforme o fluxograma da Figura 38.

Figura 38 - Fluxograma de funcionamento *firmware*



Fonte: Próprio autor.

Os tipos de sensores que fazem as leituras para o sistema são:

3.5.1.1 *Leitura dos sensores de alarmes das portas*

Estes sensores (*reed switches*), foram instalados nas duas portas e tem como função principal, executar a leitura de sua abertura, fazendo com que o sistema dispare em caso de intrusão (abertura da porta com sistema ativado). Para isso foram utilizados dois pinos de interrupções da *launchpad* da placa central, pois se o *software* estiver executando uma tarefa, ele para, executa a interrupção e depois volta a executar a tarefa anterior.

Estes sensores são desativados quando um *tag* ou senha é lido, ou digitada no teclado de uma das *interfaces* dos usuários. O mesmo envia as informações para o *launchpad* da placa central via UART, comparando com as senhas e *tags* armazenadas na EEPROM. Se estiverem devidamente cadastradas o sistema é desarmado, e por sua vez, o *software*, envia para as *interfaces* através da UART o *status* de liberação, simbolizado pelo *led* verde aceso e mais dois bips sonoros.

3.5.1.2 *Leitura dos sensores de intertravamento das portas*

Estes sensores (*reed switches*), são responsáveis por fazer o intertravamento das portas, ou seja, uma somente abre mediante o fechamento da outra. Ao permanecer aberta o *firmware* bloqueia a leitura da senha, inibindo a comparação com a EEPROM, e emitindo três bips de negação, sinalizado também pelo *led* vermelho, piscando três vezes em sequência. Além de intertravarem as portas, estes reconhecem se a mesma foi deixada aberta, fazendo com que o *firmware* ative um *buzzer*, durante um tempo pré-definido via programação, para tentar chamar a atenção do usuário caso deixe-a aberta, ou não à feche, sendo assim, a sirene ativa-se e aciona uma saída, a qual é ligada no transmissor que enviará um evento para a base de monitoramento.

3.5.1.3 *Leitura do sensor de incêndio*

Como o sistema de controle de acesso, precisa ser ligado a um sistema de detecção de incêndio, para que haja a liberação das portas automaticamente para a evacuação do local, foi instalado na maquete, um detector de fumaça (CO₂) que fará as liberações das duas portas simultaneamente. Ao detectar a fumaça ele vai entrar em disparo, acionando uma interrupção dentro do *firmware*, a qual libera ambas as portas, desligando o alarme, e deixando-as abertas.

Também a sirene é acionada e toca um som intermitente, para que haja a diferenciação do alarme de arrombamento, além disso é acionado o transmissor, para enviar os eventos de incêndio para o monitoramento. Para o sistema voltar ao funcionamento normal, basta resetar o microcontrolador, pressionando o botão *reset* da placa central, conforme Figura 37.

3.5.1.4 Liberação das portas

As liberações das portas irão ser feitas, através da leitura dos tags ou senhas, executadas nas *interfaces* com os usuários. O *firmware* irá comparar esses dados enviados pela UART e se forem os mesmos (dados lidos e cadastrados), o sistema atribui um valor inteiro em uma variável que desabilita a função de alarme do sistema, fazendo com que o mesmo não dispare ao abrir a porta. Ao mesmo tempo, ele retorna para o teclado um dado fazendo com que o led verde acenda, simbolizando que o alarme da porta acessada está desarmado. Ao acessar com *tag* ou senha a outra porta, o sistema executa a mesma rotina.

3.5.1.5 Leitura dos sensores de rearme

Estes sensores (*reed switches*), fazem o rearme do sistema, quando uma das portas fechar. Após fechá-la, o sistema faz com que a variável que desabilitou o alarme anteriormente, volte ao seu valor inicial, reativando sistema. Por sua vez, a UART se comunica novamente enviando um dado para a *interface* do usuário, fazendo com que o *led* vermelho acenda, simbolizando que o alarme da porta está ativado. Para a outra porta, o sistema executa a mesma tarefa.

3.5.1.6 Leitura da botoeira /Interfone da 1ª porta

Ao pressionar este botão, o *software* desativa somente o alarme da 1ª porta, fazendo, com que a UART envie um dado para a *interface* com o usuário desta porta, acendendo o *led* verde e liberando a saída de algum visitante que esteja dentro da clausura. Também é possível liberar esta entrada através do sistema de interfonia, retirando o visitante do risco de segurança proporcionado pela rua, protegendo-o dentro da clausura. Ao fechar a porta o sistema rearma, conforme descrito no item anterior.

3.5.1.7 Leitura do sensor infravermelho

Este sensor informa ao sistema que há alguma movimentação no interior da clausura, impedindo que sistema rearme por não movimento. Este recurso é útil se estiverem ligados mais sensores no sistema, evitando assim, disparos proveniente de visitantes que estão se movimentando dentro clausura.

3.5.2 Menu de ajuste

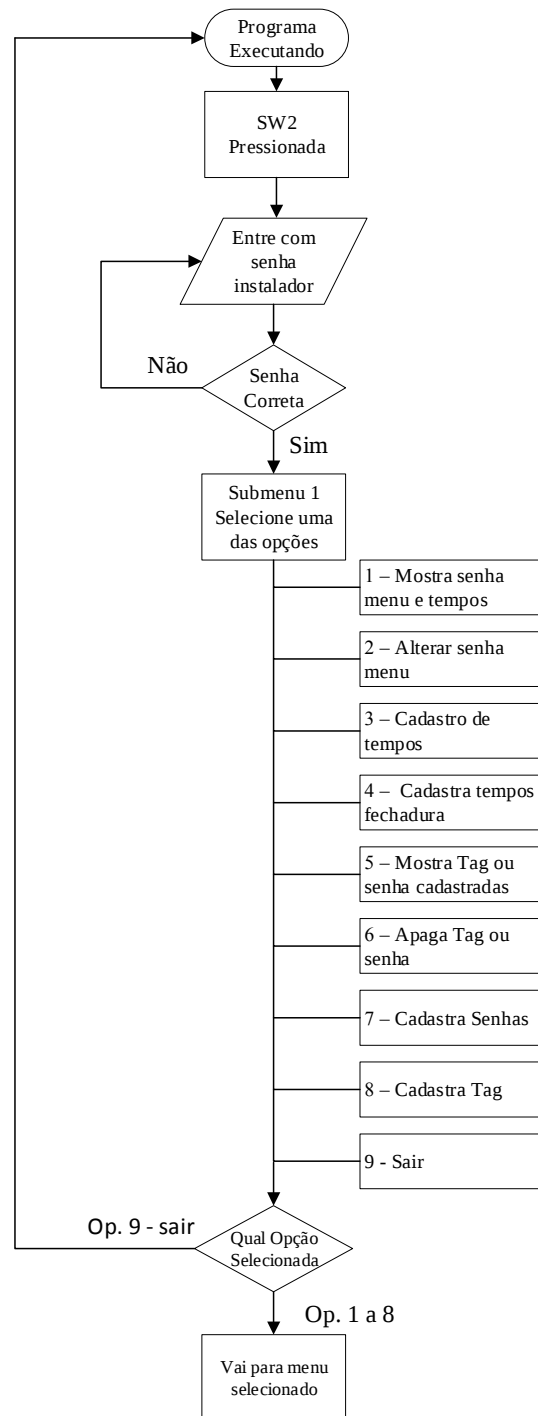
Este menu é utilizado para fazer o ajuste dos parâmetros dos tempos, senhas e *tags*. Será utilizado para isso a saída USB da *launchpad*, onde está ligada a UART. Para proteger o sistema de alterações, o menu tem uma senha de acesso. Como se trata de um protótipo que poderá ser utilizado em cenários diferentes, todos os ajustes são personalizados levando em consideração os requisitos do ambiente ao qual seja instalado. Este menu é acessado pressionando a tecla SW2 da placa central e em seguida perguntará a senha de acesso. Este menu ajusta os seguintes parâmetros:

- *tempo de liberação da porta 1e 2*: quando a porta for liberada, ela ficará aberta pelo tempo ajustado (1 a 10 segundos);
- *tempo de sirene de alarme*: caso algum disparo, dos sensores das portas venham a acontecer, a sirene irá soar pelo tempo estabelecido (1 a 5 segundos);
- *tempo de pré-alarme de porta deixada aberta*: este ajuste é responsável por monitorar o tempo em que a porta poderá ficar aberta, após isso, alarmes serão gerados (1 a 30 segundos);
- *cadastramento de Senha*: inserir, recadastrar ou excluir senhas. O sistema permite o cadastramento de 4 senhas;
- *cadastramento de tag*: Inserir, recadastrar ou excluir *tag* são. O sistema permite o cadastramento de 4 *tags*;
- *recadastro da senha Instalador*: virá programada por padrão 123456, e poderá ser alterada;
- *visualização de senhas e TAG*: mostra as senhas e *tags* cadastrados no sistema;
- *tempo de buzzer para porta deixada aberta*: após terminar o tempo de pré-alarme, o sistema vai emitir um sinal sonoro via *buzzer* no seu teclado correspondente, alertando o usuário (tempo de 1 a 30 segundos);

- *tempo de sirene de porta deixada aberta*: após terminar o tempo de *buzzer* a sirene irá soar, acionando também uma saída, a qual, aciona o transmissor para o envio do evento de “porta aberta” (tempo de 1 a 5 segundos);
- *visualização da senha menu e tempos*: o sistema mostra a senha que protege o menu, e os valores ajustados para: tempo de sirene de alarme, tempo de pré-alarme de porta aberta, tempo de buzzer, porta deixada aberta, tempo de sirene porta deixada aberta, tempo de abertura das fechaduras um e dois e tempo de auto arme;
- *tempo de auto arme*: se por algum motivo o usuário digitar a senha ou passar o *tag* e não acessar a clausura, o sistema vai ficar desarmado por um período estabelecido de 0 a 60 segundos, voltando a se ativar após decorrido este tempo.

A figura 39, mostra como é organizada a tela de seleção das opções do menu de ajustes.

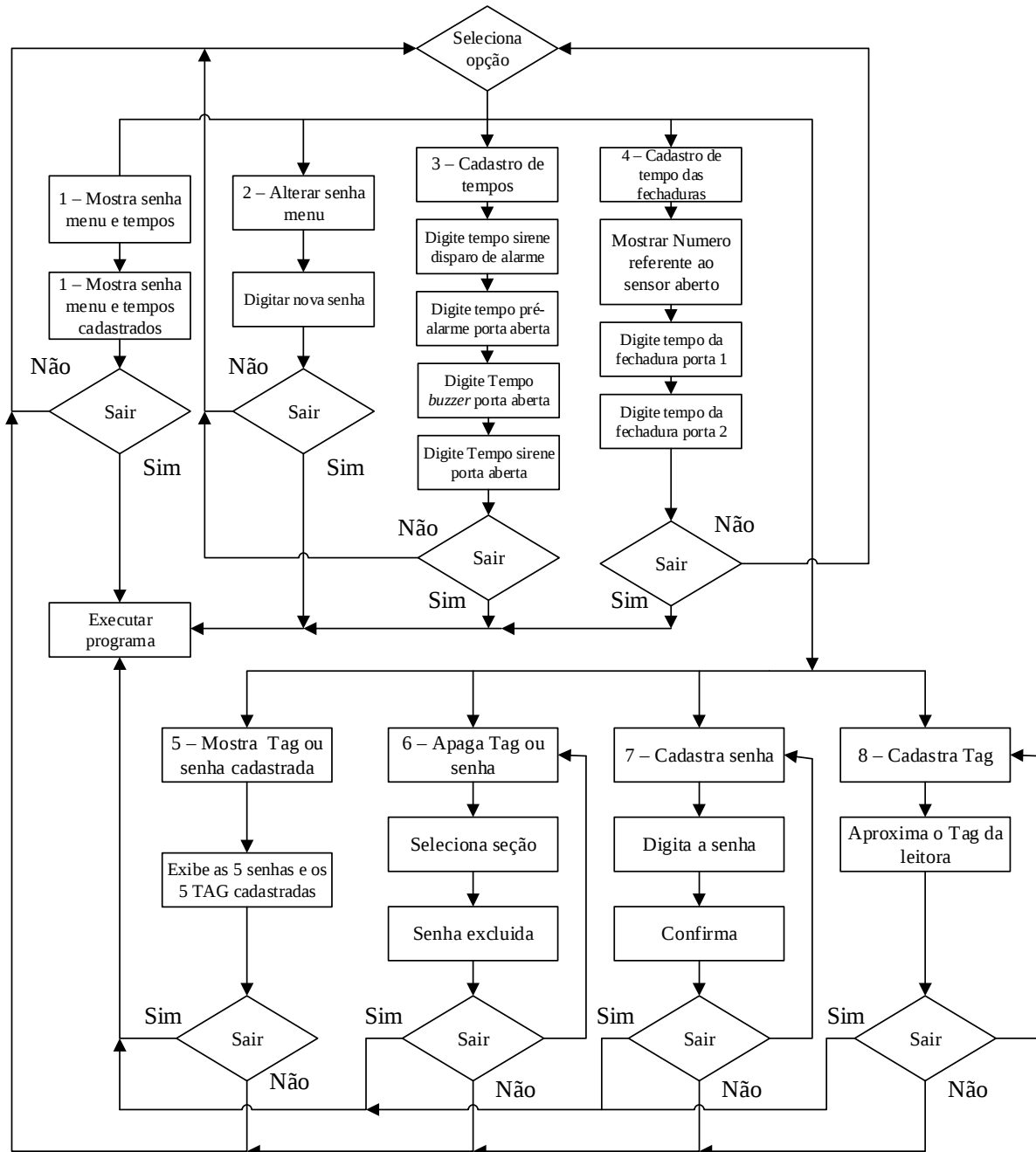
Figura 39 – Interface de seleção dos ajustes via UART.



Fonte: Próprio autor.

Na figura 40 é mostrado como funciona o *firmware*, após selecionar uma das opções do menu de ajustes da figura 39.

Figura 40 – Funcionamento do firmware que salva os valores ajustados.



Fonte: Próprio Autor.

4 RESULTADOS E DISCUSÕES

Neste capítulo serão abordados os testes realizados com o protótipo e seus resultados, possíveis falhas dos componentes e o que isso implicaria na segurança. Para melhor entendimento dos testes efetuados, os mesmos serão feitos em simulações.

4.1 LEITURA DE SENHA E TAG PELO TECLADO

A Figura 41 mostra como é feita a leitura do *tag*, através do módulo leitor RDM6300 instalado na *interface* do usuário. Para gerar a detecção é preciso aproximar bastante o TAG da antena do RDM. O *datasheet* do módulo informa que a distância máxima é de 5 cm, o que parece não se aplicar na prática, já que temos que encostá-lo no leitor. A leitura dos caracteres é feita corretamente pelo dispositivo, se mostrando rápida e precisa, assim como o envio dos dados para a placa central. A senha digitada no teclado é lida perfeitamente e também envia corretamente para o microcontrolador central, que faz a sua comparação com a senha armazenada na memória EEPROM, acontecendo o mesmo com a TAG.

A troca de informações entre os módulos pode ocorrer simultaneamente, fazendo com que as interrupções e as liberações das portas não conflitem entre si, porém, ao iniciar o sistema deve-se, obedecer a seguinte ordem de reset das *launchpads*. Começando por qualquer uma das *launchpads* das *interfaces* com os usuáeios e por último à *launchpad* da placa central. Isso ocorre, por que ao ligar o sistema, as UARTS das *launchpads* enviam um valor aleatório inicial, esse valor faz com que os dados das senhas digitadas e *tags* lidos sejam comparados erroneamente com os valores cadastrados na memória, mas resolve-se o problema fazendo o reset na ordem correta.

Figura 41 – Leitura do *tag* via interface com o usuário.

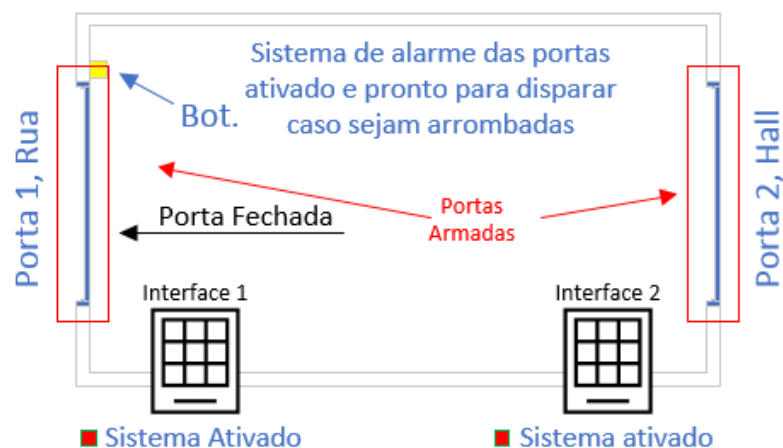


Fonte: Próprio autor.

4.2 TESTE DO ALARME

Ao inicializar o sistema, ele já parte com o alarme ativado, conforme mostra a Figura 42, ao abrir qualquer umas das portas o disparo é instantâneo, fazendo com que a sirene e o *buzzer* do teclado pertencente à porta arrombada, dispare pelo tempo programado no menu de ajustes, assim como a saída que é ligado o transmissor para o envio do evento do alarme, esta saída possui tempo de acionado setado de 3 segundos. Estes sensores estão ligados a *launchpad* central, o qual envia uma informação via UART para acionamento do *buzzer* do teclado. Se a porta ficar aberta, o sistema continua disparando até que seja fechada ou o sistema seja desacionado por *tag* ou senha. Sendo feita desta última forma, o sistema cessa o disparo e acende a luz verde simbolizando o desarme via teclado.

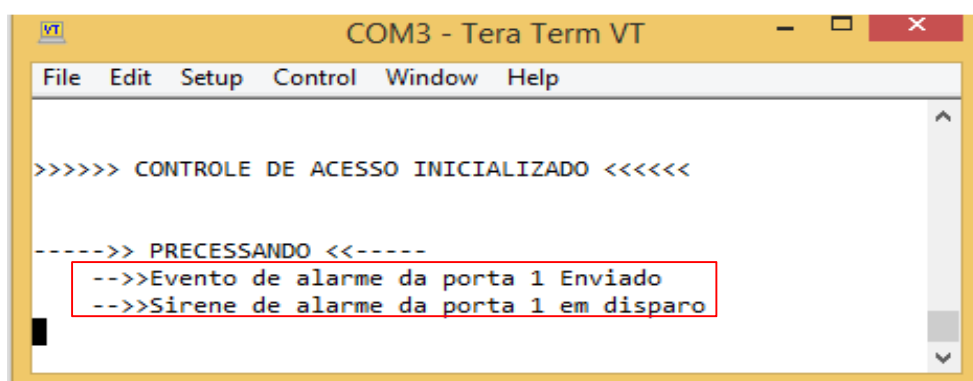
Figura 42 - Sistema armado



Fonte: Próprio autor.

Na Figura 43, segue as mensagens de disparos das portas mostradas pela UART:

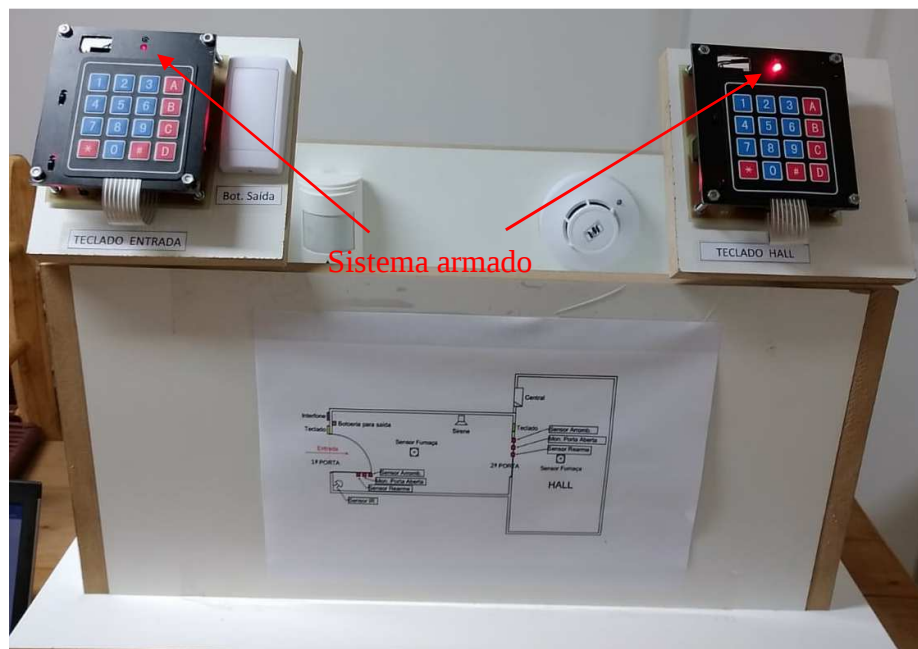
Figura 43 - Disparos de alarme da porta 1



Fonte: Próprio autor.

Abaixo na Figura 44 é mostrado o sistema de alarme da maquete, o qual, está armado.

Figura 44 - Sistema de alarme da maquete ativado



Fonte: Próprio autor.

4.3 TESTE DO SISTEMA DE ENTRADA

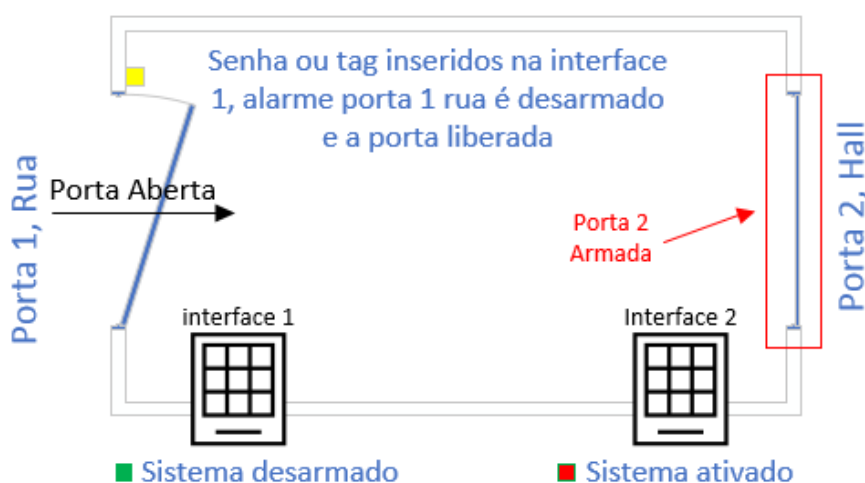
Ao chegar na 1ª porta (rua), o usuário deve digitar a senha ou passar o *tag*, na *interface* 1, ela faz a leitura dos dados e os envia para a placa central. Se estiver correto o sistema sinaliza com três bips, acende o led verde acionando a fechadura da 1ª porta e liberando o acesso para o usuário entrar, como mostra a Figura 45. Quando o mesmo acessa a clausura, o sensor infravermelho o detecta, fazendo a restrição do rearme interno da clausura, deixando-o inoperante. Ao fechar a 1ª porta, o sistema ativa somente o alarme desta porta, o qual estava desativado, mantendo assim, o usuário seguro.

Neste momento, ao fechar a 1ª porta, o usuário faz com que a 2ª porta seja liberada, podendo assim acessá-la com *tag* ou senha. O sistema executará a mesma rotina de liberação apresentada anteriormente. Se caso a 1ª porta for deixada aberta, a 2ª porta será bloqueada, até que a 1ª porta, seja fechada. Se algum usuário mesmo assim, passe o *tag* ou digite a senha na 2ª porta, com a 1ª porta aberta, será emitido 3 bips de negação e o led vermelho irá piscar, mostrando que o sistema não está apto a abrir a 2ª porta. Também, se caso a 1ª porta fique aberta, ao passar o tempo definido, um *buzzer* ligará, tentando chamar a atenção do usuário para

fechá-la. Se isso não for feito, após o tempo de *buzzer* pré-definido, soará a sirene pelo tempo ajustado. Ao mesmo tempo o transmissor é ativado e envia um evento para a central de monitoramento. O sistema ficará em disparo até que a 1ª porta seja fechada, ou o sistema desarmado por *tag* ou senha.

Se caso um visitante chegue e interfone para um apartamento, o morador tem a opção de abrir somente a 1ª porta via interfone, a fim de, retirar este indivíduo do risco que a rua oferece. Ao liberar a 1ª porta, o sistema desativa o seu alarme, mas ao fecha-la é reativado. Para sair existe uma botoeira, que ao ser pressionada, libera a 1ª porta, desacionando o seu alarme. Ao fecha-la tudo volta a ficar ativo.

Figura 45 - Liberação da porta de entrada.



Fonte: Próprio autor.

Na Figura 46, são mostradas as mensagens geradas pela UART na abertura das portas.

Figura 46 - Mensagem de liberação das portas pela UART.

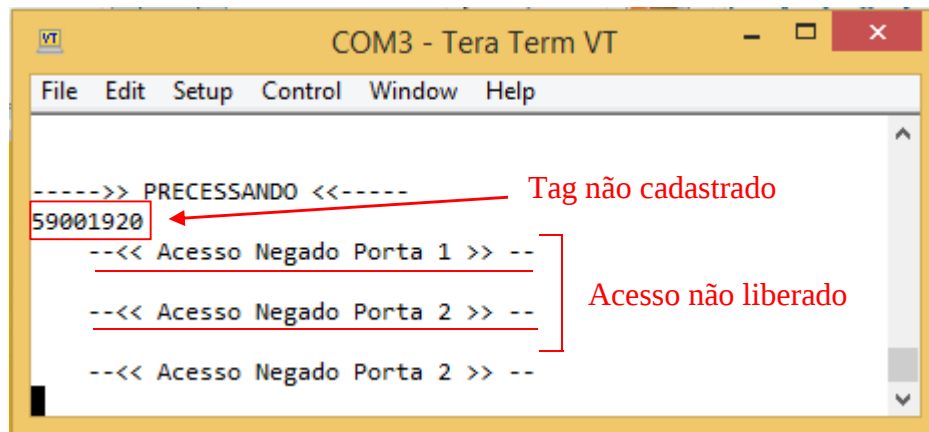
```

----->> PRECESSANDO <<-----
007208
-->> Acesso Liberado Porta 1
007208
-->> Acesso Liberado Porta 1
-->> Acesso Liberado Porta 2
  
```

Fonte: Próprio autor.

Na Figura 47, são mostradas as mensagens de acesso negado exibidas pela UART, ao tentar passar o *tag* ou digitar a senha na porta dois.

Figura 47 - Mensagem de não liberação mostrada pela UART.



Fonte: Próprio autor.

Na Figura 48 é mostrado o funcionamento do protótipo ao executar as ações descritas.

Figura 48 - Protótipo em funcionamento.



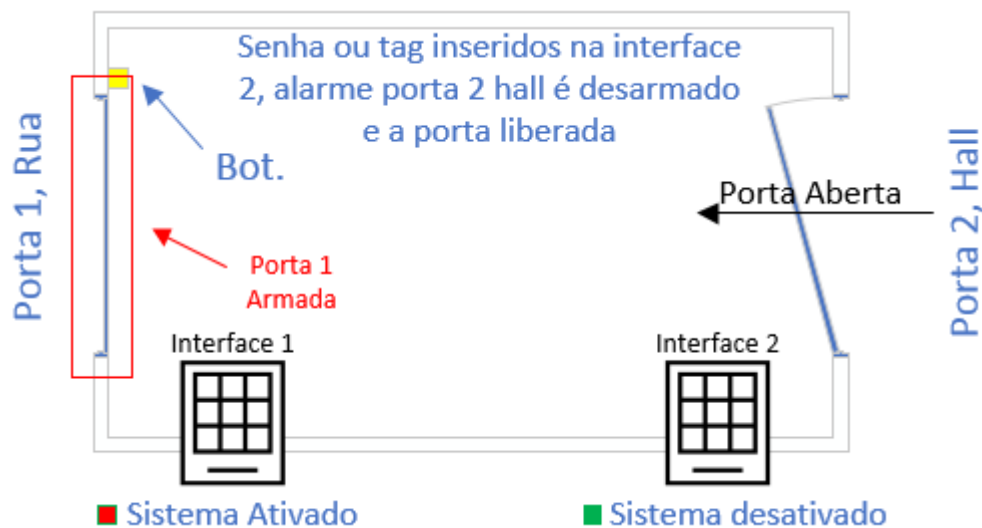
Fonte: Próprio autor.

4.4 TESTE DO SISTEMA DE SAÍDA

Para o sistema de saída, como mostra a Figura 49, o processo é o inverso do anterior (pois agora a porta que será acessada é a 2ª porta), com a exceção que para sair pela 1ª porta,

será utilizado uma botoeira, que vai desarmar o alarme, e liberar a saída, ao fecha-la o sistema rearma, assim como gera disparos se for deixada aberta, podendo impedir a saída do próximo usuário. Mas para evitar estes problemas as mensagens são enviadas para o monitoramento que tomará as medidas cabíveis.

Figura 49 – Liberação da porta de saída



Fonte: Próprio autor.

4.5 TESTE DO SISTEMA DE EVENTOS GERADOS

Abaixo será mostrado o funcionamento do protótipo transmitindo os eventos de disparos para a empresa de monitoramento. Lembrando que são monitorados três eventos:

- Disparos de sensor de porta aberta;
- Disparo de alarme (caso a porta seja arrombada);
- Disparo no sistema de incêndio;

Na Figura 50, é mostrado o evento de alarme de porta arrombada sendo enviado para o *software* de monitoramento.

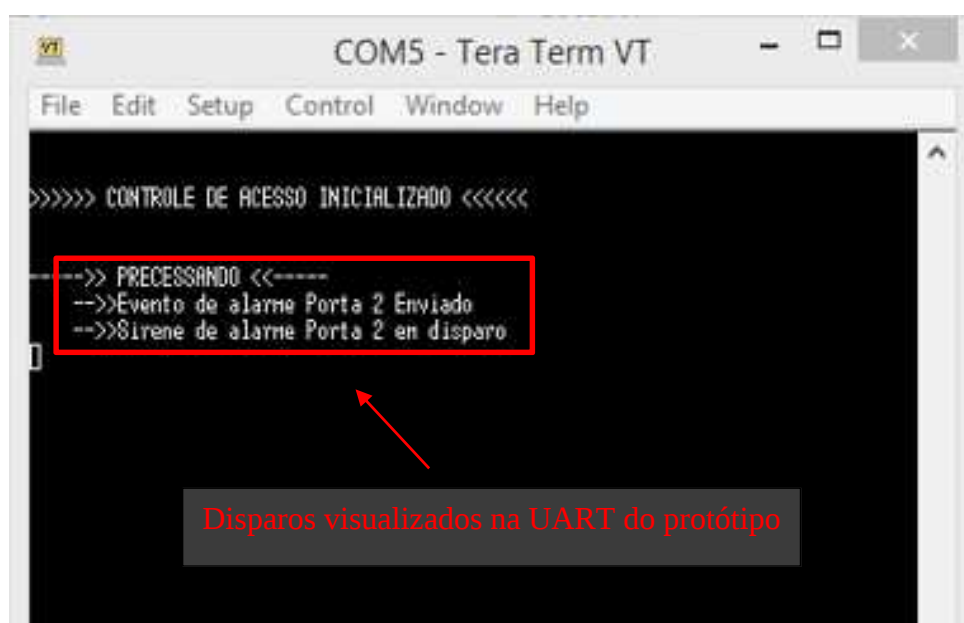
Figura 50 - Disparos dos alarmes de arrombamento recebidos pelo software de monitoramento.



Fonte: Próprio autor.

Na Figura 51, é mostrado os eventos dos alarmes gerados simultaneamente na UART do protótipo.

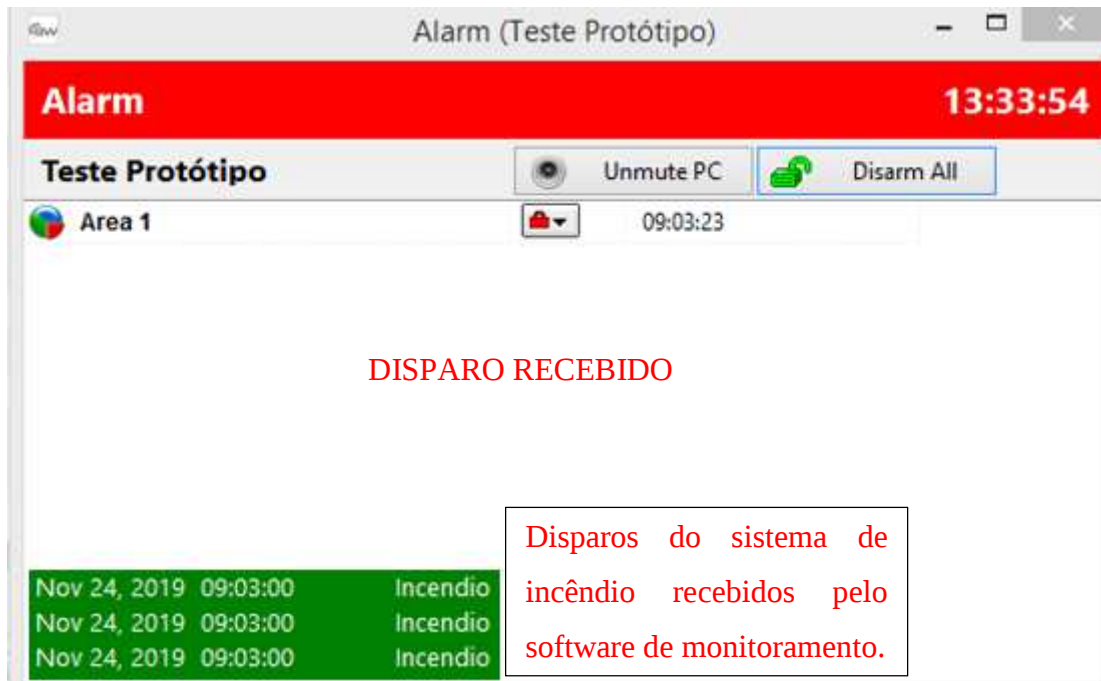
Figura 51 - Mensagens de alarmes exibidas na UART do protótipo.



Fonte: Próprio autor.

Na Figura 52, é mostrado o evento de disparo do sistema de incêndio sendo enviado para o *software* de monitoramento.

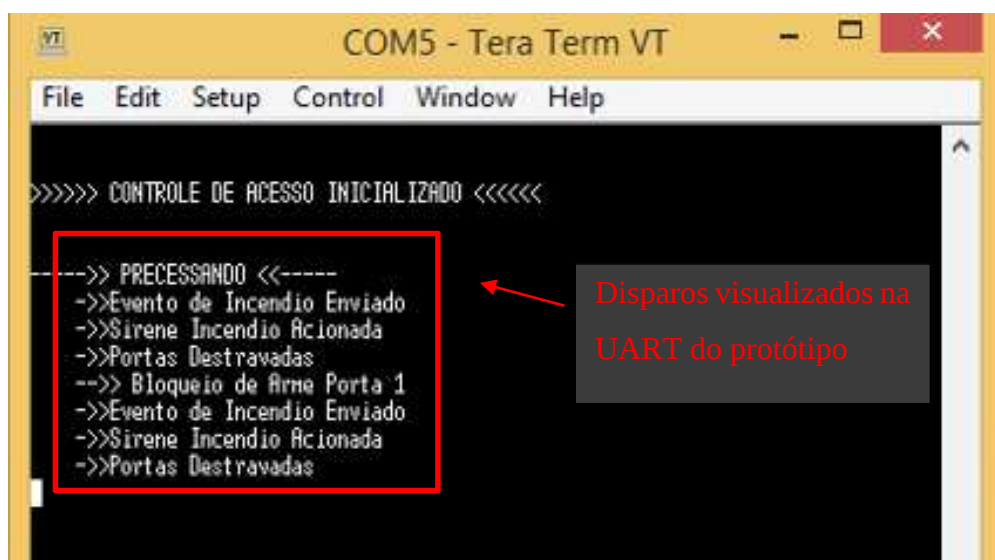
Figura 52 - Disparo do sistema de incêndio.



Fonte: Próprio autor.

Na Figura 53, é mostrado os eventos de incêndio gerados simultaneamente na UART do protótipo.

Figura 53 - Mostra os eventos de incêndio gerados pela UART.



Fonte: Próprio autor.

Na Figura 54, é mostrado o evento de porta deixada aberta sendo enviado para o *software* de monitoramento.

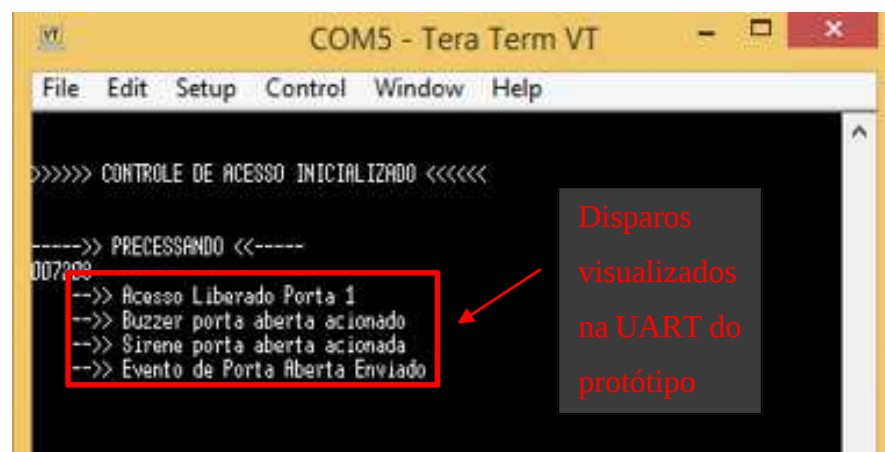
Figura 54 - Disparos do sensor de porta aberta.



Fonte: Próprio autor.

Na Figura 55, é mostrado os eventos dos alarmes de portas abertas gerados simultaneamente na UART do protótipo.

Figura 55 - Alarme de porta aberta gerados pela UART.

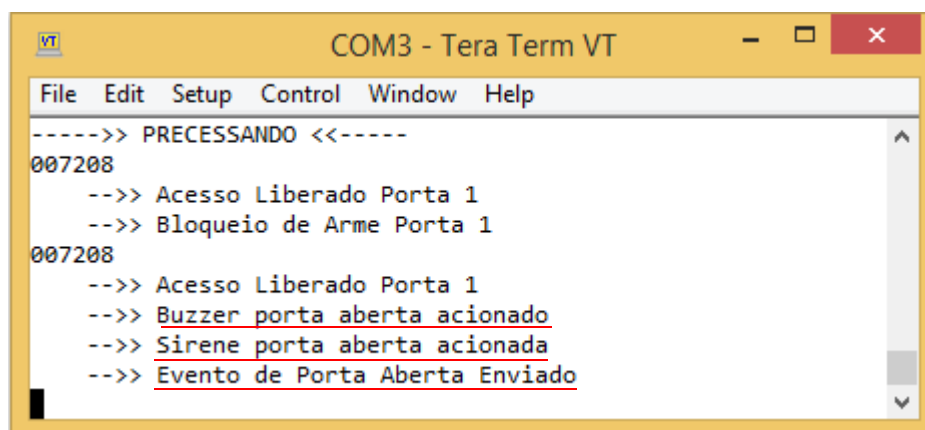


Fonte: Próprio autor.

4.6 TESTE DO SISTEMA DE DISPARO DE PORTA ABERTA

Este sistema verifica se uma das portas foi deixada aberta e faz o bloqueio da abertura da segunda, emitindo um aviso sonoro, disparando o sistema e enviando a mensagem para o monitoramento, como mostra a Figura 56.

Figura 56 – Disparo dos alarmes de porta aberta.

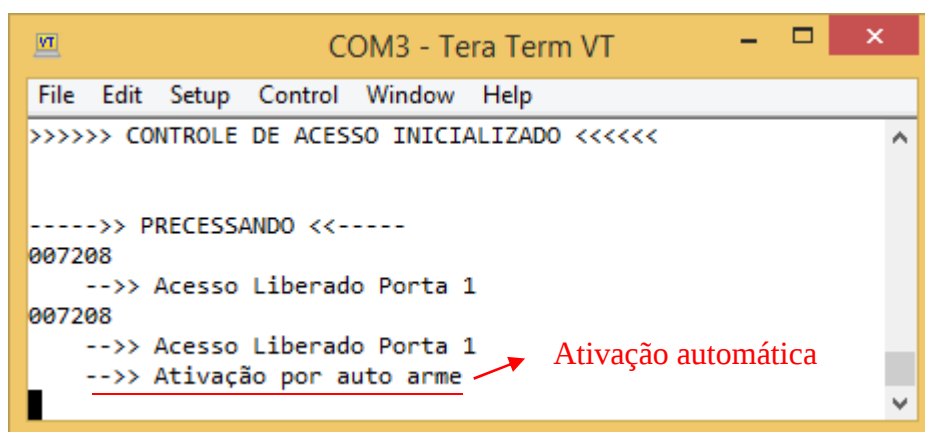


Fonte: Próprio autor.

4.7 TESTE DO SISTEMA DE REARME/AUTO ARME

O rearme é importante pois sempre mantém o sistema ativado e seguro. Ele se dá de duas formas, fechando qualquer uma das portas, ou automaticamente, se o sistema não se ativar quando fechá-las conforme mostra a Figura 57.

Figura 57 - Rearme do sistema.

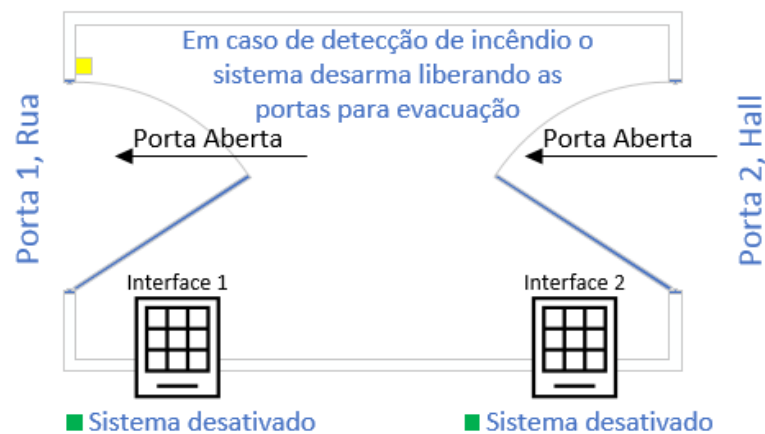


Fonte: Próprio autor.

4.8 TESTE DO SISTEMA DE INCENDIO

O sensor de detecção de fumaça tem como função fazer a liberação das portas em caso de incêndio como mostra a figura 58. Ao gerar esta detecção, o mesmo dispara fazendo com que libere as duas portas simultaneamente, desligando o sistema de alarme que às protege e possibilitando que os usuários saiam do local sem barreiras. Também o led verde é aceso simbolizando que o sistema está desarmado e liberado. As *interfaces* com os usuários e a sirene passam a fazer um som intermitente, alertando que o sistema de incêndio está em disparo. Para voltar ao seu funcionamento normal basta resetar a placa central.

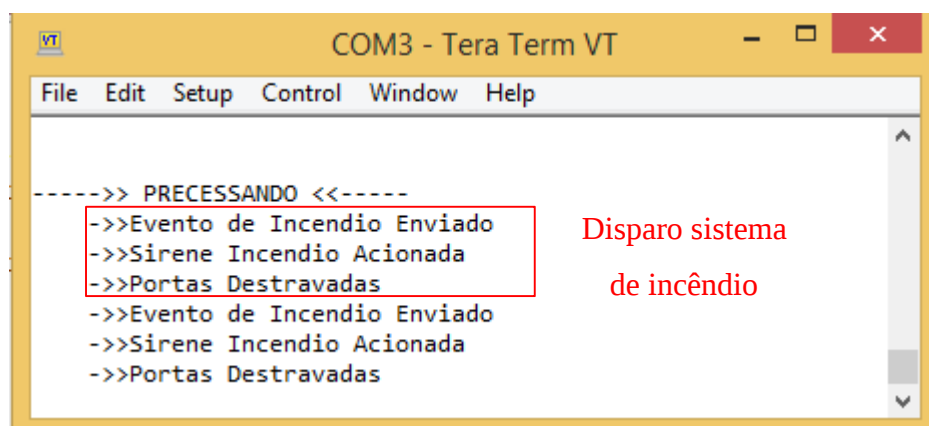
Figura 58 - Sistema de incêndio.



Fonte: Próprio autor.

Na Figura 59 é mostrado os eventos de disparos do sistema de incêndio gerados pela UART do protótipo.

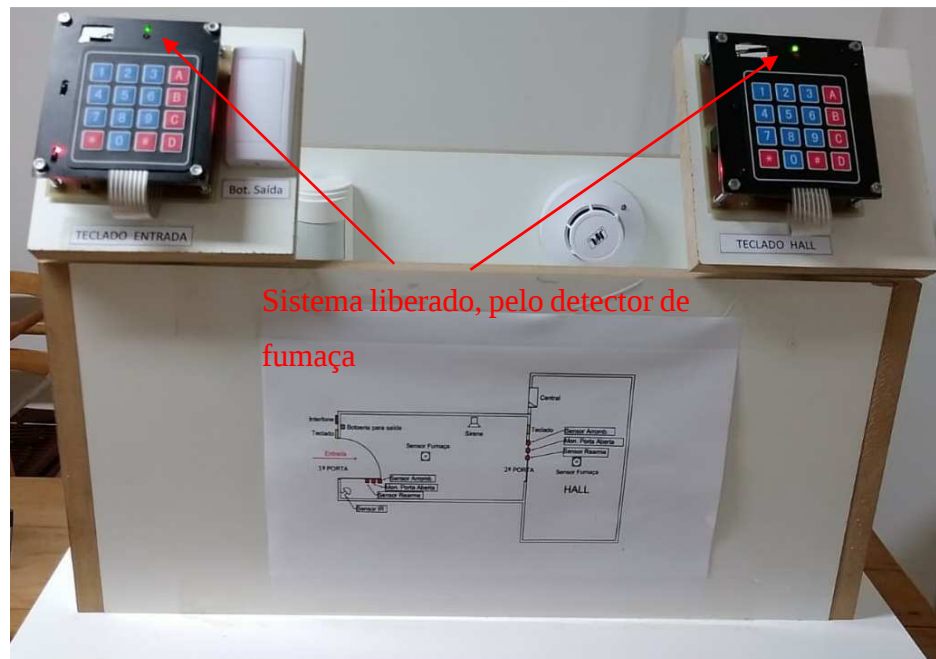
Figura 59 - Disparo de sistema de incêndio



Fonte: UART.

Na Figura 60 é mostrado os status de sistema liberado pelas *interfaces* de usuários.

Figura 60 - Liberação pelo sistema de incêndio



Fonte: Próprio autor.

4.9 IMPACTO NA SEGURANÇA CASO ALGUM COMPONENTE FALHE

Até agora foi mostrado como o sistema funciona em prol da segurança sem nenhuma falha dos dispositivos e sensores instalados. Agora será mostrado que impacto causará caso algum destes componentes venha a falhar.

- *Sensores de alarme (reed Switchs)*: estes foram instalados nas portas e tem como objetivo fazer o sistema disparar se a mesma for arrombada, mas caso venha a falhar, pode gerar disparos em falso. Por outro lado, se o contato interno não se abrir quando o ímã se afastar, o sistema que protege a porta não vai disparar. Como se trata de uma clausura, que possui mais uma porta protegida e precisa ser arrombada para entrar, ao fazer isso, o sistema vai disparar e enviar os eventos para o monitoramento.
- *Sensor rearme (reed Switch)*: se este vier a falhar ao fechar a porta, o alarme não vai se reativar, mas após decorrer o tempo de auto-arme ele se ativa automaticamente;

- *Sensor intertravamento das portas (reed Switch)*: se caso algum deles venha a falhar os usuários poderão ficar trancados dentro do local ou pelo lado de fora, não conseguindo entrar nem sair;
- *Sensor de incêndio*: se caso falhe não vai destrancar as portas, ocasionando demora na evacuação em caso de incêndio;
- *Sensor inibidor de arme (infravermelho)*: se caso falhe, vai fazer os sensores internos da clausura disparar se tiver movimentação no seu interior.
- *Placa central*: se caso falhar, todo o sistema fica inoperante;
- *Interface dos usuários*: se algum falhar o usuário será impossibilitado de entrar ou sair do local;

5 CONSIDERAÇÕES FINAIS

O projeto desenvolvido teve como desafio inicial fazer a comunicação entre as três *launchpads* (placa central e as interfaces dos usuários), para haver troca de informações entre os dispositivos. Para esta aplicação a ideia inicial era utilizar o protocolo I2C, mas devido as características das funções existentes não foi possível desabilitar a FIFO deste protocolo. Para solucionar o problema foi utilizado o protocolo UART de forma assíncrona, o qual possibilitava desabilitar a FIFO, fazendo o envio da quantidade de caracteres desejadas.

Através do desenvolvimento conjunto do *hardware* e *firmware* foi possível explorar diversas áreas da engenharia elétrica, que como consequência gerou uma ligação entre toda teoria vista no curso e a prática desenvolvida.

O protótipo não foi preparado para se tornar um produto, pois foi levado em consideração a economia e não a qualidade necessária para sua comercialização. Por exemplo, para a construção das *interfaces* com os usuários, foram utilizados materiais de baixo custo. Como não tem um bom *design*, não pode ser aplicado em locais com alto padrão de sofisticação, muito menos em locais que o deixe exposto a intempérie.

Outro desafio, já que o protótipo usa bastante funções entrelaçadas em sua programação, as quais possibilitam ou impedem o funcionamento de algumas funções do protótipo, como por exemplo, as programadas como interrupções, acabavam deixando-o lento. Para resolver o problema, foram escolhidas as funcionalidades prioritárias, que o protótipo precisa executar, tais como: disparo de alarme, disparo do sistema de incêndio, liberação das fechaduras e etc. Estas foram programadas como interrupção e o restante não sendo tão importante, como funções normais.

Com o término do projeto, verifica-se que o mesmo cumpriu com o objetivo proposto, todas as suas funcionalidades trabalham entre si em harmonia e com ótima resposta, tanto em funcionamento como em velocidade. Então pode-se concluir que o sistema apresenta as funcionalidades necessárias para ser utilizado para esta aplicação, mas, porém, tem muito a evoluir ainda para se tornar um produto, pois os componentes e layout são inapropriados para serem utilizados em uma aplicação real.

6 REFERENCIAS BIBLIOGRÁFICAS

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA. São Paulo FBSP, v.12 pg.112 e 113, agos. 2018.

ARAÚJO, José Wanderley. **Emergências Monitoradas**: segredos e técnicas aplicadas ao monitoramento de alarme. Curitiba: Editora Progressiva, 2007.

ASSISTÊNCIA SOLCIAL DIOCESANA LEÃO XIII. **Instalador de Sistemas de Segurança de Alarme Predial**. Passo Fundo, 2014.

BERNARDO, C.G. **A tecnologia RFID e os benefícios da etiqueta inteligente para os negócios**. Revista Eletrônica Unibero de Iniciação Científica, São Paulo, 2004.

BRASIL. **Constituição (1988)**. São Paulo: Ática, 1990.

BRASIL. **Lei nº 7102, de 20 de junho de 1983**. Brasília, DF, 1983.

BRASIL. **Portaria nº 3.233, de 10 de dezembro de 2012**. Brasília, DF, 2012.

BRASILIANO, A.C.R.; BLANCO L. **Planejamento tático e técnico em segurança empresarial**. 1 ed. Sicurezza: São Paulo, 2003.

BRUBEKI. **Paradox**. < <http://www.brubeki.com.br/paradox1.htm> >. Acesso em: 15/10/18 às 16:23.

CUNHA, Alessandro F. **RFID – Etiquetas com eletrônica de ponta**. SABER ELETRONICA. N 401. Junho, 2006.

FORUM DE SEGURANÇA PUBLIVA. **Anuário de Segurança Pública 2014 a 2017**. Disponível:<http://www.forumseguranca.org.br/wpcontent/uploads/2018/09/FBSP_ABSP_edicao_especial_estados_faccoes_2018.pdf>. Acesso em 15/10/18 às 14:10.

INTELBRAS. **Controle de Acesso**. < <http://www.intelbras.com.br/empresarial/controle-de-acesso/linha-corporativa/controle-de-acesso-stand-alone/sem-software>>. Acesso em: 15/10/18 às 14:31.

NETO, Zamith França. **Aplicação da tecnologia RFID para gestão acadêmica, de pessoal e operacional de patrimônio e biblioteca**. SPOLM 2008. ISSN 2175-6295. Rio de Janeiro – Brasil, 05 e 06 de agosto de 2008.

NXP, founded by Philips. UM10204: **I2C-bus specification and user manual**. EUA, rev. 3, junho 2007.

PARADOX.**Products**.

<<http://www.paradox.com/Products/default.asp?CATID=7&SUBCATID=68&PRD=158>>. Acesso em: 15/10/18 às 14:27.

PORTELLA, Aguiar, Paulo Roberto. **Gestão de Segurança 2 eds.**: História, Prevenção e Sistemas de proteção. Rio de Janeiro: Editora Rio, 2012.

PORTELLA, Aguiar, Paulo Roberto. **Gestão de Segurança**: Segurança Privada, Sistemas de Proteção, História, Metodologia e Doutrina. Rio de Janeiro: Editora Rio, 2003.

REVISTA SEGURANÇA ELETRONICA. São Paulo ABESE, v.2 pg. 39, mar. 2017.

SECRETARIA DE SEGURANÇA PÚBLICA. **Indicadores Criminais**. Disponível em:< <https://www.ssp.rs.gov.br/indicadores-criminais>>. Acesso em 16/10/18 das 14:00 às 14:30.

SOFTGUARD. **Ppa**. < http://www.softguard.com/71_ppa-compatibilidad-total-ip>. Acesso em: 15/10/18 às 16:34.

SOUZA, Marcos Antônio. **Vendendo Segurança com Segurança**.

THEVEAR. **Produtos**. < <http://www.thevear.com.br/new/VerProdutos.aspx?IDSubCat=143>>. Acesso em 15/10/18 às 16:29.

APÊNDICE A – FIRMWARE DE COMUNICAÇÃO DAS LAUNCH PADS.

```
#define GPIO_PB0_U1RX 0x00010001//TECLADO 1
```

```
#define GPIO_PB1_U1TX 0x00010401//TECLADO 1
```

```
#define GPIO_PE0_U7RX 0x00040001//TECLADO 2
```

```
#define GPIO_PE1_U7TX 0x00040401//TECLADO 2
```

```
void RecepcaoTEC1_UART(void)
```

```
{
```

```
    SysCtlPeripheralReset(SYSCTL_PERIPH_UART1);
```

```
    SysCtlPeripheralEnable(SYSCTL_PERIPH_GPIOB);
```

```
    SysCtlPeripheralEnable(SYSCTL_PERIPH_UART1);
```

```
    GPIOPinConfigure(GPIO_PB0_U1RX);
```

```
    GPIOPinConfigure(GPIO_PB1_U1TX);
```

```
    GPIOPinTypeUART(GPIO_PORTB_BASE, GPIO_PIN_0 | GPIO_PIN_1);
```

```
    UARTClockSourceSet(UART1_BASE, UART_CLOCK_SYSTEM);
```

```
    UARTFIFOLevelSet(UART1_BASE, UART_FIFO_TX1_8, UART_FIFO_RX7_8);
```

```
    UARTConfigSetExpClk(UART1_BASE, SysCtlClockGet(), 9600, (
```

```
    UART_CONFIG_PAR_ZERO|UART_CONFIG_WLEN_8
```

```
    | UART_CONFIG_STOP_ONE));
```

```
    UARTIntEnable(UART1_BASE, UART_INT_RT);
```

```
    IntEnable(INT_UART1_TM4C123);
```

```
    IntRegister(INT_UART1_TM4C123, UART1_IntHandler);
```

```
}
```

```
void RecepcaoTEC2_UART(void)
```

```
{
```

```
    SysCtlPeripheralReset(SYSCTL_PERIPH_UART7);
```

```
    SysCtlPeripheralEnable(SYSCTL_PERIPH_GPIOE);
```

```
    SysCtlPeripheralEnable(SYSCTL_PERIPH_UART7);
```

```
    GPIOPinConfigure(GPIO_PE0_U7RX);
```

```
    GPIOPinConfigure(GPIO_PE1_U7TX);
```

```
    GPIOPinTypeUART(GPIO_PORTE_BASE, GPIO_PIN_0 | GPIO_PIN_1);
```

```

UARTClockSourceSet(UART7_BASE, UART_CLOCK_SYSTEM);
UARTFIFOLevelSet(UART7_BASE, UART_FIFO_TX1_8, UART_FIFO_RX7_8);
UARTConfigSetExpClk(UART7_BASE,      SysCtlClockGet(),      9600,      (
UART_CONFIG_PAR_ZERO|UART_CONFIG_WLEN_8
| UART_CONFIG_STOP_ONE));
UARTIntEnable(UART7_BASE,UART_INT_RT);
IntEnable(INT_UART7_TM4C123);
IntRegister(INT_UART7_TM4C123,UART7_IntHandler);
}

```

APÊNDICE B – TRECHO DO FIRMWARE DAS INTERFACES DOS USUÁRIOS.

```
#define GPIO_PB0_U1RX 0x00010001
#define GPIO_PB1_U1TX 0x00010401
#define GPIO_PC6_U3RX 0x00021801
#define GPIO_PC7_U3TX 0x00021C01
#define GPIO_PA0_U0RX 0x00000001
#define GPIO_PA1_U0TX 0x00000401
```

```
void ConfigureUART_RFID(void)
{
    SysCtlPeripheralReset(SYSCTL_PERIPH_UART1);
    SysCtlPeripheralEnable(SYSCTL_PERIPH_GPIOB);
    SysCtlPeripheralEnable(SYSCTL_PERIPH_UART1);
    GPIOPinConfigure(GPIO_PB0_U1RX);
    GPIOPinConfigure(GPIO_PB1_U1TX);
    GPIOPinTypeUART(GPIO_PORTB_BASE, GPIO_PIN_0|GPIO_PIN_1);
    UARTClockSourceSet(UART1_BASE, UART_CLOCK_SYSTEM);
    UARTFIFOLevelSet(UART1_BASE, UART_FIFO_TX6_8, UART_FIFO_RX6_8);//
    UARTFIFODisable(UART1_BASE);//tamanho do buffer de 8 posições//
    UARTConfigSetExpClk(UART1_BASE, SysCtlClockGet(), 9600, (
UART_CONFIG_PAR_NONE|UART_CONFIG_WLEN_8
| UART_CONFIG_STOP_ONE));
    UARTIntEnable(UART1_BASE,UART_INT_RT);
    IntEnable(INT_UART1_TM4C123);
    IntRegister(INT_UART1_TM4C123,UART1_IntHandler);
}
```

```
void TransmisaoUART(void)
{
    SysCtlPeripheralEnable(SYSCTL_PERIPH_GPIOC);
    SysCtlPeripheralEnable(SYSCTL_PERIPH_UART3);
    GPIOPinConfigure(GPIO_PC6_U3RX);
    GPIOPinConfigure(GPIO_PC7_U3TX);
```

```

GPIOPinTypeUART(GPIO_PORTC_BASE, GPIO_PIN_6|GPIO_PIN_7);
UARTClockSourceSet(UART3_BASE, UART_CLOCK_SYSTEM);
UARTFIFOLevelSet(UART3_BASE, UART_FIFO_TX7_8, UART_FIFO_RX1_8);//
UARTConfigSetExpClk(UART3_BASE,      SysCtlClockGet(),      9600,      (
UART_CONFIG_PAR_ZERO|UART_CONFIG_WLEN_8
| UART_CONFIG_STOP_ONE));
UARTIntEnable(UART3_BASE,UART_INT_RT);
IntEnable(INT_UART3_TM4C123);
IntRegister(INT_UART3_TM4C123,UART3_IntHandler);
}

```

APÊNDICE C – TRECHO DO FIRMWARE DO CADASTRO DAS SENHAS.

```

void option_7(void)
{
    eeprom_check();
    uint32_t numeros[6], primeiro;

    UARTprintf("\n\tDigite o endereco de 10 a 40: ");
    do
    {
        primeiro=UARTDecGet(UART0_BASE);
        if((primeiro!=10)&&(primeiro!=20)&&(primeiro!=30)&&(primeiro!=40))
        {
            UARTprintf("\n\tEsse endereco nao existe!!\n");
            UARTprintf("\n\tDigite o endereco de 10 a 40: ");
        }
    }
    while((primeiro!=10)&&(primeiro!=20)&&(primeiro!=30)&&(primeiro!=40));
    UARTprintf("\n\tDigite a senha com 6 digitos:\n ");
    UARTprintf("\t>>Senha: ");
    for ( int i=1; i<=6; i++)
    {
        // UARTprintf("\t>>Senha: ");
        numeros[i-1]=UARTCharGet(UART0_BASE)-48;
        UARTprintf("%d",numeros[i-1]);
        //if(((i%10)==0)|(i%10)==5) UARTprintf("\n\t\t\t ");
    }
    if(i==6) i=1;

    EEPROMProgram(numeros, primeiro*4,sizeof(numeros));
    SysCtlDelay(2000000);
    UARTprintf("\n\n\tGravado.");
}

```

APÊNDICE D – FIRMWARE DE PROTEÇÃO DA INTERFACE DE AJUSTES.

```

void Senha_Inst(void)
{
    uint32_t teste[10],h;
    int i,f=0;
    //Menu senha
    UARTprintf("\x1B[2J");
    UARTprintf("\x1B[0;0H");
    UARTprintf("\n\n>>> CONTROLE DE ACESSO PARADO <<<\n\n");
    UARTprintf("\n>>>>> CONTROLE DE ACESSO <<<<<\n");
    UARTprintf("\n Para acessar menu Digite a senha\n ");
    UARTprintf("-----\n ");
    UARTprintf("      Senha:");
    //recebimento da senha
    h=UARTDecGet(UART0_BASE);
    EEPROMRead(teste, 0, sizeof(teste));
    for (i=0;i<2;i++)
    {
        if(teste[i]==h)
        {
            f=5;
        }
    }
    //senha igual executa
    if(f==5) // se a tentativa for igual
    {
        UARTprintf("\x1B[2J");
        UARTprintf("\x1B[0;0H");
        exe=1;//>> entra laço menu
        f=0;
    }
    //senha diferente retorna
    else // se a tentativa for diferente

```

```
{  
    UARTprintf("\n\nSenha Errada");  
    delay(),delay(),delay();  
    UARTprintf("\x1B[2J");  
    UARTprintf("\x1B[0;0H");  
    f=0;  
    sen=0;///  
    > permanece no laço senha  
    exe='s';  
}  
}
```

APÊNDICE E – TRECHO DO FIRMWARE DE COMPARAÇÃO DE TAGS, SENHAS.

```

void UART1_IntHandler(void)
{
    if(BC==0)
    {
        //Recebe a senha ou TAG
        UARTIntClear(UART1_BASE,UART_INT_RT);
        if(LEI1==0)
        {
            for (i=0; i<6; i++)
            {
                Receb[i]=UARTCharGet(UART1_BASE)-48;
                UARTprintf("%d",Receb[i]);

            }
            //if(i==6) i=0;
            UARTprintf("\n");
            //Verifica se está cadastrada
            for(int z=1;z<=9;z++)
            {
                c=0;
                EEPROMRead(senh,z*40, sizeof(senh));
                for (j=0;j<6;j++)
                {
                    if(Receb[j]==senh[j]) c++;
                }
                if(c==6 && EC2==0&&LEI1==0)
                {
                    LEI1=1;
                    UARTprintf("  --> Acesso Liberado Porta 1\n");
                    UARTCharPutNonBlocking(UART1_BASE,0x31);
                    m=1;
                    //lib_port1=1;
                }
            }
        }
    }
}

```

```

    AR1=1;
    LEDS=BLUE;
    FE1=0x08;
    //UARTprintf("  -->> Porta 1 liberada\n");
    tempo_fechadura1();
    FE1=0x00;
    LEDS=0;
    SysCtlDelay(4000000);
    HU=0;
    //lib_port1=0;
    AUT1=1; //HABILITA AUTO ARME PORTA 1
    //LEI=0;
}
if(c==6 && EC2==1)
{
    m=2;
}
}

if((c!=6&& m==0&& LEI1==0)|| (m==2))
{
    LEI1=1;
    UARTprintf("  --<< Acesso Negado Porta 1 >> --\n");
    SysCtlDelay(2000000);
    UARTCharPutNonBlocking(UART1_BASE,0x32);
}
}
SysCtlDelay(9000000);
LEI1=0;
m=0;
}
}

```

APÊNDICE F – LIGAÇÃO DOS DISPOSITIVOS NO SISTEMA

