



Universidade de Taubaté
Autarquia Municipal de Regime Especial pelo
Dec. Fed. nº 78.924/76 Recredenciada
Reconhecida pelo CEE/SP
CNPJ 45.176.153/0001-22

Departamento de Engenharia Elétrica
Rua Daniel Danelli s/nº Jardim Morumbi
Taubaté-Sp 12060-440
Tel.: (12) 3625-4190
e-mail: eng.eletrica@unitau.br

FERNANDO LÉO BUENO DE OLIVEIRA E SILVA

**SISTEMA DE CONTROLE DE ACESSO PARA
ESTACIONAMENTO**

TAUBATÉ - SP

2018



Universidade de Taubaté
Autarquia Municipal de Regime Especial pelo
Dec. Fed. nº 78.924/76 Recredenciada
Reconhecida pelo CEE/SP
CNPJ 45.176.153/0001-22

Departamento de Engenharia Elétrica
Rua Daniel Danelli s/nº Jardim Morumbi
Taubaté-Sp 12060-440
Tel.: (12) 3625-4190
e-mail: eng.eletrica@unitau.br

FERNANDO LÉO BUENO DE OLIVEIRA E SILVA

***SISTEMA DE CONTROLE DE ACESSO PARA
ESTACIONAMENTO***

Trabalho de Graduação apresentado ao Departamento de Engenharia Elétrica da Universidade de Taubaté, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Elétrica.

Orientador: Prof. Rubens Castilho

TAUBATÉ - SP

2018



Universidade de Taubaté
Autarquia Municipal de Regime Especial
pelo Dec. Fed. nº 78.924/76
Recredenciada Reconhecida pelo CEE/SP
CNPJ 45.176.153/0001-22

Departamento de Engenharia Elétrica
Rua Daniel Danelli s/nº Jardim Morumbi
Taubaté-Sp 12060-440
Tel.: (12) 3625-4190
e-mail: eng.eletrica@unitau.br

SISTEMA DE CONTROLE DE ACESSO PARA ESTACIONAMENTO

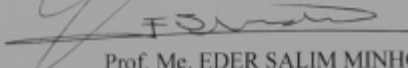
FERNANDO LÉO BUENO DE OLIVEIRA E SILVA

ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE DO REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE "GRADUADO EM ENGENHARIA ELÉTRICA"

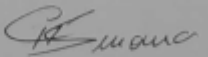
BANCA EXAMINADORA:



Prof. RUBENS CASTILHO JUNIOR
Orientador/UNITAU-DEE



Prof. Me. EDER SALIM MINHOTO
UNITAU-DEE



Eng. CARLOS HENRIQUE SILVA MOURA
Membro Externo

novembro de 2018

S586s Silva, Fernando Léo Bueno de Oliveira e
Sistema de controle de acesso para estacionamento / Fernando Léo
Bueno de Oliveira e Silva. -- 2018.
110 f. : il.

Monografia (graduação) – Universidade de Taubaté, Departamento de
Engenharia Mecânica e Elétrica, 2018.

Orientação: Prof. Rubens Castilho Junior, Departamento de Engenharia
Elétrica.

1. Automatização de estacionamento. 2. Controle de acesso veicular.
3. Identificador de rádio frequência. 4. RFID. 5. Sistema de controle de
acesso. I. Título. II. Graduação em Engenharia Elétrica e Eletrônica.

CDD – 621.384

SIBi – Sistema Integrado de Bibliotecas / UNITAU

Ficha catalográfica elaborada por Shirlei Righeti – CRB-8/6995

DEDICATÓRIA

Este trabalho é dedicado à Denise Ap. Léo Bueno e Fernando de Oliveira e Silva, pois sem eles não teria as chances e oportunidades que tive.

AGRADECIMENTOS

Agradeço a esta Universidade e todo o seu corpo docente que me proporcionaram as condições necessárias para que alcançasse meus objetivos. Agradeço em especial ao orientador Rubens Castilho Junior, por toda a sua dedicação que direcionou minha pesquisa a fim de se atingir os resultados esperados, ao meus pais por todo o apoio e suporte ao longo desta jornada de formação em Engenharia Elétrica e Eletrônica. Enfim, a todos que contribuíram para a realização deste trabalho, seja de forma direta ou indireta, registro o meu muitíssimo obrigado.

“Não importa quanto a vida possa ser ruim, sempre existe algo que você possa fazer e triunfar.” (Stephen Hawking)

RESUMO

Estudaremos nesta dissertação a implementação de um projeto de sistema de controle para uma instituição de ensino pelo método de identificação por RFID, contendo informações sobre as pessoas da instituição e seus bens, resolvendo uma série de problemas. O objetivo desta implementação está diretamente ligado as melhorias do fluxo de automóveis e motocicletas que causam um sério problema de organização e segurança e ainda possibilitar uma forma ideal de identificação das pessoas que entram e saem da instituição. Além de reduzir as chances de furtos e roubos dos automóveis e motocicletas das mesmas. Comentaremos sobre os tipos de sistemas de controle, que são os mais diversos atualmente, devido as novas tecnologias do mercado, o porquê do uso do sistema por RFID, suas vantagens e desvantagens e como poderá ser feita sua implementação. Apresentaremos a parte física do projeto, a parte lógica e de programação e uma estipulação de quanto o projeto poderá custar.

PALAVRAS-CHAVE: Controle de acesso. RFID. Identificação.

ABSTRACT

We will study in this dissertation the implementation of a control system project for an educational institution through the RFID identification method, containing information about the people of the institution and its assets, solving a series of problems. The purpose of this implementation is directly linked to improvements in the flow of automobiles and motorcycles that cause a serious problem of organization and security and also provide an ideal way of identifying the people who enter and leave the institution. In addition to reducing the chances of thefts and thefts of automobiles and motorcycles of the same. We will comment on the types of control systems, which are the most diverse currently, due to the new technologies in the market, the use of the RFID system, their advantages and disadvantages and how they can be implemented. We will present the physical part of the project, the logical and programming part and a stipulation of how much the project could cost.

KEYWORDS: Access control. RFID. Identification

LISTA DE FIGURAS

Figura 1 - Diagrama dos níveis de controle de acesso	23
Figura 2 - Cartão de proximidade.....	25
Figura 3 - Smart Card.....	26
Figura 4 - Cartão magnético	26
Figura 5 - Cartão de código de barras	26
Figura 6 - Leitor de digitais	27
Figura 7 - Sensor biométrico para as mãos.....	27
Figura 8 - Scanner de retina	28
Figura 9 - Scanner da íris	28
Figura 10 - Scanner de Voz.....	28
Figura 11 - Scanner de assinatura	29
Figura 12 - QR Code.....	30
Figura 13 - Usuário e senha.....	30
Figura 14 – Token	31
Figura 15 - Onda plana se propagando no espaço.....	33
Figura 16 - Regra da mão direita para identificação do Vetor de Poynting.....	35
Figura 17 - Banda de Frequência do RFID	41
Figura 18 - Faixas de banda no mundo para RFID em UHF.....	43
Figura 19 - Princípio de funcionamento de um acoplamento indutivo	44
Figura 20 - Princípio de funcionamento de um acoplamento Backscatter ou capacitivo	45
Figura 21 - Componentes de uma TAG	45
Figura 22 - TAG adesiva de UHF	46
Figura 23 - Exemplos de Tags passivas para UHF.....	47
Figura 24 - Princípio de Mestre-Escravo	48
Figura 25 - Exemplo de Leitoras UHF (Esquerda) e HF (Direita).....	49
Figura 26 - Polarização Linear (Esquerda) e Circular (Direita).....	51
Figura 27 - Exemplos de antenas de tags para determinadas frequências	52
Figura 28 - Componentes de um sistema RFID	52
Figura 29 - Sistemas Full Duplex, Half Duplex e Sequencial no tempo	53
Figura 30 - Alimentação da tag a partir do acoplamento indutivo	54
Figura 31 - Operação de uma tag com acoplamento capacitivo ou backscatter	55
Figura 32 - Circuito equivalente de um sistema RFID com acoplamento capacitivo	55
Figura 33 - Família de padrões para cartões inteligentes com e sem contato	56
Figura 34 - Formato de um código EPC.....	58
Figura 35 - Microcontrolador Arduino Uno.....	62
Figura 36 - Módulo MFRC522.....	63
Figura 37 - Tag's de 13,56Mhz.....	63
Figura 38 - Buzzer	64
Figura 39 - LED's	65
Figura 40 - Resistores	66
Figura 41 - Jumpers	66
Figura 42 - Fluxograma do protótipo	67
Figura 43 - Protótipo	68
Figura 44 - Campus JUTA com vista superior	69
Figura 45 - Componentes do projeto	70
Figura 46 - Módulo guarita.....	72

Figura 47 - Multiconversor	73
Figura 48 - Módulo Botoeira	74
Figura 49 - Receptor CTW-4	75
Figura 50 - Leitor L101 - A	76
Figura 51 - Controladora LN5 - P	76
Figura 52 - Sistema detector por laço indutivo	77
Figura 53 - Cancela Automática	78
Figura 54 - Software HCS 2010.....	79
Figura 55 - Central de laço indutivo	80
Figura 56 - Esquema físico do projeto.....	81
Figura 57 - Fluxograma do processo de inicialização	83
Figura 58 - Fluxograma do procedimento de entrada	84
Figura 59 - Fluxograma do procedimento de saída.....	85
Figura 60 - Barra de status	91
Figura 61 - Monitoramento On-line Linear HCS.....	92
Figura 62 - Programação do módulo guarita	93
Figura 63 - Identificação modulo guarita	94
Figura 64 - Labels do software Linear HCS.....	94
Figura 65 - Leitura dos eventos	95
Figura 66 - Leitura dos dispositivos.....	96
Figura 67 - Relatório de eventos	97
Figura 68 - Relatório de dispositivos	98
Figura 69 - Pré-visualização.....	98
Figura 70 - Gerenciador de dispositivos.....	99
Figura 71 - Gerenciar dispositivos Off-line.....	104
Figura 72 - Aviso de erro	105
Figura 73 - Teste da porta serial.....	106

LISTA DE TABELAS

Tabela 1 - Tabela com as expressões de α e k para meios com e sem perdas	36
Tabela 2 - Tabela de comparação de algumas Tecnologias de identificação	38
Tabela 3 - Tabela com a frequência, características e aplicações do RFID	42
Tabela 4 - Tabela indicativa de vagas.....	69
Tabela 5 - Tabela de valores dos componentes.....	86

Lista de termos e abreviaturas

AAR – *Association of American Railroads*. Associação da indústria ferroviária dos EUA.

CONTRAN – Conselho Nacional de Trânsito do Brasil do Brasil.

dB – Abreviatura para Decibel, que é uma unidade logarítmica de medida que expressa a magnitude de uma grandeza física relativa a um determinado nível de referência.

dBm – Ganho em decibéis relativo a uma referência de 1 miliwatt.

CI – Circuito Integrado.

CRC16 – *Cyclic Redundancy Check*, ou verificação de redundância cíclica. É um código detector de erros que gera um valor expresso em 16 bits em função de um bloco maior de dados.

EAN – *European Article Numbering*. Padrão de simbologia de código de barras usado na Europa.

EAS – *Electronic Article Surveillance*. Tecnologia para identificar roubo de produtos em lojas de varejo.

EIRP – *Effective Isotropic Radiated Power*. É uma medida da potência da antena de uma leitora usada nos Estados Unidos, normalmente expressa em Watts. $EIRP = 1.64 ERP$.

EPC – *Electronic Product Code*. Padrão para identificação única de produtos.

ETSI – *European Telecommunications Standards Institute*. Organização independente cuja missão é definir e regulamentar padrões de telecomunicações na Europa.

FCC – *Federal Communications Commission*. Agência ligada ao congresso dos EUA para regular as comunicações via rádio, televisão, cabo e satélite nos EUA.

HF – *High Frequency*. Faixa de alta frequência que compreende a faixa de 3 MHz a 30 MHz, sendo 13.56 MHz a frequência típica usada em RFID nesta faixa.

Inlay – Uma *tag* completamente montada em um substrato, ainda não pronta para o uso.

Inlet – Um *inlay*.

ISM – *Industrial, Scientific, and Medical*. Sigla para a faixa de frequência de 2.4 GHz que é aceita mundialmente para uso em equipamentos da área industrial científica e médica.

ISO – *International Organization for Standardization*. A ISO é uma entidade não governamental formada por rede dos institutos nacionais de padrões de 46 países, na base de um membro por país, com secretariado sediado em Genebra, na Suíça.

LF – *Low Frequency*. Faixa de baixa frequência que compreende a faixa de 30 kHz a 300 kHz, sendo 125kHz a frequência típica usada em RFID nesta faixa.

RF – Rádio frequência.

RFID – Identificação por Radiofrequência.

SINIAV – Sistema Nacional de Identificação Automática de Veículos.

SO – Sistema operacional.

Tag – Etiqueta eletrônica que contém um microchip.

Transponder – uma *tag* que pode atuar tanto como transmissor como receptor. Na prática, é comum usar *transponder* como sinônimo de *tag*.

UCC – *Uniform Code Council*. Organização que administrava o UPC nos EUA.

UHF – *Ultra High Frequency*. Faixa de altíssima frequência que compreende a faixa de 300 MHz a 3 GHz, sendo 915 MHz a frequência típica usada em RFID para sistema UHF passivos nos EUA e Brasil, e 868 MHz na Europa. Para sistemas ativos, as frequências típicas são 315 MHz e 433 MHz.

UPC – *Uniform Product Code*. Sistema popular de código de barras usado nos EUA.

SoC - *System On Chip* ou, em português, sistema-em-um-chip, se refere a todos os componentes de um computador, ou qualquer outro sistema eletrônico, em um circuito integrado (*chip*).

RAM - A Memória de acesso aleatório (do inglês *Random Access Memory*, frequentemente abreviado para *RAM*) é um tipo de memória que permite a leitura e a escrita, utilizada como memória primária em sistemas eletrônicos digitais.

NOR flash - A memória *flash NOR* (*Not OR*) permite acessar os dados da memória de maneira aleatória, com alta velocidade.

PROM - Uma *PROM* (do inglês *programmable read-only memory*) ou *OTP NVM* (*one-time programmable non-volatile memory*) é uma memória programável só de leitura. É uma forma de memória digital onde o estado de cada bit está trancado por um fusível ou antifusível.

BIOS - O *BIOS* (um acrônimo de *Basic Input/Output System*, em português Sistema Básico de Entrada/Saída, e também conhecido como *System BIOS*, *ROM BIOS* ou *PC BIOS*) é um firmware não-volátil usado para realizar a inicialização do hardware durante o processo de inicialização (por meio do botão de inicialização da máquina) e para fornecer serviços de tempo de execução para sistemas operacionais e programas.

RTOS - Sistema Operacional de Tempo Real (RTOS da sigla anglo-saxónica *Real Time Operating System*) é um sistema operacional/operativo destinado à execução de múltiplas tarefas onde o tempo de resposta a um evento (externo ou interno) é pré-definido.

IEC - A Comissão Eletrotécnica Internacional (*International Electrotechnical Commission*) é uma organização internacional de padronização de tecnologias elétricas, eletrônicas e relacionadas. Alguns dos seus padrões são desenvolvidos juntamente com a Organização Internacional para Padronização (ISO).

MIFARE - É a marca comercial da *NXP Semiconductors* de uma série de chips amplamente utilizados em *smart card* sem contato e cartões de proximidade.

NTAG - O NTAG® é uma família de produtos de circuito integrado sem fio de comunicação de campo próximo produzidos pela *NXP Semiconductors* que aderem aos padrões publicados pelo *NFC Forum*.

CAN - é um protocolo de comunicação serial síncrono. O sincronismo entre os módulos conectados à rede é feito em relação ao início de cada mensagem lançada ao barramento (evento que ocorre em intervalos de tempo conhecidos e regulares).

Sumário

1 - Introdução.....	19
1.1 – Objetivo.....	19
1.2 – Organização do trabalho.....	19
1.3 - Motivação.....	19
2 – Revisão Bibliográfica.....	20
2.1 – Conceito sobre segurança privada.....	20
2.2 – Objetivos do sistema de controle de acesso.....	21
2.3 – Controle de acesso físico.....	24
2.3.1 - Controle de acesso mecânico.....	24
2.3.2 – Controle de acesso eletrônico.....	25
2.3.2.1 – Equipamentos existentes para o controle de acesso eletrônico.....	25
2.4 - Controle de acesso lógico.....	29
2.4.1 - Elementos do controle de acesso lógico.....	30
3 - RFID.....	32
3.1 - Propriedade das ondas eletromagnéticas.....	32
3.2 – Comparação com outras tecnologias.....	37
3.3 – História do RFID.....	38
3.4 – Faixas de frequência e tipos de acoplamento.....	41
3.5 – Tipos de acoplamento.....	43
3.5.1 – Acoplamento indutivo.....	43
3.5.2 – Acoplamento capacitivo ou <i>Backscatter</i>	44
3.6 - TAGs.....	45
3.6 – Leitoras.....	47
3.7 – Antenas.....	50
3.8 – Operação do RFID.....	52
3.9 – Padrões e Protocolos.....	56
3.10 – Aplicações do RFID.....	59
4 – Projeto.....	61
4.1 – Protótipo.....	61
4.1.2 - Microcontrolador.....	61
4.1.3 – Módulo RFID RC522.....	62
4.1.4 – Tag’s de 13,56Mhz.....	63
4.1.5 – Buzzer.....	63
4.1.6 – LED.....	64

4.1.7 – Resistores	65
4.1.8 – Jumpers	66
4.1.9 – Funcionamento	66
4.1.10 – Resultado.....	67
4.2 – Estudo do caso específico	68
4.3 – Projeto Final	69
4.3.1 – Modulo Guarita	70
4.3.1 – Multiconversor	73
4.3.2 – Módulo Botoeira	73
4.3.3 – Receptor CTW-4	74
4.3.4 - Leitor <i>RFID Wiegand</i> L101-A	75
4.3.5 – Controladora digital de acesso LN5 – P.....	76
4.3.6 – Laço indutivo	77
4.3.7 – Cancela automática	77
4.3.8 – Software de cadastro, controle e monitoramento	78
4.3.9 – Sistema anti <i>by-pass</i>	79
4.3.10 – Esquemática do projeto	81
4.3.11 – Fluxogramas do sistema de controle de acesso.....	82
4.3.12 – Planilha de custos.....	86
5 – Conclusão	87
Anexos e apêndices.....	88
Referências bibliográficas	107

1 - Introdução

1.1 – Objetivo

O objetivo deste trabalho é elaborar um projeto de controle de entrada e saída de automóveis e motocicletas da instituição de ensino juntamente com o estudo da tecnologia de Identificação por Radiofrequência (RFID) e a verificação da viabilidade, com estudo de caso e coleta de preços, do seu uso em cancelas eletrônicas como forma de controlar e monitorar o estacionamento da instituição.

Para esta análise, será desenvolvido um protótipo de catraca eletrônica com a tecnologia de RFID, envolvendo a análise de alguns modelos de dispositivos e equipamentos, bem como a definição do layout do protótipo. O desenvolvimento do protótipo físico do sistema RFID e as pesquisas que foram realizadas, utilizarão uma metodologia que também será desenvolvida.

1.2 – Organização do trabalho

A estrutura do trabalho será organizada da seguinte forma:

- No capítulo 2 será apresentado a revisão bibliográfica, abordando a base de informações para o projeto;
- No capítulo 3 será apresentado todas as informações sobre RFID;
- No capítulo 4 será apresentado a elaboração do protótipo, lista e explicação dos componentes para o projeto final e tabela de valores;
- No capítulo 5 será apresentado à conclusão.

1.3 - Motivação

A principal motivação deste projeto foi a falta de segurança que existe em nossa instituição de ensino. Embora haja funcionários em ambas portarias não existe um sistema de controle de acesso que permita a identificação de alunos, funcionários e tampouco seus veículos utilizados. Há também, relatos sobre furtos de automóveis e motocicletas dentro do limite da instituição causando, ao meu ver, um certo receio nos alunos e funcionários de estacionar seus veículos em seu estacionamento.

2 – Revisão Bibliográfica

2.1 – Conceito sobre segurança privada

Segurança pode ser definida como sendo o estado, qualidade, condição daquilo que está seguro ou isento de perigo (MANDARINI, 2005).

A atividade de segurança privada não substitui nem concorre com a Segurança Pública apenas a complementa e atua onde a pública não possa operar normalmente, onde apresente deficiência ou onde sua ação não seja conveniente. Assim a Atividade de Segurança deve ser praticada de forma prioritária, mas não exclusiva para esfera privada dos ativos ou pessoas que se busca salvaguardar e, sem constrangimentos, explorar ao máximo a Segurança Pública disponível, sempre que possível, aconselhável ou pertinente (MANDARINI, 2005).

A segurança privada visa proteger pessoas e ativos no ambiente que não é pertinente que a segurança pública o faça. No ambiente corporativo exige participação integrada de toda empresa ou instituição em cada área e imbricada no próprio processo empresarial ou institucional. Mais do que apenas tentar reduzir a ocorrência de danos isoladamente é necessário também organizar todo o esforço corporativo a ser estabelecido nesse sentido, desta forma é aberta a discussão sobre o custo que eventuais danos poderão ocasionar e os recursos necessários para mitigar as possíveis perdas resultantes, desta forma, os recursos que seriam desembolsados com eventuais perdas, que passarão a ser evitadas, são investidos em ações necessárias para evitá-las (MANDARINI, 2005).

Toda organização funciona segundo normas de um caráter geral que orientam suas atividades administrativas e operacionais, da mesma forma as políticas de segurança devem ser estabelecidas com normas expressas e claras formalizadas em documento próprio avaliado, aprovado e apoiado pela alta gestão. Em suma a segurança corporativa trata das ações de segurança a serem tomadas no ambiente das empresas, portanto nesse ambiente há uma preocupação com a segurança das pessoas dos ativos.

Em termos de segurança, ativo é todo e qualquer item que possa ser economicamente considerado, ao qual possa ser estimado um valor. Os ativos podem ser tangíveis ou intangíveis, os quais se diferenciam por:

- **Ativos tangíveis:** São os patrimônios produtivos como instalações, máquinas e equipamentos, produtos acabados, matérias primas estocadas, sistemas de informática ou patrimônios financeiros como recursos, aplicações e ações;
- **Ativos intangíveis:** São considerados intangíveis o patrimônio social e institucional, como as pessoas (recursos humanos), meio ambiente, imagem, segredos da empresa, planejamentos, estratégias, dados, conhecimentos, processos, logística, mercado marcas, fornecedores e clientes.

A segurança privada é dividida em níveis, os quais integrados entre si constituem um sistema de segurança, segundo MANDARINI (2005) esses níveis são:

- **Nível institucional (ou estratégico):** Envolve toda a empresa, porém está mais identificado com a alta administração. Neste nível são elaboradas a filosofia e políticas de segurança e definida a missão do departamento responsável;

- **Nível departamental (ou tático):** Busca a otimização dos recursos. É desenvolvido nos níveis organizacionais intermediários e estabelece os meios necessários para implantação de sistema de segurança integrado. Detalha condições, prazos e responsabilidades.

- **Nível executivo (ou técnico):** Trata da descrição técnica detalhada do sistema integrado, como também de seus equipamentos, manutenção, instalação e equipes de operação e reparos;

- **Nível operacional:** Trata do manual de operações de segurança propriamente dito, descrevendo normas, condutas, procedimentos de rotina ou emergenciais e os seus responsáveis, ou seja, define como as tarefas devem ser cumpridas.

Dentro desses conceitos são utilizados sistemas eletrônicos de segurança com o objetivo de minimizar todos os riscos ao patrimônio da instituição, sejam eles tangíveis ou não. E os sistemas de controle de acesso estão presentes nessa concepção desde o início das instituições nos quais as pessoas eram responsáveis diretas por esse controle, seja o porteiro permitindo alguém adentrar a instituição ou um funcionário que porta a chave de uma área da qual é responsável ou simplesmente por conhecimentos procedimentais sabendo se pode ou não adentrar determinadas áreas.

2.2 – Objetivos do sistema de controle de acesso

Controle de acesso é compreendido pela atividade que resulta no controle de circulação de pessoas ou veículos à determinada instituição através de barreiras físicas que dificultam, retardam e controlam toda movimentação.

Os controles de acesso são geralmente agrupados em três tipos de controle: Físico, Lógico e Administrativo. As empresas e instituições necessitam desses três tipos de controles. As políticas de segurança das empresas e instituições, através da documentação dos padrões de segurança governam o uso desses controles.

A seguir temos alguns exemplos de cada tipo de controle:

- **Físico* (mecânico e eletrônico):** portas, trancas, guardas, travas de acesso a disquetes, sistemas de travamento por cabos para mesas/paredes, circuito interno de TV, retalhadora de papéis e sistemas de controle de incêndio;

- **Lógico* (Técnico):** senhas, *tokens*, permissões para arquivos, listas de controle de acesso, privilégios de contas e sistemas de proteção de energia;

- **Administrativo:** conscientização sobre segurança, revogação de contas de usuários e políticas.

*Os tipos físico e lógico serão exemplificados logo a seguir.

Os controles de acesso podem ser divididos em dois tipos os quais são: **procedimentais ou propriamente ditos.**

Os controles de acesso procedimentais são restrições impostas por procedimento através de informações, treinamentos, ou mesmo controlado somente por alguma pessoa (segurança, porteiro, recepcionista), o reconhecimento e controle das pessoas é feito por crachás, credenciais, passes de trânsito livre, código de cores etc. (BRASILIANO, 2003).

Os controles de acesso propriamente ditos são meios que estabelecem restrições a circulação e/ou acesso. Este tipo de controle é o que nos interessa, pois nele estão contidas, em conjunto com a ação humana, barreiras físicas que restringem acesso a determinadas áreas como cancelas, catracas, portas, portões e torniquetes. Essas barreiras físicas podem ser automatizadas de tal forma utilizando-se recursos de eletrônica, eletromecânica e programas de computadores de forma que a ação humana utilizada para controle das mesmas seja reduzida a um posto de monitoramento, uma vez que a solicitação de acesso é feita com a aproximação do cartão da pessoa que deseja acessar determinada área (BRASILIANO, 2003).

O controle de acesso trata prioritariamente a identificação das pessoas, veículos e objetos verificando suas autorizações de entrada e saída nas áreas controladas. Os projetos desses sistemas devem seguir alguns critérios básicos para atender seus objetivos, dentre os quais se destacam:

- **Definir os perímetros de controle:** Os perímetros são espaços internos, as áreas das edificações, incluindo o limite periférico, que podem ter todas suas conexões controladas. Como exemplo pode ser citado salas com as suas portas, as salas são o perímetro de controle e as portas suas conexões controladas. Outro exemplo seria o muro ou alambrado com a portaria de uma empresa, onde toda área murada é o perímetro de controle e a portaria dotada de dispositivos de bloqueio (portões, cancelas e catracas) é a conexão controlada.

- **Definir os critérios de verificação:** São os parâmetros estabelecidos para as pessoas, veículos ou objetos pelos quais o sistema permitirá ou não a entrada ou saída no perímetro de controle. Os critérios de verificação é a forma de identificação do indivíduo ao sistema de controle de acesso, seja uma senha, cartão ou características biométricas. Os critérios de verificação estão contidos nas tecnologias existentes e são considerados os parâmetros mais importantes no controle de acesso, pois é o que difere os indivíduos no sistema.

- **Registros de todos os eventos decorrentes destas atividades;**

- **Armazenar e disponibilizar os eventos para auditoria.**

Os sistemas de controle de acesso podem ser classificados em **manuais, semiautomáticos e automáticos** a escolha de cada um é feita de acordo com as necessidades e valores disponíveis para investimentos.

- **Sistemas manuais** são controlados direta e exclusivamente pela ação humana (porteiros e recepcionistas), seu funcionamento é operacionalizado pela simples verificação da identidade da pessoa que requer acesso e sua respectiva autorização. O controle é feito visualmente, como por exemplo, a identificação de crachá. Este é o mais simples e vulnerável sistema de controle de acesso, pois como é diretamente operado pelo recurso humano, que tem maior chance de cometer erros, além de enfrentar conflitos com usuários da empresa ou instituição (BRASILIANO, 2003).

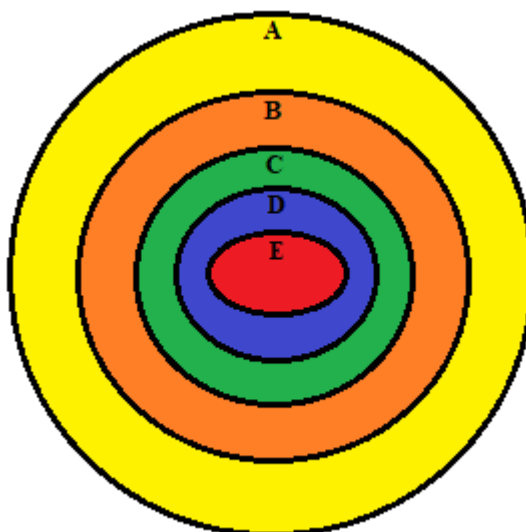
- **Sistemas Semiautomáticos** integram o recurso humano com a tecnologia. Geralmente esses sistemas selecionam o acesso por meio de um interfone e/ou porteiro eletrônico, supervisionados ou não por circuito interno de televisão, sendo a autorização liberada se as condições de acesso forem preenchidas. Neste caso são estipuladas senhas e contrassenha, ou verificação através de câmeras, as empresas e instituições que optam por esse tipo de sistema orientam que a pessoa responsável pela liberação do controle de acesso observe crachás, uniformes, adesivos que identificam veículos, por exemplo. O erro mais comum é o desleixo na identificação o que torna o sistema completamente burocrático e as

peças o consideram como mais um “empecilho” da segurança, para atrapalhar a circulação dos usuários; (BRASILIANO, 2003)

• **Sistemas Automáticos** independem da ação humana para identificar e autorizar o acesso ao interior das instalações. Este é o sistema que será tratado neste trabalho. Todos os eventos são registrados e armazenados no servidor do sistema de controle de acesso, o que é uma grande vantagem, pois não depende da ação humana para que esses registros sejam feitos. Os sistemas automáticos utilizam como meios de identificação para liberação ou restrição do acesso teclados para digitação de senha, cartões de códigos de barras ou proximidade (RFID), *tag* (RFID) para identificação de veículos, leitores de características biométricas e bloqueios como cancelas, catracas e portas, essas tecnologias de identificação serão abordadas com mais detalhes adiante (BRASILIANO, 2003).

Um sistema projetado com todas essas funcionalidades em conjunto com uma política de segurança clara e funcional irá atender os objetivos dos controles de acessos julgados necessários pela segurança corporativa da empresa.

Figura 1 - Diagrama dos níveis de controle de acesso



Fonte – Autoria própria (2018)

O diagrama da figura 1 ilustra os níveis de controle de acesso nas empresas e instituições começando pelas portarias até áreas específicas, a partir dela serão citados exemplos de aplicação dos sistemas de cada um dos níveis apresentados no diagrama acima proporciona uma etapa do controle de acesso e podem ser representadas da seguinte forma:

- A camada A pode ser representada pelo local de chegada das pessoas ou veículos, ou seja, as portarias, que mais do que controlar acesso tem a função de orientar e direcionar as pessoas. A partir dessa área se começam os controles procedimentais, ou seja, a partir dessa área todas as atividades devem se sujeitar as regras de segurança da instituição. A continuidade do fluxo é uma das principais preocupações por principalmente nos horários entrada e saída de funcionários, por isso os procedimentos nessa área devem ser rápidos e

precisos. Normalmente essas áreas utilizam dispositivos de bloqueio como catracas e cancelas para restringir e registrar, principalmente os horários de entradas e de saídas.

- A camada B pode ser representada pela recepção de uma empresa ou secretaria de uma instituição, pois a partir dessa área há direcionamento para os setores, seja por acesso as escadarias, elevadores ou diretamente aos corredores que levam aos departamentos e salas. Para o caso de visitantes, nesta camada os dados dos mesmos são confirmados e sua chega é comunicada ao responsável pela visita. Nesta área é comum a utilização de catracas como dispositivos de bloqueios.
- A camada C pode ser representada pelo caminho que direciona as pessoas aos departamentos da empresa ou instituição, os quais podem ser compostos por escadarias, elevadores e corredores. Na maioria dos casos os dispositivos de bloqueio utilizados são portas muitas vezes sem sistema eletrônico de controle para facilitar a integração entre os departamentos;
- A camada D são as áreas internas aos departamentos, dependendo do departamento das políticas da empresa ou instituição a circulação de pessoas nesta área é restrita somente a funcionários deste setor, caso haja algum terceiro este deve estar acompanhado de algum funcionário da área.
- A camada E é representada pelas áreas específicas. Essas áreas são de competência de algum departamento e pode estar contida em um espaço segregado dentro do departamento ou até mesmo em alguma área fora deste. O acesso as áreas específicas muitas vezes é permitido somente a alguns funcionários de determinado departamento, por exemplo, o acesso a sala de reuniões é permitido somente aos professores e coordenadores.

A partir disso é possível notar que o controle de acesso fica melhor concebido não só com a utilização de barreiras físicas, mas também com políticas procedimentais que dividem os departamentos e suas responsabilidades individuais em relação ao acesso as suas áreas mais restritas.

2.3 – Controle de acesso físico

2.3.1 - Controle de acesso mecânico

Esse é o tipo de controlador de acesso não eletrônico, ou seja, utiliza da mecânica para permitir o acesso à área restrita. Os tipos de equipamentos de controle de acesso mecânico mais comuns são: chaves; cadeados; fechaduras e catracas mecânicas.

Também é um sistema antiquado e apresenta baixa eficiência contra delitos, como por exemplo invasões e furtos, e é por isso que esse tipo de sistema geralmente utiliza de artifícios complementares, como um sistema de alarme.

2.3.2 – Controle de acesso eletrônico

É o sistema de acesso mais abrangente e tecnológico. Pode utilizar de tecnologias como cartões magnéticos até a leitura da íris, e é de grande dificuldade para ser burlado, já que cada indivíduo tem sua identificação única, como por exemplo em instituições que apenas quem possui o cartão magnético registrado ao sistema poderá adentrar.

Os controles de acesso utilizando sensores biométricos são os mais caros, porém de maior confiabilidade. Eles trabalham com leitura da digital e/ou leitura da íris, ou reconhecimento facial. Os equipamentos que vão permitir ou restringir a entrada do indivíduo poderão ser fechaduras eletrônicas com painéis de controle e catracas eletrônicas.

Investir em sistemas de controle de acesso, além de garantir a segurança das pessoas que moram, estudam ou trabalham no ambiente em questão, significa também estar investindo para manter os bens da empresa ou instituição, agregando ainda mais valor aos seus produtos e negócios.

2.3.2.1 – Equipamentos existentes para o controle de acesso eletrônico

Cartões ou chaveiros de proximidade (RFID's) (Figura 2): São muito práticos e podem ser aplicados em soluções de controle de ponto e acesso. São flexíveis e mais resistentes para o uso diário, pois não entram em contato direto com os leitores. Este equipamento será o foco do trabalho e será apresentada todas as suas informações a seguir.

Figura 2 - Cartão de proximidade



Fonte - Robocore (2008)

Smart Card (Figura 3): É um tipo de Cartão com um ou mais microchips embutidos, capaz de armazenar e processar dados. Na autenticação com *smart cards* é utilizada a combinação de um cartão com uma senha (Cartões de banco, por exemplo).

Figura 3 - Smart Card



Fonte – Aliexpress (2014)

Cartões de tarja magnético (Figura 4): O cartão de tarja magnética é composto de partículas magnéticas à base de ferro espalhadas por uma película semelhante a um filme e pode ter informações gravadas e lidas em sua superfície.

Figura 4 - Cartão magnético



Fonte - Blog Cartões magnéticos (2009)

Cartões de código de barras (Figura 5): O código de barras é uma forma de representar a numeração, que viabiliza a captura automática dos dados por meio de leitura óptica nas operações automatizadas.

Figura 5 - Cartão de código de barras



Fonte - Master Ponto (2013)

A biometria é uma tecnologia que é capaz de medir determinada característica de tal forma que o indivíduo seja realmente único. A biometria pode verificar ou identificar indivíduos através dos seguintes meios:

Biometria Digital (Figura 6): Ela armazena informações sobre pontos das digitais para realizar a comparação.

Figura 6 - Leitor de digitais



Fonte - Mega Especial (2015)

Biometria das mãos (Figura 7): São capturadas comprimento, largura, altura e outras características únicas da mão e dedos.

Figura 7 - Sensor biométrico para as mãos



Fonte 1 – InfoWester (2015)

Biometria da Retina (Figura 8): Os sistemas armazenam elementos únicos no padrão vascular da retina. A verificação ocorre através de uma câmera com uma luz de baixa intensidade, porém a maioria é feita com câmeras utilizando seu flash, já outros aparelhos usam equipamentos a laser.

Figura 8 - Scanner de retina



Fonte – Ytdk (2014)

Biometria da Íris (Figura 9): A verificação é feita da mesma forma que a retina com uma pequena exceção, utiliza-se apenas da parte colorida do olho que contorna a pupila. O usuário deve se colocar a uma distância de 7.5 a 25 cm do dispositivo para permitir o processo de *scan* da Iris por uma câmera.

Figura 9 - Scanner da íris



Fonte – Mark Pellegrini (2007)

Biometria da voz (Figura 10): Capturam características únicas da voz do usuário e pode realizar padrões fonéticos e linguísticos.

Figura 10 - Scanner de Voz



Fonte - AbleData (2006)

Biometria da Assinatura (Figura 11): O sistema requer que o usuário assine seu nome em um *tablet*. São analisadas características da assinatura para comparação com um valor previamente salvo.

Figura 11 - Scanner de assinatura



Fonte – DCHP (2005)

Como esse sistema de controle de acesso tem como base a participação de um funcionário, a compra e manutenção periódicas de equipamentos e ainda o treinamento de equipes (próprias ou terceirizadas) para administrar as mais diversas situações, pode ser relativamente dispendioso para algumas organizações ou instituições.

2.4 - Controle de acesso lógico

Controle de acesso lógico é um conjunto de medidas e procedimentos adotados pela organização apropriados aos softwares utilizados, cujo objetivo é proteger dados, programas e sistemas contra tentativas de acesso não autorizado feitas por usuários ou não.

Objetivo é proteger os recursos computacionais contra perda, danos, modificação ou divulgação não autorizada.

A conscientização do usuário é fundamental para que a estratégia de acesso seja eficaz. Um usuário bem treinado é uma das melhores maneiras de garantir a segurança da informação. Quando se trata de controles de acesso a primeira coisa a fazer é determinar o que se pretende proteger.

Alguns recursos e informações normalmente sujeitos a controles lógicos são:

Aplicativos: programas fonte e objeto. O acesso não autorizado ao código fonte dos aplicativos pode ser usado para alterar suas funções e a lógica do programa.

Arquivos de dados: base de dados, arquivos ou transações de bancos de dados devem ser protegidas para evitar que os dados sejam apagados ou alterados sem autorização adequada.

Utilitários e sistema operacional: o acesso a utilitários como compiladores, softwares de manutenção, de monitoração e diagnóstico devem ser de uso restrito, pois essas ferramentas podem ser usadas para alterar arquivos de dados, aplicativos e arquivos de configuração do sistema operacional.

O sistema operacional é bastante visado. Principalmente, arquivos de senha e arquivos de log. Os logs registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando o acesso ocorreu e que tipo de operações foram efetuadas. Se esse histórico não for devidamente protegido, um invasor poderá alterar seus registros para encobrir suas ações.

2.4.1 - Elementos do controle de acesso lógico

O Processo de *Logon* define o processo através do qual o acesso a um sistema informático é controlado através da identificação e autenticação do utilizador através de credenciais fornecidas por esse mesmo utilizador. Essas credenciais são normalmente constituídas por um nome de utilizador e uma senha.

A identificação do usuário deve ser única.

Autenticação: A maioria dos sistemas solicita uma senha, mas já existem sistemas utilizando imagens (*QR Codes – Figura 12*) que devem ser scaneadas e analisadas por uma câmera ou software que deverá estar instalado no aparelho para que libere o acesso para pesquisa ou alteração em determinado documento.

Figura 12 - QR Code



Fonte 2 - Tecmundo (2010)

Senhas: Uma palavra ou código secreto previamente convencionado entre as partes como forma de reconhecimento. Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios para agir como administradores de um sistema, ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

Figura 13 - Usuário e senha



Fonte - ServerVoip (2006)

Tokens: Objeto que o usuário possui que o diferencia das outras pessoas e o habilita a acessar algum sistema. Sua desvantagem é que podem ser roubados ou reproduzidos.

Figura 14 – Token



Fonte – Amazon (2009)

3 - RFID

O termo RFID é um acrônimo para a tecnologia de identificação por radiofrequência, originada da sigla em inglês para *Radio Frequency Identification*. Como será visto ao longo deste capítulo e da dissertação, várias expressões da língua inglesa são misturadas com expressões em português nesta tecnologia. Até mesmo a sigla apresenta uma “mistura”: ela é pronunciada metade em inglês e metade em português (usualmente, RFID lê-se: /erre-efe-áidi/).

A tecnologia de identificação por radiofrequência usa ondas de rádio para identificar objetos de forma automática, sejam seres vivos ou objetos inanimados. Outra definição, colocada por Glover e Bhatt (2006), descreve RFID como um sistema de identificação automática que faz uso da eletrônica para armazenar informação e transportá-la através de ondas de rádio. RFID é um dos tipos de tecnologia de identificação pelo qual um objeto pode ser identificado automaticamente (LAHIRI, 2005). Existem outros exemplos de tecnologias de identificação automática apresentadas anteriormente como: código de barras, sistemas de identificação biométrica (pela impressão digital, voz, geometria da mão e retina), cartões inteligentes de contato (*smart cards*) e reconhecimento ótico de caracteres.

Para demonstrar melhor a palavra “identificação”, analise o seguinte exemplo: cartuchos de tinta para impressoras. Embora dois cartuchos do mesmo modelo presentes em uma mesma loja aparentem ser idênticos, várias diferenças podem ser apontadas, como: local de fabricação (um deles pode ter sido produzido na China e o outro no Japão); as datas de validade; o número do pedido que a loja solicitou os produtos ao fornecedor; as datas de entrega dos cartuchos; etc. Ao ser usada no contexto de RFID, a palavra identificação se refere à unicidade de um objeto, permitindo distingui-lo de outro similar, mesmo que seja do mesmo fabricante, modelo e lote de fabricação.

3.1 - Propriedade das ondas eletromagnéticas

Algumas propriedades das ondas eletromagnéticas se propagando no espaço aberto estabelecem a base necessária para compreender melhor os problemas de propagação e antenas relacionados à RFID.

A existência de propagação de ondas eletromagnéticas foi prevista pelas equações de Maxwell, que especificam as relações entre as variações do vetor campo elétrico E, o vetor campo magnético H no tempo e no espaço em um determinado meio.

Como os problemas nas aplicações sistêmicas de RFID raramente exigem as equações de Maxwell para resolvê-los, pode-se resumir as quatro equações de Maxwell conforme descrevem Saunders e Aragon (2007):

“Um campo elétrico é produzido por um campo magnético variante no tempo. Um campo magnético é produzido por um campo elétrico variante no tempo ou por uma corrente. Linhas de campo elétrico podem começar e terminar nas cargas ou são contínuas. Linhas de campo magnético são contínuas.”

As duas primeiras equações, as equações espirais de Maxwell, apresentam duas constantes relacionadas ao meio que influem nas intensidades dos campos. São a constante de permeabilidade do meio μ ($H.m^{-1}$) e a constante de permissividade do meio ϵ ($F.m^{-1}$).

Normalmente, elas são expressas em relação ao vácuo:

$$\mu = \mu_0 \cdot \mu_r \quad (1)$$

$$\epsilon = \epsilon_0 \cdot \epsilon_r \quad (2)$$

em que μ_0 e ϵ_0 são os valores no vácuo:

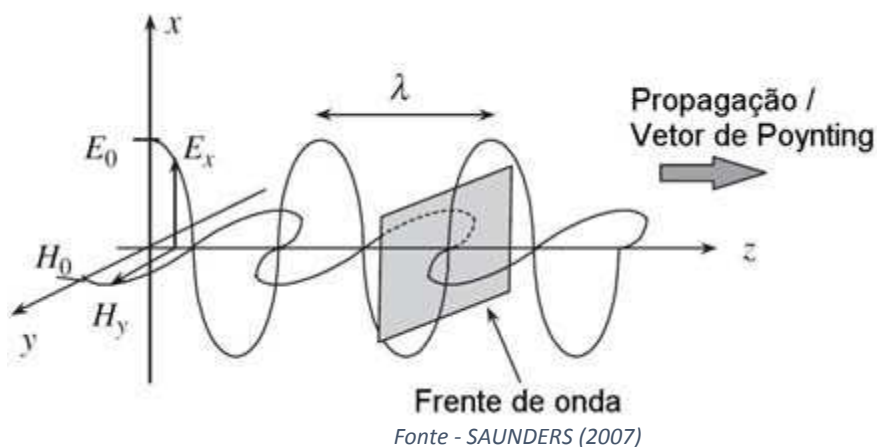
$$\mu_0 = 4\pi \times 10^{-7} H.m^{-1} \quad (3)$$

$$\epsilon_0 = 8,854 \times 10^{-12} \approx \frac{10^{-9}}{36\pi} F.m^{-1} \quad (4)$$

sendo μ_r e ϵ_r são os valores relativos ($\mu_r = \epsilon_r = 1$ no vácuo).

Existem várias soluções para as equações de Maxwell e todas elas representam campos que poderiam ser reproduzidos na prática. Entretanto, todas elas podem ser representadas como um somatório de ondas planas, que representam a solução variante no tempo mais simples possível (SAUNDERS; ARAGON, 2007), conforme mostrado na Figura 15.

Figura 15 - Onda plana se propagando no espaço



Os campos elétrico e magnético são perpendiculares entre si e com a direção de propagação da onda, que é ao longo do eixo z. O vetor nesta direção é o vetor de propagação ou vetor de *Poynting*. Os dois campos estão em fase em qualquer ponto no tempo e no espaço. O campo elétrico oscilante produz um campo magnético, que por sua vez oscila, recriando um campo elétrico e assim por diante. Esta interação entre os dois campos armazena energia e então transmite potência ao longo do vetor de *Poynting*. A variação ou modulação das

propriedades da onda (amplitude, frequência ou fase) então permite que a informação seja transmitida na onda entre sua fonte e o destino, que é o objetivo central dos sistemas de comunicação por radiofrequência.

Os vetores dos campos seriam senoidais com amplitude constante, caso o meio não apresentasse perdas. Devido ao decaimento exponencial do campo, Saunders e Aragon (2007) sugerem que é conveniente representar a amplitude e a fase da onda usando números complexos, já que a onda varia de forma senoidal tanto em relação ao tempo como à distância, resultando nas equações para os campos:

$$E = E_0 e^{j(\omega t - kz)} \hat{x} \quad (5)$$

$$H = H_0 e^{j(\omega t - kz)} \hat{y} \quad (6)$$

Sendo E_0 e H_0 são a amplitude dos campos elétrico e magnético, respectivamente, $\omega = 2\pi f$ é a frequência angular, t é o tempo decorrido, k é o número de onda, z é a distância no eixo z , e \hat{x} e \hat{y} são vetores unitários na direção positiva dos eixos x e y , respectivamente. O número de onda representa a taxa de mudança da fase do campo com a distância, que, para o comprimento de onda λ , a fase da onda varia de 2π . Portanto:

$$k = \frac{2\pi}{\lambda} \quad (7)$$

O vetor de *Poynting* S , medido em watts por metro quadrado, define a magnitude e a direção do fluxo de potência transmitido pela onda por metro quadrado de área paralela ao plano xy , ou seja, a densidade de potência da onda. Seu valor instantâneo é dado por:

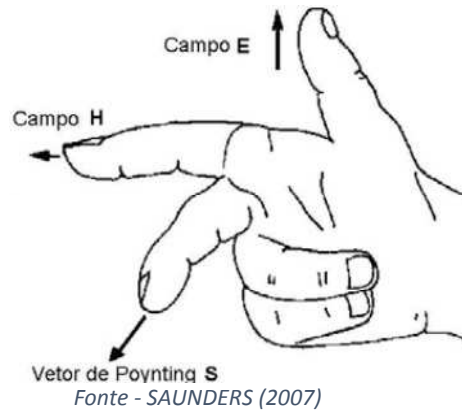
$$S = E \times H^* \quad (8)$$

Usualmente, é necessária apenas a média do fluxo de potência em um período:

$$S_{av} = \frac{1}{2} E_0 H_0 \hat{z} \quad (9)$$

vetor de direção na equação acima enfatiza que E , H e S_{av} formam a regra da mão direita, conforme mostrado na figura 16:

Figura 16 - Regra da mão direita para identificação do Vetor de Poynting



A velocidade de um ponto de fase constante na onda, que define a velocidade V na qual as frentes de onda avançam na direção S , é dada por:

$$v = \frac{\omega}{k} = \frac{1}{\sqrt{\mu\epsilon}} \quad (10)$$

Como k é definido em função do comprimento de onda, então este é dado por:

$$\lambda = \frac{v}{f} \quad (11)$$

No vácuo, a velocidade de fase se torna:

$$v = c = \frac{1}{\sqrt{\mu_0\epsilon_0}} \approx 3 \times 10^8 \text{ m/s} \quad (12)$$

Quando o meio apresenta condutividade elétrica significativa, a amplitude da onda diminui com a distância percorrida, pois a energia é removida da onda e convertida em calor. Portanto, as equações para os campos podem ser substituídas por:

$$E = E_0 e^{[j(\omega t - kz) - \alpha z]} \hat{x} \quad (13)$$

$$H = H_0 e^{[j(\omega t - kz) - \alpha z]} \hat{y} \quad (14)$$

em que α é a constante de atenuação, que depende da permeabilidade e da permissividade do meio, da frequência da onda e da condutividade elétrica do meio σ , conforme mostrado na Tabela 1. Juntas, σ , μ e ϵ são conhecidas como os parâmetros constituintes do meio.

Em consequência, as intensidades dos campos elétrico e magnético diminuem exponencialmente à medida que a onda avança pelo meio. A distância que a onda atravessa o meio até atingir uma redução no campo de $e^{-1} = 36,8\%$ do seu valor inicial é chamada de profundidade pelicular δ , que é dada por:

$$\delta = \frac{1}{\alpha} \quad (15)$$

Portanto, a amplitude da intensidade do campo elétrico em um ponto z comparado com seu valor em $z = 0$ é dada por:

$$E(z) = E(0)e^{-\left(\frac{z}{\delta}\right)} \quad (16)$$

Na Tabela 1 são apresentadas as expressões para α e k que se aplicam tanto para um meio sem perdas como para um meio com perdas.

Tabela 1 - Tabela com as expressões de α e k para meios com e sem perdas

$n = ck/\omega$ in all cases	Exact expression	Good dielectric (insulator) $(\sigma/\omega\epsilon)^2 \ll 1$	Good conductor $(\sigma/\omega\epsilon)^2 \gg 1$
Attenuation constant α [m^{-1}]	$\omega \sqrt{\frac{\mu\epsilon}{2} \left[\sqrt{1 + \left(\frac{\sigma}{\omega\epsilon}\right)^2} - 1 \right]}$	$\approx \frac{\sigma}{2} \sqrt{\frac{\mu}{\epsilon}}$	$\approx \sqrt{\frac{\omega\mu\sigma}{2}}$
Wave number k [m^{-1}]	$\omega \sqrt{\frac{\mu\epsilon}{2} \left[\sqrt{1 + \left(\frac{\sigma}{\omega\epsilon}\right)^2} + 1 \right]}$	$\approx \omega \sqrt{\mu\epsilon}$	$\approx \sqrt{\frac{\omega\mu\sigma}{2}}$
Wave impedance Z [Ω]	$\sqrt{\frac{j\omega\mu}{\sigma + j\omega\epsilon}}$	$\approx \sqrt{\frac{\mu}{\epsilon}}$	$\approx \sqrt{\frac{\omega\mu}{2\sigma}}(1 + j)$
Wavelength λ [m]	$\frac{2\pi}{k}$	$\approx \frac{2\pi}{\omega\sqrt{\mu\epsilon}}$	$\approx 2\pi\sqrt{\frac{2}{\omega\mu\sigma}}$
Phase velocity v [$m\ s^{-1}$]	$\frac{\omega}{k}$	$\approx \frac{1}{\sqrt{\mu\epsilon}}$	$\approx \sqrt{\frac{2\omega}{\mu\sigma}}$

Fonte - SAUNDERS (2007)

Com o campo predominantemente magnético presente na antena, um acoplamento indutivo pode ser feito nas proximidades da antena. A uma distância de $\lambda/2\pi$, o campo eletromagnético começa a se separar da antena e se propaga no espaço na forma de uma onda eletromagnética. A região entre a antena até o ponto onde o campo eletromagnético está se formando é denominada de campo próximo (*near field*) da antena. A partir do ponto onde o campo eletromagnético está totalmente formado e se separa da antena, é chamado de campo distante (*far field*). Na região do campo próximo, a intensidade do campo magnético decai com a distância em 60 dB por década de distância, já que a intensidade do campo decai com a distância d pela relação de $1/d^3$. No campo distante, esta taxa cai para 20 dB por década, já que a intensidade do campo passa a variar com a distância pela razão de $1/d$, pois nessa região se dá apenas a atenuação do espaço livre.

3.2 – Comparação com outras tecnologias

O código de barras é, provavelmente, o tipo de identificação automática de produtos mais utilizado. Um dos motivos é o seu custo, que é o mais barato de todos, conforme mostrado na Tabela 2. Os códigos de barras apresentam a vantagem de serem rápidos e precisos de serem lidos, chegando a uma taxa de erro de apenas 1 em 2-3 milhões de leituras. Outra vantagem é o custo da etiqueta, que é facilmente gerada por impressoras relativamente simples e baratas utilizando apenas papel ou etiquetas adesivas. Por outro lado, as etiquetas são sensíveis à sujeira, tinta, umidade e descoloração pela ação do sol. Além disso, o código de barras exige visada direta entre a leitora e a etiqueta, pois qualquer obstáculo entre eles inviabiliza a leitura.

A biometria é definida como a ciência dos procedimentos de contagem e medição de características físicas que envolvem os seres vivos (*FINKENZELLER, 2010*). Nas aplicações de identificação de seres humanos, a biometria apresenta algumas vantagens. A exclusividade de traços biométricos permite uma identificação eficaz, impede que uma pessoa se passe por outra e não precisa de etiquetas ou outros objetos associados à pessoa. Entretanto, a identificação biométrica é a mais lenta e a que exige um maior custo de implantação do sistema, como pode ser observado na Tabela 2, que realiza a comparação entre RFID e outras tecnologias de identificação, ficando claras as vantagens de RFID sobre elas.

Tabela 2 - Tabela de comparação de algumas Tecnologias de identificação

Parâmetro	Código de barras	Biometria	Cartões magnéticos	RFID
Densidade de dados	Baixa	Alta	Muito Alta	Muito Alta
Influencia de sujeira	Muito Alta	-	Médio	Não influencia
Obstaculo físico	Causa Falha	Possivel falha	-	Não influencia
Mudança de orientação	Baixa	-	Unidirecional	Não influencia
Degradação	Limitada	-	Médio	Não influencia
Custo de implantação	Baixo	Muito Alto	Baixo	Médio
Custo de manutenção	Baixo	Nenhum	Médio	Baixo
Adulteração	Razoável	Raro	Muito Raro	Muito Raro
Velocidade de leitura (Processo completo)	3s	3 - 7 s	3s	0,5 - 1 s
Alcance	até 50cm	0 - 50 cm	0	0,1 - 25 m

Fonte – HerrTech (2009)

3.3 – História do RFID

“A tecnologia de identificação por radiofrequência ou RFID (*Radio Frequency Identification*) tem suas origens no século XIX quando houve grandes avanços científicos em eletromagnetismo, com as descobertas de Michael Faraday sobre a indutância elétrica, as equações que descrevem o eletromagnetismo de James Clerk Maxwell, e os experimentos de Heinrich Rudolf Hertz que confirmaram as afirmações de Faraday e Maxwell.

Antes dos sistemas de identificação por radiofrequência vieram os sistemas de detecção de objetos. Uma das primeiras patentes foi o rádio transmissor para sistema de detecção de objetos desenvolvido por John Logie Baird em 1926. Mais tarde, em 1935, o físico escocês Robert Alexander Watson-Watt patenteou o conhecido sistema de RADAR (*Radio Detection and Ranging*). Durante a Segunda Guerra Mundial, os países em conflito usavam o radar para alertar a aproximação de aviões. O problema é que não havia como distinguir se era um inimigo ou não. Então, os alemães descobriram que ao girar seus aviões, quando voltavam à base, o sinal de rádio refletido era alterado, diferenciando a identificação dos aviões alemães. Este foi, o primeiro sistema RFID passivo.

Watson-Watt liderou um projeto secreto britânico e ajudou a criar o primeiro sistema de identificação ativo, o *Identify Friend or Foe* (IFF), que foi implantado pela Força Aérea Real britânica durante a Segunda Guerra Mundial. Um transmissor era colocado em cada

avião britânico. Quando recebia sinal das estações de radar, o transmissor retornava um sinal identificando aquela aeronave como amiga. O sistema IFF ajudava a evitar incidentes de "fogo amigo" e auxiliava na perseguição de aviões inimigos. O sistema RFID funciona com o mesmo conceito. Um sinal é enviado para um transponder, que é ativado e reflete o sinal de volta (sistema passivo) ou propaga um sinal (sistema ativo).

Nos anos 60, diversas companhias começaram a usar comercialmente sistemas de *Electronic Article Surveillance* (EAS). Os sistemas de EAS consistem em um dispositivo magnético embutido nos produtos, chamado de etiqueta ou *tag*, que é desativado ou removido quando o item é comprado. A presença de *tags* ativas dispara alarme se passarem por sensores colocados nas portas dos estabelecimentos. Diferente do RFID, esse tipo de EAS não identifica automaticamente uma *tag* específica, apenas detecta sua presença. Por isso, para esta aplicação, a *tag* tem apenas 1-bit.

No início década de 70, após o surgimento dos transistores e da microeletrônica, começaram a surgir as primeiras pesquisas de uso de UHF para identificação. Uma *tag* com maior capacidade de identificação e relativamente barata, sem a necessidade de bateria, podia ser construída usando um circuito ressonante composto de um capacitor e um indutor, que juntos determinam a frequência na qual certa corrente flui na *tag* através de um acoplamento indutivo. Retificando esta corrente, a alimentação da *tag* é obtida. O sinal emitido pela fonte também pode ser modulado pela *tag*, através da variação de sua carga vista pelo transmissor, gerando uma sinalização passiva.

Em 1973, Charles Walton, um empreendedor da Califórnia, patenteou o transponder passivo usado para abrir portas sem uso de chave. O transponder fica embutido em um cartão, que passa por um leitor. Quando o leitor detecta um número de identificação válido, que está armazenado na *tag* RFID, a porta é desbloqueada.

No final dos anos 70, o Departamento de Energia do governo dos Estados Unidos requisitou ao Laboratório Nacional de Los Alamos o desenvolvimento de um sistema para rastreamento de material nuclear. Um grupo de cientistas teve a ideia de colocar transponders nos caminhões e leitores nos portões das instalações.

Depois disso, nos anos 80, o mesmo grupo de cientistas que trabalharam no projeto, saíram e formaram uma empresa que desenvolveu o sistema de pagamento de pedágio automatizado.

A pedido do Departamento de Agricultura, o laboratório de Los Alamos também desenvolveu a *tag* de RFID passiva usada para rastrear vacas. Isto era usado para evitar que hormônios e medicamentos fossem dados a vacas doentes, além de controlar a dosagem dada a cada animal.

Mais tarde, as empresas desenvolveram um sistema de baixa frequência (LF), que funciona em 125 kHz, resultando em transponders menores, que eram encapsulados e injetados sob a pele das vacas. Esse sistema é usado em todo o mundo até hoje. Os transponders de baixa frequência também eram colocados em cartões e usados para o controle de acesso à edifícios.

Com o tempo, as empresas começaram a comercializar os transponders de baixa frequência e evoluíram do espectro de rádio para alta frequência (HF), cuja frequência é 13,56 MHz. Altas frequências ofereciam maior alcance e velocidade de transferência de dados.

No final da década de 80, foi estabelecido o padrão S-9183 pela associação da indústria ferroviária americana – AAR – para identificação de vagões nos EUA, baseado nas *tags* passivas operando na faixa ISM (Industrial, Científica e Médica) de 902 a 928 MHz. Em 1994, praticamente todos os vagões estavam equipados com *tags* S-918.

No início de 1990, engenheiros da IBM desenvolveram e patentearam o RFID de ultra alta frequência (UHF). Alguns testes foram feitos na Wal-Mart, mas a tecnologia não chegou a ser comercializada. Também surgiram os padrões para cartões de identificação de pessoas e cartões de crédito, tipicamente os padrões ISO 14443 e ISO 15693.

Depois, em meados de 1990, por problemas financeiros, a IBM vendeu a patente para a *Intermec*, uma fornecedora de códigos de barra. O sistema de RFID da *Intermec* foi instalada em inúmeras aplicações, desde rastreamento de estoque até em agricultura.

O UHF RFID teve um salto significativo em 1999, quando a *Uniform Code Council*, a *EAN International*, a Procter & Gamble e a Gillette investiram fundos e criaram o Auto-ID Center no Instituto de Tecnologia de Massachusetts (MIT). Dois professores do MIT, David Brock e Sanjay Sarma, fizeram pesquisas para o uso de RFID *tags* de baixo custo em todos os produtos para rastreá-los na cadeia logística. A ideia era colocar apenas um número serial na *tag*, pois um simples microchip contendo poucas informações seria mais barato de produzir do que um chip complexo com mais memória. Além disso, os dados associados ao número serial na *tag* seriam armazenados em um banco de dados na internet.

Entre 1999 e 2003, o *Auto-ID Center* ganhou o apoio de mais de 100 empresas consumidoras, do Departamento de Defesa dos EUA e de vários vendedores importantes de RFID. Foram abertos centros de pesquisa em diversos países, que desenvolveram dois protocolos de interface de ar (Class 1 e Class 0), que ditam como a *tag* e o leitor se comunicam, o *Electronic Product Code* (EPC), e a arquitetura de redes para busca de informações sobre a RFID *tag* na internet. A tecnologia foi licenciada pela *Uniform Code Council* em 2003, que criou o *EPCglobal*, um conjunto de normas e serviços, para comercializar a tecnologia EPC. O *Auto-ID Center* foi encerrado em outubro de 2003 e as pesquisas passadas para o *Auto-ID Labs*, uma rede de pesquisas envolvendo 7 universidades em todo o mundo.

As companhias da *EPCglobal* adotaram o nome GS1 em 2005 para refletir sua consolidação, simbolizando um padrão global, um sistema global e uma organização global. Os antigos padrões Classe 0 e Classe 1 definiam o uso de EPC para identificação e usavam a mesma faixa de frequência, mas definiam protocolos completamente diferentes. O novo protocolo criado no final de 2004 pela *EPCglobal* foi denominado EPC Geração 2, ou EPC Gen2.

Na mesma época da criação da *EPCglobal*, a maior cadeia de supermercados do mundo, Wal-Mart, definiu que seus 100 maiores fornecedores deveriam colocar *tags* em todos os paletes entregues à sua rede até janeiro de 2005. Os 100 maiores fornecedores seguintes

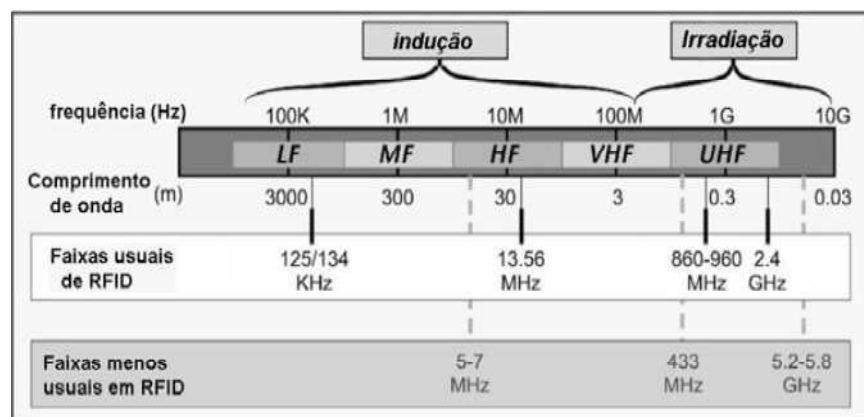
deveriam atender esta exigência até janeiro de 2006. Apesar dessa manobra ousada para a época, tais exigências foram cumpridas e o investimento se justificou. O Departamento de Defesa dos EUA, que já havia usado RFID no rastreamento de containers, também deliberou que embalagens com produtos de alto valor deveriam receber *tags* em 2006.” (HWANG, CERDEIRA, MONTEIRO, 2013)

3.4 – Faixas de frequência e tipos de acoplamento

RFID usa ondas de rádio que estão geralmente entre as frequências de 30 kHz e 5.8 GHz. Conforme os sistemas foram evoluindo e os padrões foram estabelecidos, algumas faixas mais específicas foram adotadas para utilização. As faixas de frequência mais comumente encontradas são 125/134 kHz, 13,56 MHz, 860-960 MHz e 2,4- 2,45 GHz. Leitoras e *tags* na faixa de 900 MHz e em 2,4 GHz são ambas da banda de ultra alta frequência (UHF), que termina formalmente em 3 GHz, mas para fazer uma distinção conveniente entre os dois, as leitoras e *tags* de 900 MHz são normalmente chamados de dispositivos de UHF, enquanto as de 2,4 GHz são conhecidas como leitoras de micro-ondas. Na Figura 17 é ilustrado o espectro de frequência usado em RFID e os tipos de acoplamento usuais para cada faixa.

A forma de transmissão do sinal de RFID é particular para cada faixa de frequência. Isto implica que diferentes aplicações podem exigir diferentes frequências e, conseqüentemente, equipamentos distintos.

Figura 17 - Banda de Frequência do RFID



Fonte 3- DOBKIN (2008)

A seguir na Tabela 3, será colocado de forma mais resumida as faixas de frequências, principais características e aplicações do RFID.

Tabela 3 - Tabela com a frequência, características e aplicações do RFID

Frequência	Principais Características	Aplicações
LF Abaixo de 135 kHz	<ul style="list-style-type: none"> •Amplamente utilizada desde os anos 80 •Funciona bem com líquidos e metais •Menor velocidade de transf. De dados •Alcance na faixa de centímetros 	<ul style="list-style-type: none"> •Identificação de animais •Automação industrial •Controle de acesso
HF 13,56 MHz	<ul style="list-style-type: none"> •Amplamente utilizada desde os anos 90 •Desempenho limitado na presença de metais • Padrões mundiais populares •Alcance acima de 1 m •Custo das Tags menor que as de LF 	<ul style="list-style-type: none"> •Cartões de crédito e fidelidade (smart cards) •Controle de acesso •Combate à falsificação •Várias aplicações de rastreamento de itens •Identificação e monitoria de pessoas e veículos
UHF 433 MHz e 860-930 MHz	<ul style="list-style-type: none"> •Em uso desde o final da década de 90 •Alcance maior que a de HF (mais de 3 metros) •Alcance longo para sistemas ativos em 433 MHz (até centenas de metros) •Potencial de oferecer os tags mais baratos •Problemas de incompatibilidade entre regulamentações locais •Suscetibilidade de interferência de líquido e metal 	Cadeia de suprimentos e logística: <ul style="list-style-type: none"> • Controle de estoque • Gerenciamento de depósitos • Rastreamento de bens
Microondas 2,45 e 5,8 GHz	<ul style="list-style-type: none"> • Em uso por várias décadas • Transferência de dados rápida • Comum nos modos ativo e passivo • Faixa de alcance similar a UHF • Pior desempenho com líquido e metal 	<ul style="list-style-type: none"> • Controle de acesso • Coleta eletrônica de pedágio • Automação industrial

Fonte – Marcos Antônio (2015)

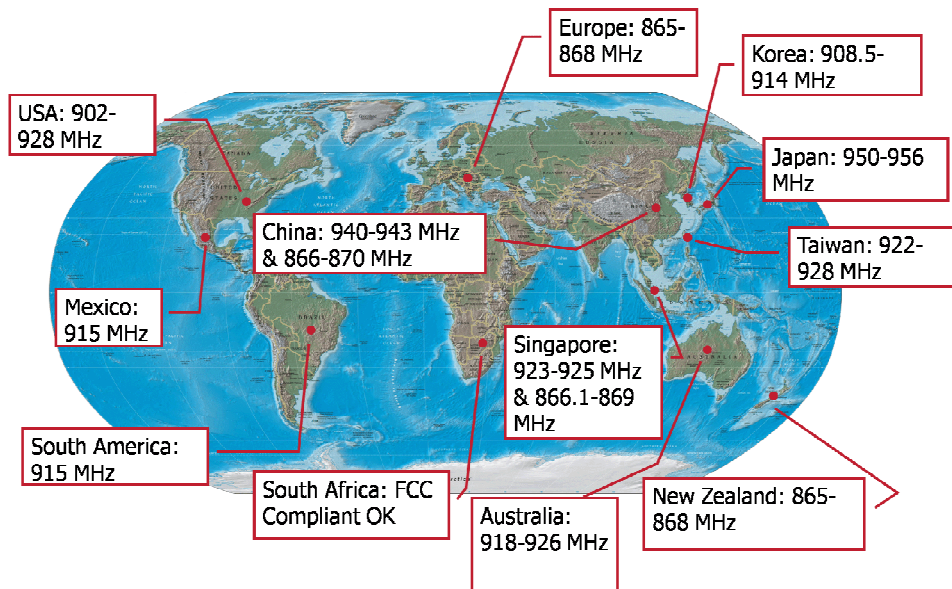
Baixas frequências são ideais em situações onde a *tag* precisa ser lida através de materiais que contenham líquidos ou partes metálicas. Com o aumento da frequência, as ondas de rádio passam a ter um comportamento semelhante ao da luz, ou seja, elas não passam com facilidade por alguns materiais e são refletidas por alguns outros. Sinais na faixa de UHF são facilmente absorvidos por líquidos, já que a profundidade pelicular δ diminui com o aumento da frequência, conforme visto no item 3.1 – Propriedades das ondas eletromagnéticas. Isso se constitui em um dos grandes desafios da indústria de RFID/UHF.

Cada país possui uma entidade regulatória do uso das faixas de frequência, incluindo a concessão de faixa, o nível de potência permitido em cada faixa, tipo de modulação, etc. No Brasil, a Anatel (Agência Nacional de Telecomunicações) é o órgão responsável por regular o uso de radiofrequência. Nos Estados Unidos, é a *Federal Communications Commission* (FCC), vários países da comunidade europeia são regidos pela *European Telecommunications Standards Institute* (ETSI), e assim por diante.

O ambiente regulatório mundial na faixa de 860-960 MHz é muito complexo. Conforme pode ser observado na Figura 18, cada país fez escolhas diferentes de uso desta faixa para acomodar a operação da telefonia celular e outras aplicações importantes. Por outro

lado, a banda de 2,4-2,45 GHz é disponível para operação sem licença em praticamente todo lugar, apesar de apresentar mais interferência por causa da sua utilização excessiva.

Figura 18 - Faixas de banda no mundo para RFID em UHF



Fonte – Embedded (2013)

3.5 – Tipos de acoplamento

Tipicamente, o acoplamento indutivo (campo magnético) é utilizado nas faixas de frequência LF e HF. O acoplamento capacitivo (campo elétrico) é tipicamente usado na faixa de frequência de 900 MHz e em UHF.

3.5.1 – Acoplamento indutivo

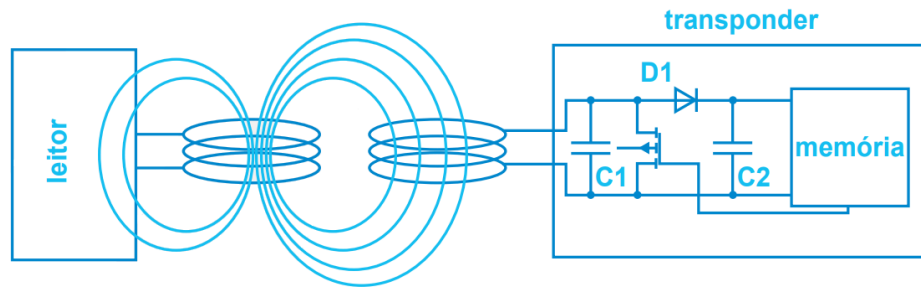
O acoplamento indutivo (Figura 19) é um tipo comum de acoplamento remoto. Um leitor fornece energia para as etiquetas acopladas indutivamente, usando uma antena espiral para gerar um campo magnético.

O campo dirige a corrente por uma espiral na etiqueta por indução de forma muito semelhante à de um transformador transferindo energia entre duas bobinas.

O campo fornece bastante energia para o chip, o qual pode então se comunicar com o leitor pela modulação de carga quase que da mesma forma que o acoplamento *backscatter* (será apresentado mais a frente).

Um resistor da etiqueta, liga e desliga, gerando flutuações no campo magnético, o que cria alterações de voltagem na antena do leitor.

Figura 19 - Princípio de funcionamento de um acoplamento indutivo



Fonte - IndusMelec (2013)

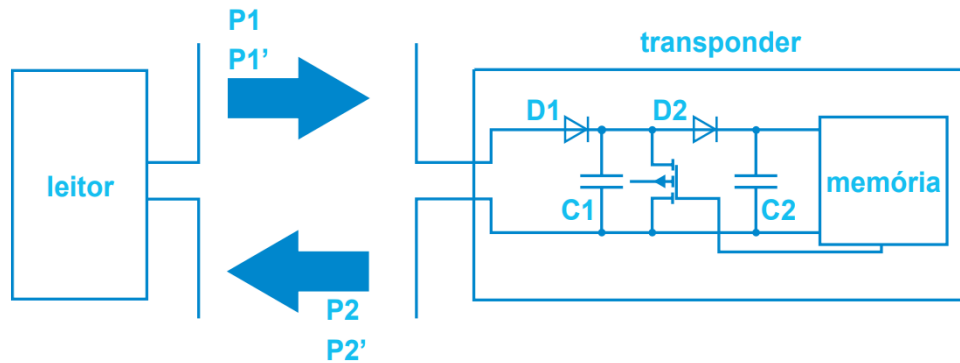
3.5.2 – Acoplamento capacitivo ou *Backscatter*

Nesse tipo de acoplamento (Figura 20) as etiquetas, normalmente de UHF e Micro-ondas refletem a mesma frequência emitida pelo leitor, mas alteram diversas qualidades dessa reflexão para enviar informações para o leitor.

Nesse processo, um leitor envia um sinal para uma etiqueta e ela responde, por reflexão, a uma parte dessa energia de volta para o leitor. Um dispositivo de carga contido na etiqueta, tal como um capacitor, possibilita essa reflexão.

O capacitor se carrega quando ele armazena a energia recebida do leitor. Quando a etiqueta responde de volta, ela usa essa energia para retornar o sinal ao leitor. O capacitor se descarrega nesse processo.

Figura 20 - Princípio de funcionamento de um acoplamento Backscatter ou capacitivo



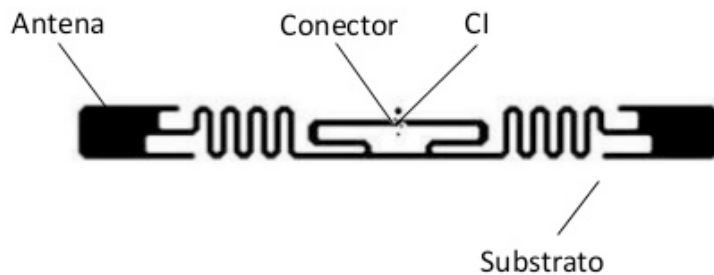
Fonte4 – IndusMelec (2013)

3.6 - TAGs

Uma *tag* de RFID é um dispositivo que pode armazenar e transmitir dados para uma leitora sem a necessidade de contato, usando ondas de rádio. Usualmente, a *tag* também é chamada de transponder, derivado dos termos em inglês *transmitter e responder* (transmissor e respondedor). O propósito de uma *tag* de RFID é anexar fisicamente a um objeto os dados pertinentes a ele. Desta forma, pode-se chamar a *tag* de etiqueta eletrônica.

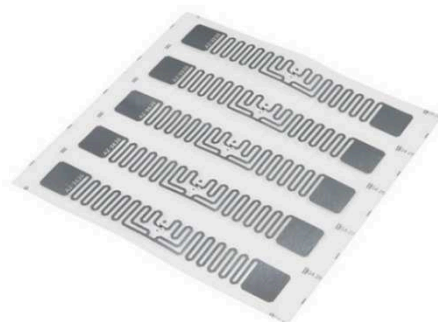
Fisicamente, uma *tag* passiva é formada por um microchip conectado a uma pequena antena. Tipicamente, este arranjo é montado em um substrato de plástico ou papel. A *tag* neste formato bruto é chamada de *inlay ou inlet* e posteriormente pode ser transformada em etiquetas, cartões ou outro formato que melhor se adapte ao tipo de aplicação final. Nas Figuras 21 e 22 é mostrada a representação de uma *tag* e um de seus usos como tag adesiva.

Figura 21 - Componentes de uma TAG



Fonte – FINKENZELLER (2010)

Figura 22 - TAG adesiva de UHF



Fonte - Spark Eletronics (2009)

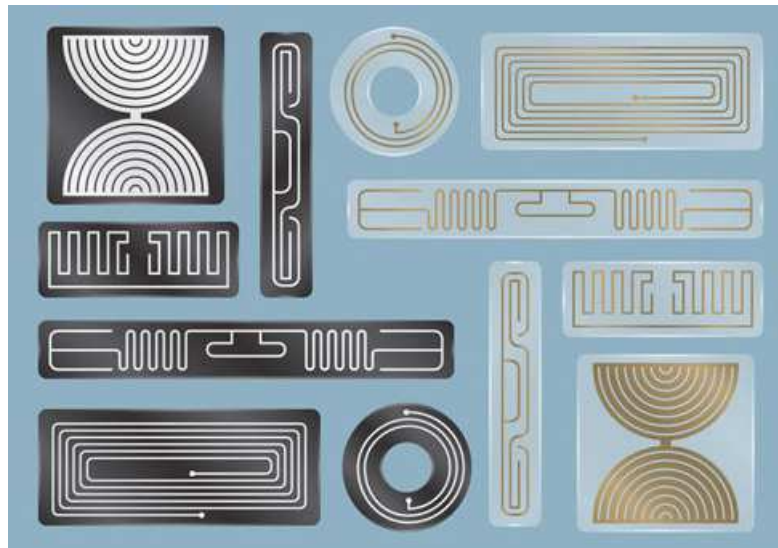
Há dois tipos básicos de chips encontrados nas *tags* de RFID: somente-leitura (read-only) e leitura-escrita (read-write). Chips do tipo somente-leitura são programados com dados gravados no momento da fabricação e essas informações não podem ser alteradas posteriormente. Com chips do tipo leitura-escrita, o usuário pode adicionar informações às *tags* ou sobrescrever as existentes quando a *tag* se encontra dentro da zona de alcance de uma leitora. Chips leitura-escrita são mais caros que os do tipo somente-leitura. Outro método bastante utilizado é chamado de WORM (*write once read many*). Este tipo de chip permite que uma *tag* seja gravada uma única vez pelo usuário e depois permaneça em estado somente-leitura. A capacidade de armazenamento de um chip varia bastante de modelo para modelo.

Outro tipo de classificação das *tags* é baseado no tipo de alimentação utilizado em seus circuitos, que pode ser obtida a partir do sinal recebido das antenas da leitora ou pode fazer uso de uma bateria interna. Dependendo da fonte de energia, as *tags* podem ser classificadas como ativas, passivas e semi-ativas (ou semi-passivas) (LAHIRI, 2005).

As *tags* ativas têm uma fonte de alimentação interna que é usada para ativar os circuitos do microchip e para enviar o sinal de resposta à leitora. Esse tipo de *tag* pode ser lido a grandes distâncias e consegue responder a sinais bastante atenuados. Algumas *tags* ativas podem atingir um alcance de centenas de metros.

As *tags* passivas não possuem uma fonte de alimentação própria e precisam retirar energia do campo eletromagnético criado pelo sinal propagado em torno das antenas da leitora. A *tag* utiliza esta energia para alimentar todo o seu circuito e também para enviar o sinal de resposta à leitora. Isso limita o seu alcance a pouco mais de 2.5 - 3 metros. Como não usa bateria e sua constituição é basicamente o microchip e a antena, este tipo de *tag* é a opção mais barata para rastreamento de produtos. Na Figura 23 são ilustrados alguns modelos de *tags* passivas UHF.

Figura 23 - Exemplos de Tags passivas para UHF



Fonte - RFID Library (2008)

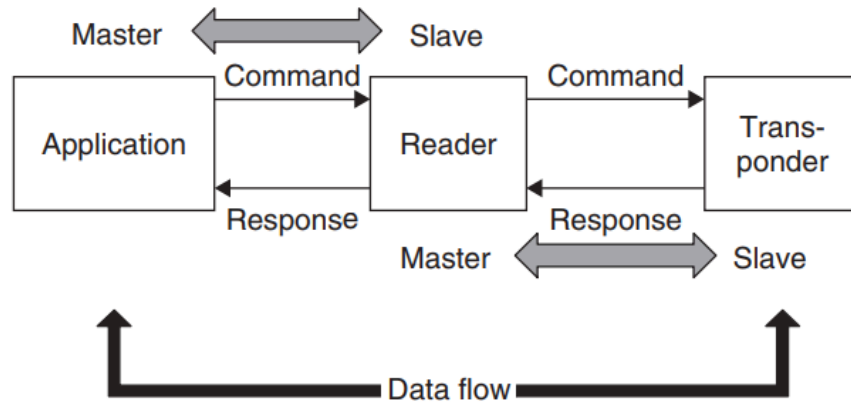
As tags semi-ativas (ou semi-passivas) usam uma bateria interna para alimentar o circuito do microchip, porém, para comunicação, retiram energia do sinal originado na leitora. Este tipo de projeto permite o aumento do alcance de leitura que pode chegar a 30 metros em condições ideais usando a modulação refletida (*backscatter*) em UHF e micro-ondas. A energia extra permite também uma memória com maior capacidade de armazenamento e mais poder de processamento.

Cada tipo de *tag* apresenta uma necessidade mínima de energia para responder adequadamente à leitora. Dependendo do tipo e do padrão aos quais ela pertença, existe uma especificação neste sentido. Por exemplo, Sweeney (2005) descreve que a energia mínima necessária para ler uma tag EPC é na ordem de 100 microwatts ou -10 dBm.

3.6 – Leitoras

As leitoras de RFID, também chamadas de interrogadores, são equipamentos que podem ler e escrever dados de *tags* compatíveis com seu sistema (LAHIRI, 2005). Portanto, apesar do nome, uma leitora de RFID também tem a capacidade de escrever na *tag*, caso ela tenha este recurso. Operações de leitura e escrita na *tag* são executadas usando o princípio mestre-escravo (FINKENZELLER 2010), mostrado na figura 24. A leitora assume o papel de mestre e a *tag* apenas responde aos comandos da leitora.

Figura 24 - Princípio de Mestre-Escravo



Fonte - FINKENZER (2010)

De forma resumida, os componentes básicos de uma leitora são o sistema de controle e o sistema de RF, formado pelo receptor e pelo transmissor. O transmissor deve ser preciso, eficiente, e transmitir dentro da faixa de frequência permitida. O receptor deve ter boa sensibilidade, seletividade e detectar uma faixa extremamente ampla de sinal. Ambos devem ser flexíveis. Como as leitoras de RFID normalmente trabalham nas faixas de frequências não licenciadas, elas devem implementar saltos de frequência (*frequency hopping*) e outros recursos de minimização de interferências.

Uma leitora de RFID que se comunica com *tags* passivas ou semi-passivas deve operar no modo full duplex, pois deve transmitir uma onda contínua (para que a *tag* possa enviar o sinal refletido) enquanto recebe a resposta da *tag* simultaneamente. Para minimizar a interferência do transmissor no receptor da leitora, antenas distintas podem ser usadas para a transmissão do campo da leitora e para a recepção do sinal da *tag*. Este tipo de configuração de antenas da leitora é chamado de bi-estático. Em aplicações mais sensíveis a custo e tamanho, uma única antena pode ser utilizada, formando a configuração mono-estática, em que a mesma antena transmite e recebe. Neste caso, o receptor deve tratar o forte sinal do transmissor ao qual ele será exposto (DOBKIN, 2008). Outra variação de configuração é o tipo multi-estático, que é uma mistura das configurações mono e bi-estático. O tipo multi-estático tem as suas antenas trabalhando em pares: durante um determinado intervalo de tempo uma antena transmite e outra recebe. No intervalo de tempo seguinte, elas invertem sua função.

Nas leitoras de RFID, a taxa de transmissão de dados é tipicamente inferior a 100 kbps. A taxa de dados recebidos das *tags* é um pouco maior: 640 kbps para *tags* EPC Gen2, que operam na frequência central de 915 MHz (DOBKIN, 2008). Estas taxas definem a banda base de modulação da portadora. Como as leitoras de RFID recebem um sinal refletido como resposta das *tags*, os rádios dos receptores de UHF normalmente são do tipo homodino

(*homodyne*), que não utilizam uma frequência intermediária entre a modulação e a portadora, se tornando mais simples e baratas.

As leitoras mono-estáticas empregam componentes de micro-ondas específicos, como circuladores e acopladores direcionais, que são capazes de selecionar os sinais baseados em sua direção.

Depois de recebido, o sinal emitido pela *tag* passa do módulo de RF para o módulo de controle, onde é digitalizado e submetido a um processador digital de sinais para que seja decifrado. O receptor deve amostrar o sinal adequadamente, apesar da base de tempo irregular da *tag*. Esquemas simples empregam comparação de blocos em um número fixo de pontos super-amostrados. Abordagens mais sofisticadas, principalmente em sistema UHF, usam correlacionadores deslizantes e a Transformada Rápida de Fourier nos dados.

As especificações principais de uma leitora são: sua faixa de frequência de operação, os protocolos de dados e de interfaces aéreas suportados (serão descritos mais adiante) e o tipo de configuração suportada para suas antenas. Na Figura 25 são mostradas uma leitora de UHF e outra de HF com antena em circuito impresso.

Figura 25 - Exemplo de Leitoras UHF (Esquerda) e HF (Direita)



Fonte 5- Sunray e RimaLabs (2013)

3.7 – Antenas

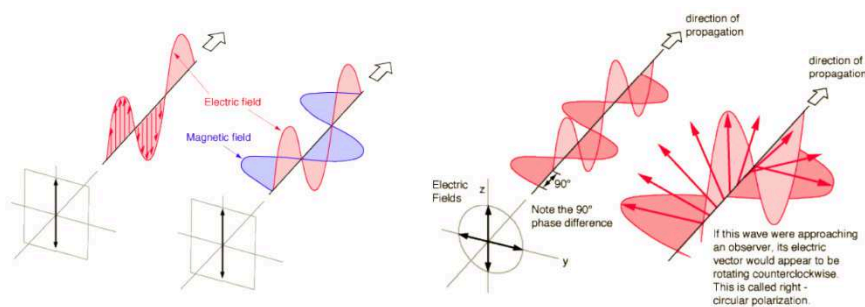
Existem várias definições para antenas. Do ponto de vista de transmissão, DOBKIN (2008) descreve antena como uma estrutura especial arranjada para criar ondas eletromagnéticas a partir de tensões e correntes elétricas que não se cancelam. Fundamentalmente, uma antena é uma maneira de converter as ondas guiadas (presentes em um guia de onda, cabo ou linha de transmissão) em ondas irradiadas que viajam no espaço, ou vice-versa. Os principais parâmetros de uma antena são: padrão de irradiação, diretividade, impedância, ganho, largura de banda, abertura efetiva e polarização.

Um parâmetro da antena de vital importância em RFID é a polarização. Uma onda eletromagnética move elétrons no plano perpendicular à direção de propagação, e não ao longo da direção de propagação. A direção apontada pelo campo elétrico determina a polarização da onda irradiada. Quando esta direção é constante no tempo, a onda é considerada linearmente polarizada. Caso a direção de polarização seja dependente do tempo, onde o campo elétrico gira em torno do eixo de propagação perfazendo 360° a cada comprimento de onda percorrido neste eixo, com amplitude constante, a irradiação é considerada circularmente polarizada. Estas polarizações são esboçadas na Figura 26.

Dependendo do sentido de rotação, a polarização circular pode ser para a direita ou para a esquerda. A polarização linear pode ser horizontal, caso a propagação ocorra paralela ao plano terra, ou pode ser vertical, caso o sinal seja propagado perpendicularmente ao plano terra.

Se os tipos de polarização da antena da leitora e da antena da *tag* não apresentarem uma boa interação, poderá haver um fraco acoplamento do sinal. Muitas antenas de *tags* de RFID são formadas por uma linha de metal. Caso esta linha não esteja alinhada com a direção do campo elétrico emitido pela antena da leitora, a corrente induzida na antena da *tag* será mínima, inviabilizando a alimentação de energia para a *tag*. Caso uma antena de polarização circular seja usada na leitora, a onda irá interagir com uma antena linear da *tag* disposta em qualquer ângulo no plano perpendicular ao eixo de propagação, mas em todo caso, apenas metade da potência do sinal transmitido será recebida, já que a polarização circular é dividida nas componentes vertical e horizontal em cada instante de tempo. Portanto, antenas com polarização circular devem ser usadas apenas quando não for possível garantir a orientação da *tag*, como mostrado na Figura 26.

Figura 26 - Polarização Linear (Esquerda) e Circular (Direita)

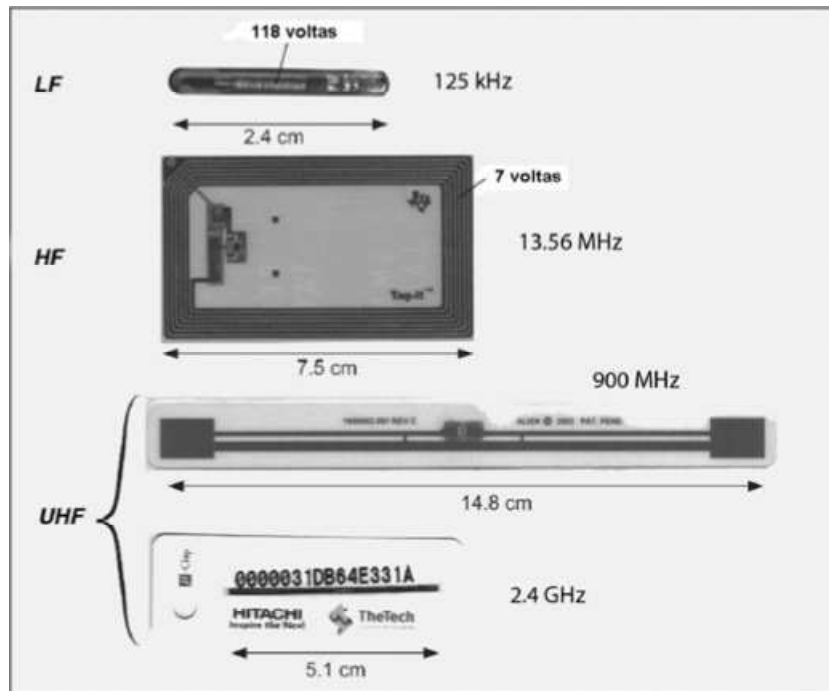


Fonte - DOBKIN (2008)

Em RFID, duas antenas são cruciais: a(s) antena(s) da leitora e a antena da *tag*. Elas operam sob os mesmos princípios, mas os desafios práticos entre elas são bastante distintos, relacionados principalmente com custo e tamanho. Segundo DOBKIN (2008), enquanto uma boa antena de UHF para uma leitora custa em torno de US\$ 150,00, uma *tag* completa, incluindo microchip, antena, substrato, montagem e teste, tem um preço alvo de US\$ 0,05 para aplicações de alto volume em cadeias de suprimento. O tamanho da antena da *tag* também é bastante limitado. Normalmente, as aplicações em diversos setores do planeta exigem *tags* minúsculas, mas o tamanho para a ressonância natural, que é metade do comprimento de onda, é cerca de 16 cm para a faixa de 915 MHz.

As antenas de LF e HF são basicamente utilizadas em aplicações com acoplamento indutivo. Neste caso, as antenas são basicamente bobinas. A tensão induzida em uma bobina é proporcional ao número de espiras, tamanho, e frequência de operação. Em 115 kHz, uma antena de *tag* típica usa pouco mais de 90 - 100 espiras para produzir a tensão necessária para alimentar seu microchip. Em 13,56 MHz, uma *tag* típica do tamanho de um cartão de crédito precisa de 3 a 6 espiras para produzir alguns volts a alguns centímetros de distância (DOBKIN, 2008). Alguns exemplos de *tags* e antenas são mostrados na Figura 27.

Figura 27 - Exemplos de antenas de tags para determinadas frequências

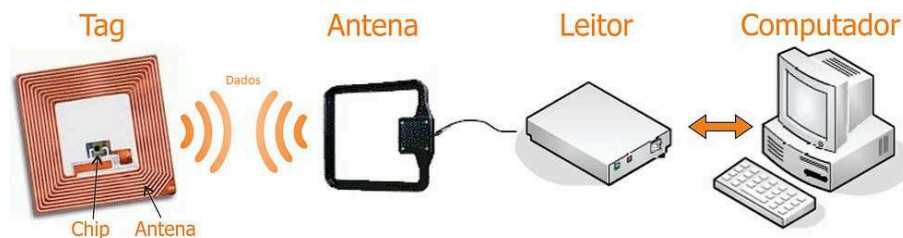


Fonte - DOBKIN (2008)

3.8 – Operação do RFID

Os principais componentes específicos de um sistema de RFID são a “tag” (etiqueta eletrônica), a leitora e sua antena, além do computador que executará o software aplicativo de RFID, conforme é ilustrado na Figura 28. Estes são os componentes que ficam situados na fronteira de um sistema de identificação, como em uma loja, por exemplo. Cada um destes itens será descrito detalhadamente nas seções a seguir.

Figura 28 - Componentes de um sistema RFID

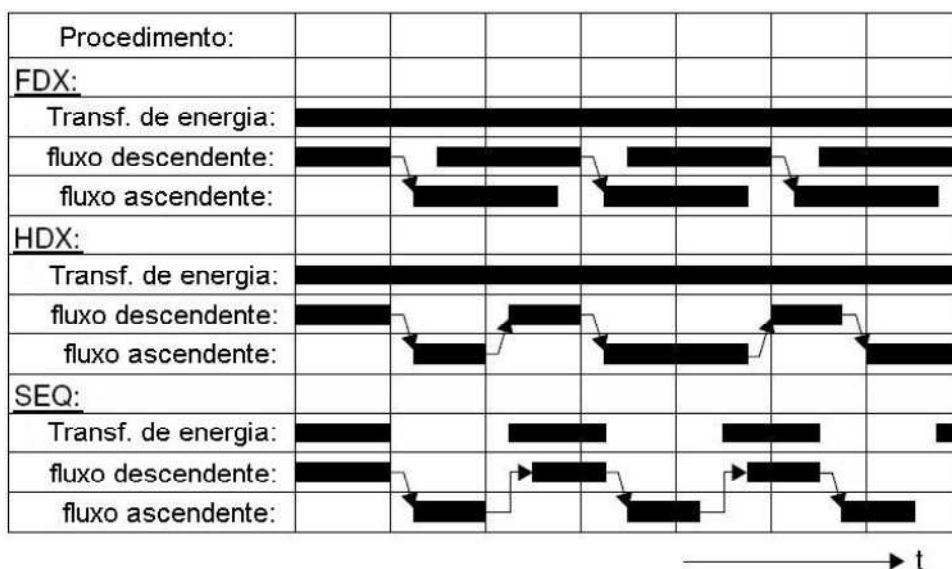


Fonte – HerrTech (2012)

A interação entre a *tag* e a leitora pode ser implementada de várias maneiras, de acordo com o tipo de aplicação e com a frequência de operação. A interação se aplica principalmente na forma de transferir energia para a *tag* e na forma de transferência de dados entre elas.

A transferência de dados entre a *tag* e a leitora pode acontecer através dos procedimentos *half duplex* (HDX), *full duplex* (FDX) e *sequencial* (SEQ) (FINKENZELLER, 2010). Como pode ser visto na Figura 29, a transferência de energia sempre está presente nos procedimentos HDX e FDX, se diferenciando na simultaneidade entre os dois sentidos da comunicação. No modo sequencial, por sua vez, a transferência de energia acontece apenas durante o fluxo de dados no sentido leitora → *tag*. A transferência de dados da leitora para a *tag* é chamada de *downlink*, enquanto a transferência da *tag* para a leitora é denominada *uplink*.

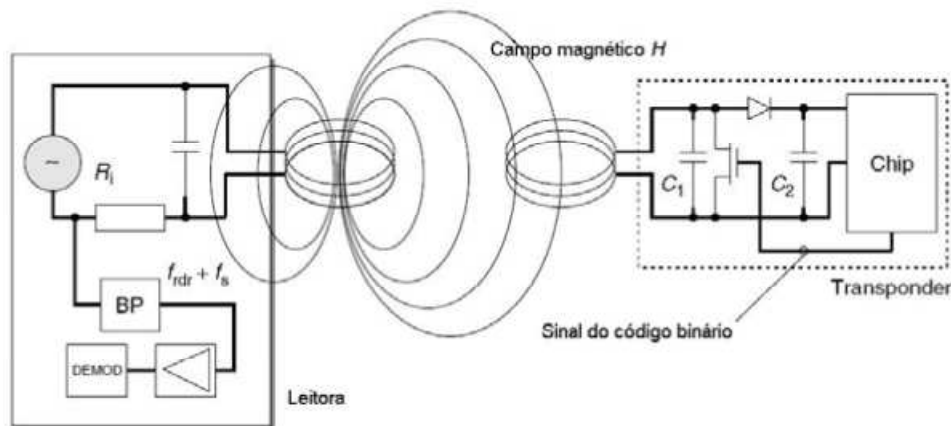
Figura 29 - Sistemas Full Duplex, Half Duplex e Sequencial no tempo



Fonte – FINKENZELLER (2010)

As *tags* que utilizam o acoplamento indutivo são, normalmente, do tipo passivo. Este tipo de acoplamento é usado quando o comprimento de onda da frequência utilizada pela leitora é bem maior que a distância entre a leitora e a *tag*, já que neste caso, o campo eletromagnético pode ser tratado apenas como um campo magnético, como é mostrado mais detalhado na Figura 30 (Acoplamento indutivo simplificado – Figura 19). Uma tensão alternada é gerada na antena da *tag* por indutância, através da ressonância gerada pelo circuito LC sintonizado, formado pela antena e um capacitor em paralelo. Como este acoplamento pode ser considerado como um transformador, o secundário (bobina da antena da *tag*) age como uma carga para o primário (bobina da leitora). Desta forma, a transferência de dados da *tag* para a leitora se dá por modulação de carga.

Figura 30 - Alimentação da tag a partir do acoplamento indutivo



Fonte – FINKEZELLER (2010)

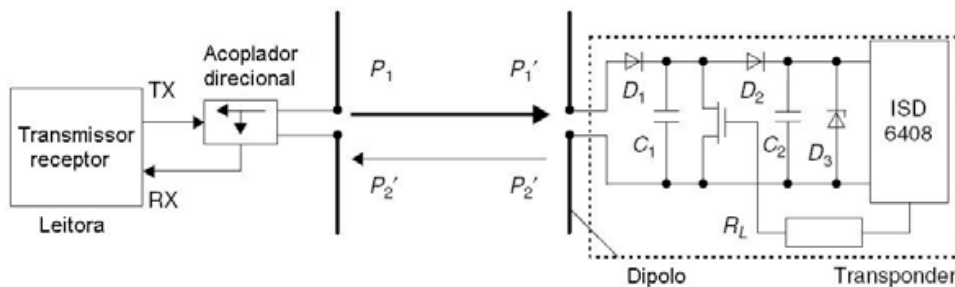
Sistemas de RFID em que a distância entre a leitora e a tag é maior que 1 metro são chamados de sistemas de longo alcance (FINKEZELLER, 2010). Estes sistemas operam tipicamente na faixa de UHF e podem utilizar o acoplamento eletromagnético refletido (backscatter). A energia que a tag precisa é fornecida pelo campo eletromagnético emitido pela leitora, que gera uma tensão alternada na antena da tag e, então, esta tensão é retificada. De acordo com Finkenzeller (2010) dada a frequência f , a distância r entre a leitora e a tag, o ganho da antena da leitora G_T e o ganho da antena da tag G_R , a perda a_F no trajeto em espaço livre é dada por:

$$a_F = -147.6 + 20 \log(r) + 20 \log(f) - 10 \log(G_T) - 10 \log(G_R)$$

Portanto, se uma tag que consome $50\mu\text{W}$ de energia estiver numa configuração em que a perda no espaço livre é de 40 dB, precisaria de uma leitora que transmitisse uma potência de $P_S = 0,5\text{W}$ EIRP (*Effective Isotropic Radiated Power*).

Para transmitir dados para a leitora, a tag reflete parte do sinal recebido, modulando-o através de uma carga resistiva (ou capacitiva), como mostrado na Figura 31 (Acoplamento capacitivo simplificado – Figura 20).

Figura 31 - Operação de uma tag com acoplamento capacitivo ou backscatter

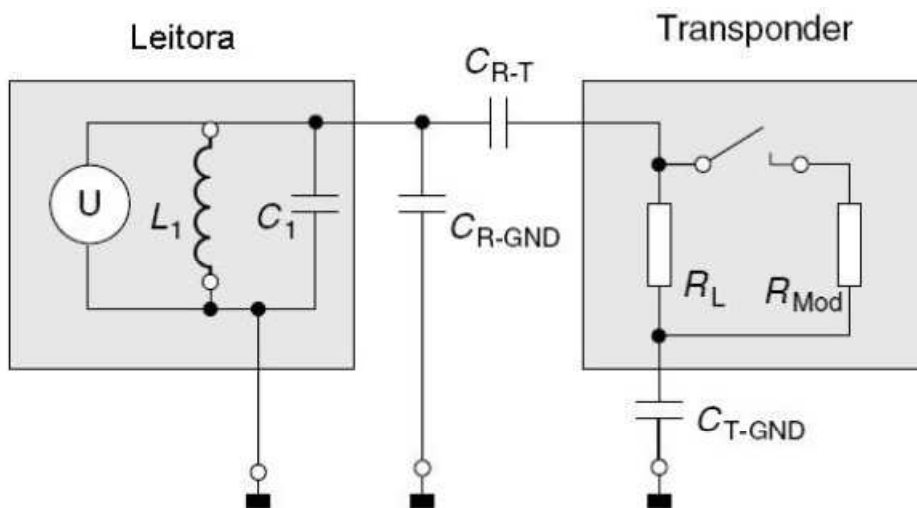


Fonte – FINKENZELLER (2010)

Os sistemas de acoplamento próximo são projetados para distâncias de leitura entre 1 mm e 1 cm. A tag é então inserida na leitora ou colocada sobre sua antena para ser lida. Como este tipo de sistema não é de interesse para este trabalho, ele não será detalhado.

Nos sistemas de acoplamento elétrico (capacitivo), as leitoras geram campos elétricos intensos em suas antenas, que são formadas por uma grande placa de metal (eletrodo). Uma tensão elevada (de centenas a milhares de volts) é gerada no eletrodo através de um circuito LC sintonizado, conforme mostrado na Figura 32, formado por um indutor L1 e pelo paralelo de um capacitor interno C1 e a capacitância formada entre o eletrodo e o plano terra CR-GND.

Figura 32 - Circuito equivalente de um sistema RFID com acoplamento capacitivo



Fonte – IndusMelec (2013)

A antena da tag é feita de duas superfícies condutivas (eletrodos) dispostas em um plano. Quando a tag é submetida ao campo da leitora, forma-se um capacitor CR-T entre a

antena da leitora e a *tag*, como também um capacitor CT-GND entre a *tag* e o plano terra. A modulação de carga se dá através do chaveamento do resistor RMOD.

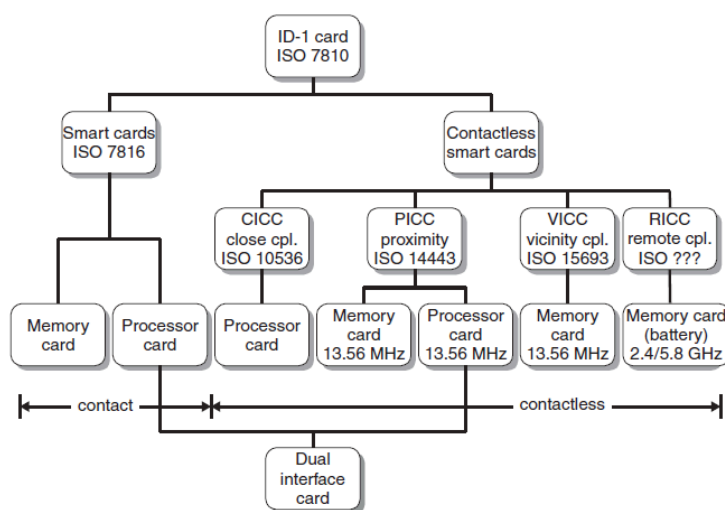
Em todos os casos, a transmissão de dados entre a leitora e a *tag* se dá através dos procedimentos de modulação de sinal usuais. As modulações usuais são por chaveamento de: amplitude (ASK), frequência (FSK) e de fase (PSK), sendo que a ASK é a mais usada por ser a mais fácil de realizar a demodulação.

3.9 – Padrões e Protocolos

A medida que os sistemas de RFID foram evoluindo e sendo utilizados por um número cada vez maior de empresas, os padrões começaram a ser imprescindíveis para garantir a interoperabilidade entre leitoras e *tags* dos vários fabricantes no mercado, como também a viabilidade econômica, através da redução de custos. A ISO (organização internacional para padronização) definiu vários padrões para interface aérea, protocolo de dados e para aplicações de RFID, começando pelos sistemas de LF e HF.

Conforme descreve FINKENZELLER(2010), foram definidos os padrões ISO 11784, 11785 e 14223 para identificação de animais, os padrões ISO 14443 (proximidade) e 15693 (vizinhança) para cartões inteligentes sem contato (mostrados na Figura 33), ISO 69873 para ferramentas, ISO 10374 para identificação de contêineres, VDI 4470 para sistemas antifurto e a série ISO 18000 para gerenciamento de produtos.

Figura 33 - Família de padrões para cartões inteligentes com e sem contato



Fonte 6 – FINKENZELLER (2003)

Os padrões ISO 14443 e 15693 foram criados na década de 90 para sistemas que operam em 13,56 MHz. Eles foram bastante utilizados em cartões sem contato para aplicações de controle de acesso e de bilhetagem eletrônica em ônibus urbanos. Em Fortaleza, a empresa Fujitec ainda utiliza esta tecnologia nos sistemas implantados em várias cidades no Brasil e Colômbia. A NXP (*spin-off* da Philips), *Infineon* (*spin-off* da Siemens) e a *Texas Instruments* desenvolveram vários componentes para fabricação de *tags* e de leitoras nestes padrões.

A série ISO 18000 é dividida em várias partes para definir o padrão dos parâmetros de interface aérea em cada faixa de frequência onde RFID é usada. A parte 6 trata da interface aérea na faixa de 860-930 MHz, definida inicialmente pelos padrões ISO 18000- 6A e -6B. Entretanto, estes padrões são incompatíveis entre si e incompatíveis com os padrões definidos pela *EPCglobal*, causando alguns problemas entre sistemas. No final de 2004, a GS1 e a ISO iniciaram um plano de unificar os padrões de interface aérea, que finalizou em 2006 com a definição da especificação EPC Classe I Geração 2 (conhecida como Gen2) como o padrão de interface aérea na norma ISO 18000-6C (GLOVER; BHATT, 2006).

Como já foi apresentada na seção 3.3, a GS1 surgiu a partir da união das administradoras mundiais dos padrões de códigos de barras. Atualmente, a *EPCglobal* é o sistema global de padrões administrado pela GS1 que combinam RFID, infraestrutura de redes de comunicação e o EPC, permitindo a identificação imediata de um produto em toda a cadeia de suprimentos no mundo (GS1 PRODUCTS, 2010). A GS1 está presente em 108 países, inclusive no Brasil (GS1 OVERVIEW, 2010).

Nos primeiros protocolos de leitura de *tags*, o ruído presente no sinal captado pelas antenas das leitoras eventualmente conseguia atuar aleatoriamente até formar um código válido pelo protocolo, mas que de fato não correspondia a uma *tag* real. Isto é o denominado de *tag* fantasma.

Um mapa de memória de uma *tag* é a estrutura de dados que define como os bytes estão organizados fisicamente na memória que compõe o chip da *tag*. Normalmente, a memória é dividida em bancos, que são compostos por um grupo específico de bytes com características específicas de acesso, funcionalidades e procedimentos de escrita e/ou leitura.

Os padrões EPC classe 0 e classe I apresentam algumas fragilidades. *Tags* fantasmas surgiam nas leituras (devido ao fraco algoritmo de checagem de erro), alta interferência quando mais de uma leitora está presente na mesma área e incompatibilidade de mapas de memórias entre as *tags*. O padrão EPC Classe I Geração 2, ou simplesmente Gen2, trouxe uma série de benefícios, além da unificação dos padrões, conforme descreve DOBKIN (2008):

- Até quatro sessões de *tag* baseadas em números aleatórios de 16 bits, independentes do número da *tag*, permitindo que a *tag* se comunique com até quatro leitoras simultaneamente, sem interferência entre elas, utilizando canais de frequência diferentes para o sinal de resposta para cada leitora;
- Senhas longas para travar e para inutilizar uma *tag*;

- Leituras fantasmas de *tags* foram praticamente eliminadas;
- Pouca interferência entre leitoras nas aplicações onde mais de uma leitora está presente na mesma área (*Dense Reader Mode*);
- Padronização dos mapas de memória das *tags*, permitindo a interoperabilidade das operações de leitura e escrita;
- Flexibilidade de bloquear bancos de memórias da *tag* temporariamente ou permanentemente.

O padrão EPC Gen2 especifica os bancos de memória e suas funções. Existem dois bancos obrigatórios e dois opcionais. O banco 0 contém (no mínimo) as senhas KILL e ACCESS de 32 bits cada. A senha KILL é usada para tornar a *tag* inoperante permanentemente. A senha ACCESS habilita a *tag* a responder aos comandos de leitura e escrita. O banco 1 contém o código EPC, o identificador do seu tamanho, informações opcionais sobre a *tag* e o código CRC16 usado para checagem de erro do código EPC. O banco 2 é opcional e contém informações específicas sobre a *tag*, em vez do produto que ela identifica. Por último, o banco 3 é livre e normalmente destinado para dados do usuário ou de uma aplicação específica. Cada banco de memória pode ser travado independentemente, permitindo que sejam restritas as operações de leitura e escrita em cada banco de memória.

O código EPC (*Electronic Product Code*) permite identificar objetos, cargas, lugares, bens e outras entidades cujo uso deve ser rastreado com RFID ou códigos de barras através do serviço EPC Network da GS1 (GS1 OVERVIEW, 2010). No padrão EPC Gen2, ele é tipicamente composto por 96 bits divididos em 4 campos, conforme mostrado na Figura 34.

Figura 34 - Formato de um código EPC



Fonte – Alessandro Cunha (2016)

3.10 – Aplicações do RFID

Cada vez mais, as aplicações de RFID vêm se disseminando nos mais diversos ramos de atividade da indústria e dos serviços. Algumas áreas já utilizam esta tecnologia há algum tempo e apresentam vários exemplos de aplicações. Com a evolução da RFID e dos dispositivos que compõem os sistemas, além do aumento da oferta de provedores de equipamentos e soluções, novas áreas de aplicação começam a surgir. Conforme LAHIRI (2005) classifica, as aplicações de RFID podem ser divididas em dois blocos: as aplicações preexistentes e as aplicações emergentes.

As aplicações preexistentes são aquelas já bem disseminadas e são divididas nos seguintes tipos: rastreamento de itens, controle e monitoração de inventário, gerenciamento e monitoração de patrimônio, sistemas antifurto, pagamento eletrônico, controle de acesso e sistemas anti-falsificação.

No **rastreamento de itens**: estes recebem uma *tag* contendo um identificador único, que é lido em determinados pontos de checagem à medida que o item se desloca pelos lugares e/ou fases do processo, permitindo saber a data e a hora da passagem por estes pontos, além de possibilitar a inserção de dados adicionais sobre o processo. As aplicações típicas deste tipo são: rastreamento de bagagem nas companhias aéreas, gerenciamento da cadeia de suprimentos e rastreamento de materiais perigosos. Exemplos dessas aplicações são: rastreamento de bagagens na British Airlines em 1999 e na Delta Airlines em 2003, gerando uma precisão de até 99%, comparado com apenas 85% com códigos de barras; exigência de rastreamento de produtos em nível de paletas na rede Wal-Mart em 2005 e na rede Metro na Alemanha ; sistema de rastreamento de produtos químicos implantado pela IBM em suas fábricas em Vermont, Nova Iorque e Quebec (LAHIRI, 2005); rastreamento de corredores em competições esportivas (FINKENZELLER, 2010).

Na **monitoração e controle de inventário**, os itens a serem monitorados recebem uma *tag* contendo um identificador único. Periodicamente, ciclos de leitura são realizados para identificar a presença ou ausência de cada item do inventário. Exemplos dessas aplicações são: prateleiras inteligentes (a serem mais detalhadas a seguir) e gerenciamento de inventário de peças em fábricas de automóveis e de aviões (LAHIRI, 2005).

No **gerenciamento e monitoração de patrimônio**, os bens de patrimônio a serem monitorados recebem uma *tag* contendo um identificador único. Periodicamente, ciclos de leitura são realizados para identificar a localização e outras propriedades do patrimônio em tempo real. Exemplos dessas aplicações são: gerenciamento de frota, em que os veículos recebem uma *tag* com seus dados, que são identificados por leitoras instaladas em locais estratégicos, como portões de acesso, bombas de combustível e áreas de manutenção, permitindo monitorar o uso e controlar o acesso a determinados locais ou serviços (LAHIRI, 2005); outro exemplo de aplicação deste tipo é o rastreamento de animais com o procedimento chamado de *chipping*, descrito por Campbell et al. (2006), em que eles recebem um implante subcutâneo de uma *tag* passiva, permitindo que as informações relativas a seu

dono, vacinação e demais dados do animal podem ser lidos e acompanhados pelos envolvidos em seu trato.

Em **sistemas antifurto**, os itens a serem monitorados recebem uma *tag*. Locais de risco, como pontos de saída ou de uso do item, recebem leitoras para identificar o furto. Opcionalmente, a *tag* pode ser removida ou desabilitada após o pagamento do item, como também pode detectar o movimento indevido do item. Exemplos dessas aplicações são: a vigilância eletrônica de itens (EAS), muito comuns em lojas de varejo, que utilizam uma *tag* passiva de 1 bit de informação; outro exemplo similar em lojas de varejo é a utilização de uma *tag* passiva de HF reutilizável, contendo detalhes do produto (preço, código EPC, etc.), sendo retiradas no momento do pagamento; outro exemplo deste tipo de aplicação é o sistema de imobilização presente na maioria dos automóveis de hoje, que utilizam uma *tag* LF na chave do veículo e uma leitora na direção, permitindo a ignição do motor somente após reconhecer a chave válida.

Nas **aplicações de pagamento eletrônico**, o usuário recebe uma *tag* contendo um identificador único. O cartão é lido em um POS5, que valida o usuário e autoriza o pagamento. Exemplos dessas aplicações são: sistema *Speedpass* da ExxonMobil, uma distribuidora de combustíveis dos EUA, no qual o usuário utiliza uma *tag* cilíndrica, aproximando-a de uma bomba de combustível, liberando o abastecimento do veículo; outro exemplo comum deste tipo de aplicação é o pagamento eletrônico de pedágio, como os sistemas *E-Z Pass* (Nordeste dos EUA), *SunPass* (Flórida) e o Sem Parar (São Paulo).

As aplicações de **controle de acesso** estão entre as mais tradicionais no uso de RFID. Neste tipo de aplicação, o usuário utiliza uma *tag* contendo um identificador único e os dados associados a ele. Ao chegar aos pontos de controle de acesso, a *tag* é lida e, se o usuário for autorizado, seu acesso é permitido. Além do uso popular deste tipo de aplicação no controle de acesso a empresas, o controle de acesso com RFID em aplicações com maior grau de segurança pode fazer o uso de *tags* aplicadas sob a pele dos usuários, como é o caso do anúncio descrito por LAHIRI (2005), feito pelo governo do México em 2004 para controlar o acesso dos empregados ao seu centro de computação de 30 milhões de dólares.

Uma grande aplicação com RFID no Brasil que envolve um pouco de cada um dos conceitos das aplicações já descritas é o SINIAV – Sistema Nacional de Identificação de Veículos. Ele fará parte da vida de todo proprietário de veículos em breve. O SINIAV foi criado pela resolução nº 212/2006 do CONTRAN e alterado pela resolução nº338/2009 do mesmo órgão, publicada em março de 2010 (CONTRAN, 2010). Entre os objetivos deste sistema, estão: acompanhamento do ciclo de vida do veículo, fiscalização urbana, gestão de trânsito, fiscalização rodoviária, recuperação de veículos, gestão de meios de pagamento, seguro de veículos, transporte de cargas e logística. A faixa de frequência escolhida é entre 915 e 928 MHz, no padrão ISO 18000-6C. As *tags* devem ser lidas com o veículo em movimento em velocidade de até 160 Km/h. Apesar da resolução não restringir o uso de *tags* passivas, o desempenho especificado provavelmente só deverá ser atingido com *tags* semipassivas.

4 – Projeto

4.1 – Protótipo

Para se obter uma base de como o sistema RFID funciona fisicamente, foi construído um protótipo, no qual foi utilizado vários componentes eletrônicos de fácil acesso e de valores razoavelmente baixos que serão apresentados:

4.1.2 - Microcontrolador

Microcontrolador (mostrado na figura 35) é um pequeno computador (*SoC*) num único circuito integrado o qual contém um núcleo de processador, memória e periféricos programáveis de entrada e saída. A memória de programação pode ser *RAM*, *NOR flash* ou *PROM* a qual, muitas vezes, é incluída no chip. Os microcontroladores são concebidos para aplicações embarcadas, em contraste com os microprocessadores utilizados em computadores pessoais ou outras aplicações de uso geral.

Microcontroladores são usados em produtos e dispositivos automatizados, como os sistemas de controle de automóvel, dispositivos médicos implantáveis, controles remotos, máquinas de escritório, eletrodomésticos, ferramentas elétricas, brinquedos e outros sistemas embarcados. Ao reduzir o tamanho e o custo em comparação a um projeto que usa um dispositivo micro processado, microcontroladores tornam-se econômicos para controlar digitalmente dispositivos e processos. Microcontroladores de sinal misto são comuns, integrando componentes analógicos necessários para controlar sistemas eletrônicos não digitais.

O seu consumo de energia é relativamente baixo, normalmente, na casa dos miliwatts e possui habilidade para entrar em modo de espera (*Sleep* ou *Wait*) aguardando por uma interrupção ou evento externo, como, por exemplo, o acionamento de uma tecla, ou um sinal que chega via uma interface de dados. O consumo destes microcontroladores em modo de espera pode chegar na casa dos Nano watts, tornando-os ideais para aplicações onde a exigência de baixo consumo de energia é um fator decisivo para o sucesso do projeto.

De forma diferente da programação para microprocessadores, que em geral contam com um sistema operacional e um BIOS, o programador ou projetista que desenvolve sistemas com microcontroladores, geralmente, cria todo programa que será executado pelo sistema ou pode usar um sistema operacional próprio para microcontroladores chamado de RTOS.

Figura 35 - Microcontrolador Arduino Uno



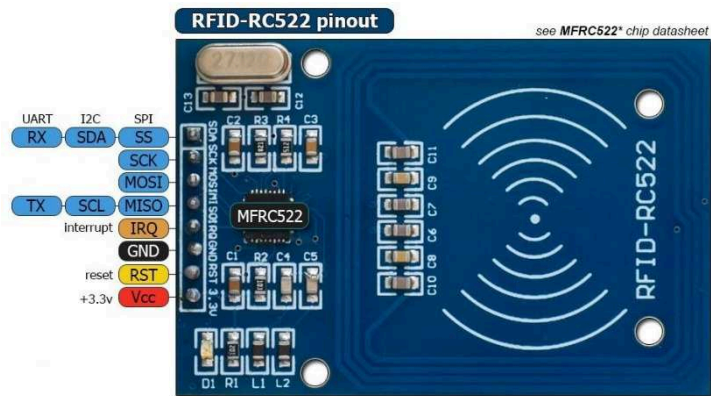
Fonte - Arduino Store (2014)

4.1.3 – Módulo RFID RC522

O MFRC522 (mostrado na figura 36) é um leitor / gravador altamente integrado para comunicação sem contato a 13,56 MHz. O leitor MFRC522 suporta ISO / IEC 14443 A / MIFARE e NTAG.

O transmissor interno do MFRC522 é capaz de acionar uma antena de leitura / gravação projetada para comunicação com cartões ISO / IEC 14443 A / MIFARE e transponders sem circuito adicional ativo. O módulo receptor fornece uma implementação robusta e eficiente para a desmodulação e decodificação de sinais de cartões e transponders compatíveis com ISO / IEC 14443 A / MIFARE. O módulo digital gerencia a funcionalidade completa de detecção de quadro e detecção de erros (paridade e CRC) ISO / IEC 14443 A.

Figura 36 - Módulo MFRC522



Fonte – Fritzing (2011)

4.1.4 – Tag's de 13,56Mhz

Uma *tag* de RFID (mostrado na figura 37) é um dispositivo que pode armazenar e transmitir dados para uma leitora sem a necessidade de contato, usando ondas de rádio. Usualmente, a *tag* também é chamada de transponder, derivado dos termos em inglês *transmitter e responder* (transmissor e respondedor). O propósito de uma *tag* de RFID é anexar fisicamente a um objeto os dados pertinentes a ele. Desta forma, pode-se chamar a *tag* de etiqueta eletrônica.

Figura 37 - Tag's de 13,56Mhz



Fonte - Vida de Silício (2009)

4.1.5 – Buzzer

Um *Buzzer* ou *Beeper* (mostrado na figura 38) é um dispositivo de sinalização de áudio, que pode ser mecânico, eletromecânico ou piezoelétrico (piezo para curto). Usos típicos dos *Buzzers* e *Beepers* incluem dispositivos de alarme, temporizadores e confirmação

de entrada do usuário, como um clique do mouse, pressionamento de tecla ou passagem de cartões magnéticos ou RFID's.

Figura 38 - Buzzer



Fonte 7- Baú da eletrônica (2012)

4.1.6 – LED

O diodo emissor de luz (mostrado na figura 39), também conhecido pela sigla em inglês LED (*Light Emitting Diode*), é usado para a emissão de luz em locais e instrumentos onde se torna mais conveniente a sua utilização no lugar de uma lâmpada.

Especialmente utilizado em produtos de microeletrônica como sinalizador de avisos, também pode ser encontrado em tamanho maior, como em alguns modelos de semáforos. Também é muito utilizado em painéis de LED, cortinas de LED, pistas de LED e postes de iluminação pública, permitindo uma redução significativa no consumo de eletricidade.

Figura 39 - LED's

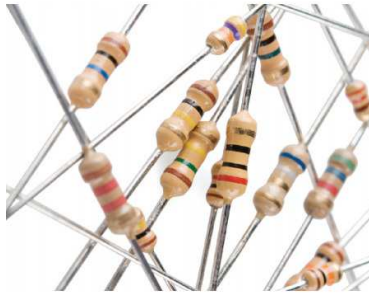


Fonte 8- Mundo da elétrica (2010)

4.1.7 – Resistores

Resistor (mostrado na figura 40) é um dispositivo elétrico muito utilizado em eletrônica, ora com a finalidade de transformar energia elétrica em energia térmica por meio do efeito joule, ora com a finalidade de limitar a corrente elétrica em um circuito.

Figura 40 - Resistores



Fonte 9- Vida de Silício (2011)

4.1.8 – Jumpers

Jumper (mostrado na figura 41) é um pequeno condutor utilizado para conectar dois pontos de um circuito eletrônico. São geralmente utilizados para configurar placas de circuitos, como placas-mãe de computadores.

Figura 41 - Jumpers

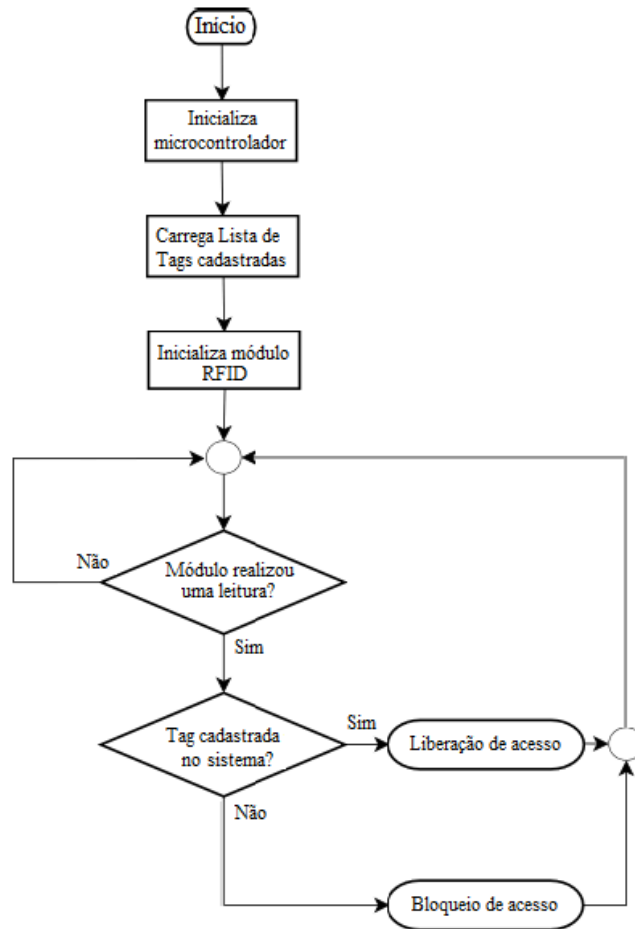


Fonte– AliExpress (2015)

4.1.9 – Funcionamento

O funcionamento do protótipo foi feito para ser de simples entendimento junto de seu fluxograma que foi demonstrado na figura 42.

Figura 42 - Fluxograma do protótipo



Fonte - Autoria própria (2018)

Sendo:

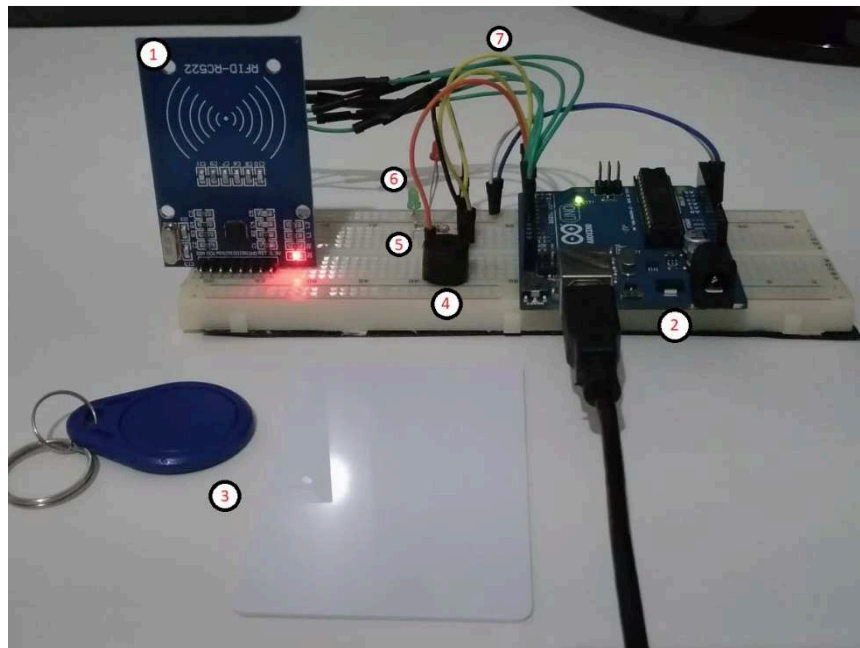
Liberação de acesso – é mostrado no monitor serial o código da *tag cadastrada* no sistema, acende-se o *LED* de liberação (*LED* verde) e é emitido um aviso sonoro de que foi liberado.

Bloqueio de acesso – é mostrado no monitor serial o código da *tag* e a observação de que ela não está cadastrada no sistema, acende-se o *LED* de bloqueio (*LED* vermelho) e é emitido um aviso sonoro de que foi bloqueado.

4.1.10 – Resultado

O protótipo montado, com suas ligações e componentes, é demonstrado na figura 43.

Figura 43 - Protótipo



Fonte - Autoria própria (2018)

- 1- Módulo MFRC522
- 2- Microcontrolador Arduino Uno
- 3- *Tag's*
- 4- *Buzzer*
- 5- Resistores
- 6- *Led's*
- 7- *Jumpers*

4.2 – Estudo do caso específico

Muitas instituições, como a nossa, ainda adotam sistemas manuais para o controle de acesso e de monitoramento dos veículos em seus estacionamentos e, conseqüentemente, enfrentam problemas decorrentes de erros humanos. A automatização do controle de acesso a estacionamentos é uma solução vantajosa, pois evitam problemas com acesso não autorizado, mau aproveitamento das vagas, estacionamentos indevidos e evitar possíveis furtos, além de

disponibilizar em tempo real informação sobre a quantidade de vagas livres e permitir consultar quais usuários acessaram o estacionamento em determinado período.

Para o caso de nossa instituição de ensino, foram estimados os números de vagas demonstrados na Tabela 4:

Tabela 4 - Tabela indicativa de vagas

Usuários e veículos	Quantidade de vagas
Automoveis (Alunos)	120
Automoveis (Professores)	50
Motocicletas	120
Total	290

Fonte - Autoria própria (2018)

Essa estimativa foi avaliada pela área disponível do Campus JUTA para uso de estacionamento. No qual a área fica demonstrada pela figura 44.

Figura 44 - Campus JUTA com vista superior



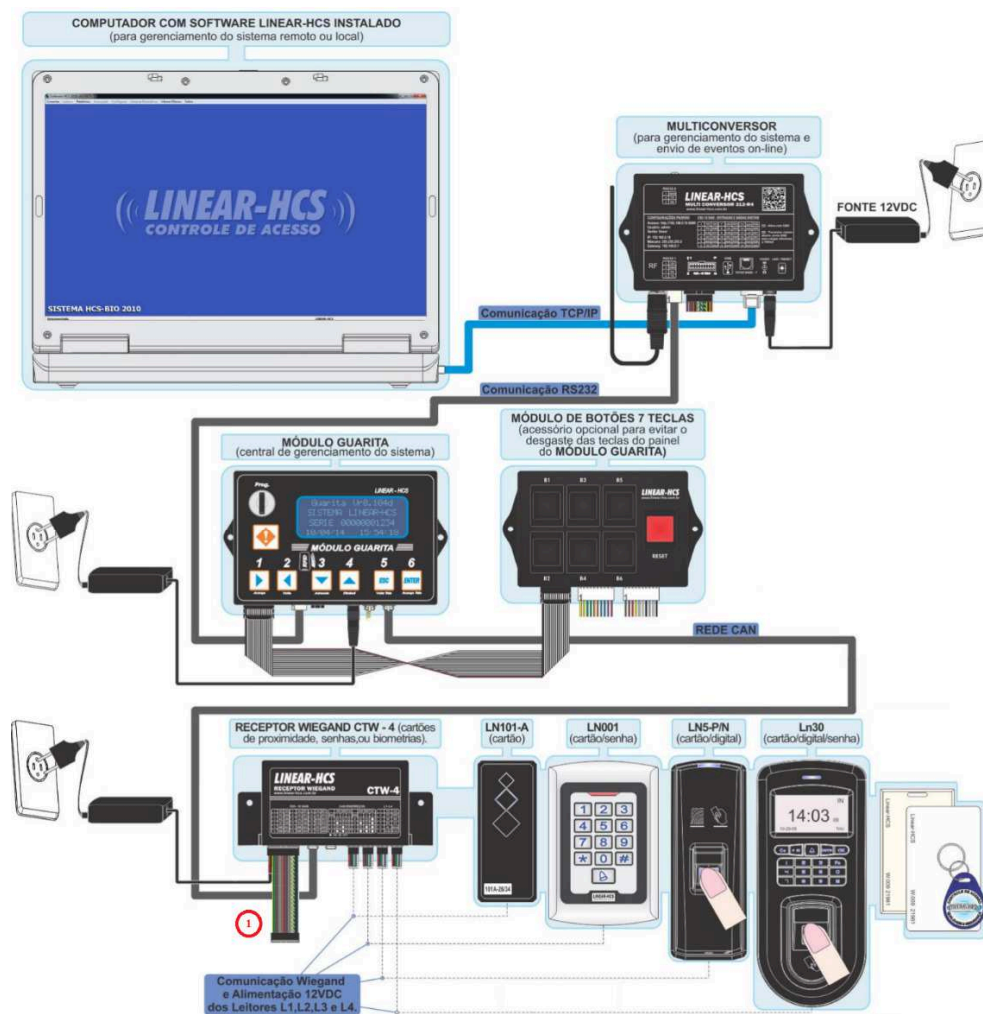
Fonte - Google Maps (2017)

4.3 – Projeto Final

O projeto será estudado e analisado a partir dos equipamentos da empresa Linear HCS, sendo uma empresa especializada no ramo de controle de acesso. Todos os componentes do sistema, sua organização, sua visão geral e uma tabela de valores serão apresentados a seguir.

Os componentes e conexões para o sistema completo de controle de acesso é mostrado na figura 45.

Figura 45 - Componentes do projeto



Fonte - Linear HCS (2016)

Sendo:

1 – Ligação do receptor com a central de laço indutivo da cancela, mostrada na figura 55.

Serão apresentadas as informações sobre cada componente e sua função. Em seguida, será apresentado o software de controle, cadastro e monitoramento para o sistema.

4.3.1 – Modulo Guarita

O Módulo Guarita 2010® (mostrado na figura 46) é um equipamento desenvolvido para gerenciar o controle de acesso em condomínios residenciais ou comerciais junto aos receptores e dispositivos linear HCS, que podem ser dos tipos:

- *Tag* ativo,
- *Tag* UHF
- Controle Remoto (ou *Tag* Táctil),
- Cartões *RFID* (opção senha).

O cadastramento dos usuários dispõe de campos distintos para identificação, sendo 18 caracteres para nome, seleção de 32 marcas (pré-definidas) de fabricantes dos veículos, 16 cores (conforme descrição Denatran) e 7 caracteres alfanuméricos para placa.

O Módulo guarita dispõe de diversos recursos para auxiliar na segurança do patrimônio e dos usuários do sistema, como por exemplo:

-Pânico de usuário, que pode ser disparado por meio de cartões RFID, Controles Remoto e Tags Tácteis

- Desperta Porteiro
- Veículo carona
- Pânico entre condomínios
- Clonagem

O módulo emite um alerta sempre que houver tentativa de clonagem de um controle remoto. Os alertas podem ser gerenciados pelo porteiro / administrador que o receberá por meio sonoro e visual diretamente painel do Módulo Guarita, pode ser expandido para computadores em rede, centrais de monitoramento ou outros dispositivos de alarme. Opcionalmente existem modems para envio de dados e alarmes por GPRS.

Figura 46 - Módulo guarita



Fonte - Linear HCS (2015)

O Módulo Guarita pode, em conjunto com os receptores dos dispositivos, funcionar em:

- Modo de comando de abertura direta do portão ou fechadura (pelo acionamento do dispositivo do usuário)

- Apenas indicar / sinalizar ao porteiro qual foi o usuário que fez o acionamento, deixando a operação de efetiva abertura a cargo do porteiro / administrador, inclui a opção de liberação da abertura pelo porteiro somente durante tempo ajustável após o acionamento do dispositivo do usuário, aumentando a segurança do sistema.

Pode-se controlar a quantidade de vagas por usuário, vinculando uma vaga a cada dispositivo cadastrado quando se utiliza controles remotos como dispositivo de acesso. Nesse modo de funcionamento, ao ocupar a vaga o dispositivo não conseguirá acessar o portão de entrada do condomínio sem ter deixado o local usando o dispositivo de acesso. Para sistemas mais complexos ou onde cada usuário possa ter mais dispositivos de acesso que as vagas que dispõe, é necessário utilizar um computador com programa de controle de acesso específico.

Todos os eventos ficam armazenados na memória interna do equipamento e podem ser extraídos por backup realizado manualmente ou automaticamente em cartão tipo “SD CARD” ou através de um computador com software gratuito.

4.3.1 – Multiconversor

O Multiconversor, mostrado na figura 47, serve para interligar o Módulo Guarita ao computador com o software principal do sistema.

Figura 47 - Multiconversor



Fonte - Linear HCS (2014)

4.3.2 – Módulo Botoeira

Sendo um equipamento opcional, o módulo botoeira mostrado na figura 48, é um dispositivo que pode ser acoplado ao Módulo Guarita para acionamento de portões e reset, com registros dos eventos de abertura feitos pelo porteiro.

Figura 48 - Módulo Botoeira



Fonte - Linear HCS (2014)

4.3.3 – Receptor CTW-4

O Receptor CTW-4 Linear-HCS, mostrado na figura 49, foi desenvolvido para gerenciar o controle de acesso em condomínios residenciais ou comerciais em conjunto com os Leitores Wiegand RFID, Teclado de Senha ou Leitores Biométricos Linear-HCS e Módulos Guarita Linear-HCS 2010. Este equipamento dispõe de recursos especiais para auxiliar na segurança do patrimônio e dos usuários do sistema, como por exemplo, o encaminhamento de eventos de Veículo Carona, Pânico e eventos de acesso enviados em tempo real ao Módulo Guarita Linear-HCS 2010 por meio da rede CAN.

Pode funcionar em modo de acionamento com autenticação, fazendo necessário que um usuário cadastrado realize um acionamento através do leitor (que não acionará o portão) e habilitará a tecla de acionamento do portão correspondente na guarita temporariamente, aumentando a segurança do sistema.

Cada receptor CTW-4 pode comandar até quatro portas, portões ou cancelas e dispõe de um sistema de endereçamento CAN, que possibilita durante o cadastramento do cartão /chaveiro, restringir o acesso do mesmo a um ou mais receptores da rede, de acordo com seu endereçamento CAN de 1 a 8.

Figura 49 - Receptor CTW-4



Fonte - Linear HCS (2012)

4.3.4 - Leitor *RFID* Wiegand L101-A

O Leitor *RFID* Wiegand LN101-A foi desenvolvido com a finalidade de uso no sistema de controle de acesso por cartões e chaveiros de proximidade. Funciona interligado ao receptor CTW-4 e Módulo Guarita Linear HCS, tendo como função, ler os cartões ou chaveiros de proximidade e transmitir as informações ao sistema para processamento e validação do acesso. O Leitor LN-101-A conta o recurso de sinalização de status, enviado por meio de um *buzzer* interno e *leds* coloridos, auxiliando no reconhecimento das respostas enviadas pelo sistema durante o acionamento com um dispositivo (cartão ou chaveiro) de proximidade.

Figura 50 - Leitor L101 - A



Fonte 10 - Linear HCS (2015)

4.3.5 – Controladora digital de acesso LN5 – P

A controladora foi desenvolvida com a finalidade de uso no sistema de controle de acesso por cartões, chaveiros de proximidade e biometria. Funciona interligado ao receptor CTW-4 e Módulo Guarita Linear HCS, tendo como função, ler os cartões, chaveiros de proximidade ou biometria e transmitir as informações ao sistema para processamento e validação do acesso. Assim como o Leitor LN-101-A a controladora conta com recursos de sinalização de status.

Figura 51 - Controladora LN5 - P

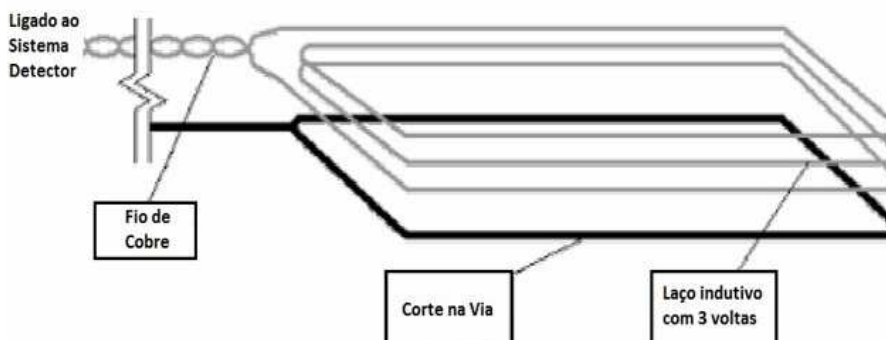


Fonte - Linear HCS (2016)

4.3.6 – Laço indutivo

O sistema de detecção de veículos mais comum no Brasil é o que utiliza laço indutivo (também conhecido como DLI – Detector por laço indutivo), que capta mudanças na indutância de uma bobina instalada no revestimento asfáltico quando um veículo (metálico) passa por sobre ela. Esta bobina é mais conhecida como laço indutivo e é feita com fio de cobre isolado de 1,5 a 2,5 mm de diâmetro que geralmente é disposto de forma retangular fazendo duas ou mais voltas de acordo com a Figura 52. A instalação do laço indutivo é feita realizando-se cortes rasos no pavimento onde ele é colocado e em seguida coloca-se um material selante, como asfalto ou cimento, para cobrir os fios. O laço indutivo é conectado a uma placa eletrônica com um circuito oscilador. Esta placa também possui um microcontrolador que monitora a frequência do conjunto formado pelo circuito oscilador e o laço indutivo e é denominada placa detectora ou placa metrológica. A popularidade deste sistema se deve ao baixo custo em relação a outras tecnologias utilizadas e à sua robustez por utilizar fios enterrados, o que protege contra degradação do material devido a ações do clima, como sol e chuva. Em alguns casos são usados em configuração simples (um único laço) para medição de tráfego e operação de trânsito de forma inteligente. Outras vezes pode ser instalado em dois ou três laços por faixa para realizar o cálculo de velocidade.

Figura 52 - Sistema detector por laço indutivo



Fonte – UFCE (2010)

4.3.7 – Cancela automática

A cancela automática, mostrado na figura 53, é um equipamento essencial para realizar o controle do fluxo de veículos em estacionamentos, integrada a um software de gerenciamento e equipamentos que auxiliam na liberação de entrada e saída do veículo.

Para que a cancela automática seja acionada ela pode ser integrada a uma expedidora de tíquete, leitor de proximidade, leitor biométrico, terminais UHF, leitor de ticket entre outros que realizam a comunicação com o software de gerenciamento do local.

Figura 53 - Cancela Automática



Fonte – Ipec (2017)

4.3.8 – Software de cadastro, controle e monitoramento

O software HCS 2010, que faz o controle do sistema, possui as seguintes funções:

- BLOQUEIO DOS MENUS
- BARRA DE STATUS
- MONITORAMENTO ON-LINE
- CONFIGURAÇÃO DO MÓDULO GUARITA
- EVENTOS
- DISPOSITIVOS
- RELATÓRIO DE EVENTOS
- RELATÓRIO DE DISPOSITIVOS
- PRÉ-VISUALIZAÇÃO
- LEITURA COMPLETA
- GERENCIAR DISPOSITIVOS
- ATUALIZAÇÃO DOS RECEPTORES
- BACKUP E RESTORE
- CARTÃO SD
- GERENCIAR DISPOSITIVOS OFF-LINE
- OPÇÕES AVANÇADAS
- PROBLEMAS E SOLUÇÕES

Na figura 54 é mostrado a tela de monitoramento on-line.

Figura 54 - Software HCS 2010



Fonte - Linear HCS (2015)

4.3.9 – Sistema anti *by-pass*

O *Bypass* é um termo da língua inglesa que significa contornar, desviar, passagem secundária ou dar a volta. Um sistema anti *by-pass* serve para impedir com que o sistema de controle seja contornado ou burlado.

O laço indutivo em conjunto com a central de laço indutivo, mostrado na figura 55, possuem a função de detectar a presença de um veículo. Para isso deverá ser instalada em conjunto de um ou dois laços indutivos. Um laço indutivo instalado antes de uma cancela, ou portão, garante que um cartão RFID cadastrado para um veículo abra a cancela apenas quando um veículo estiver presente. Dessa maneira, evite que um pedestre consiga entrar apenas com o cartão, sem o veículo. O laço instalado após a cancela envia um sinal para o fechamento da mesma. Dessa maneira o laço substituirá o fechamento por feixe infravermelho, com a vantagem de não detectar passagens de pedestres, mas somente os veículos.

Figura 55 - Central de laço indutivo

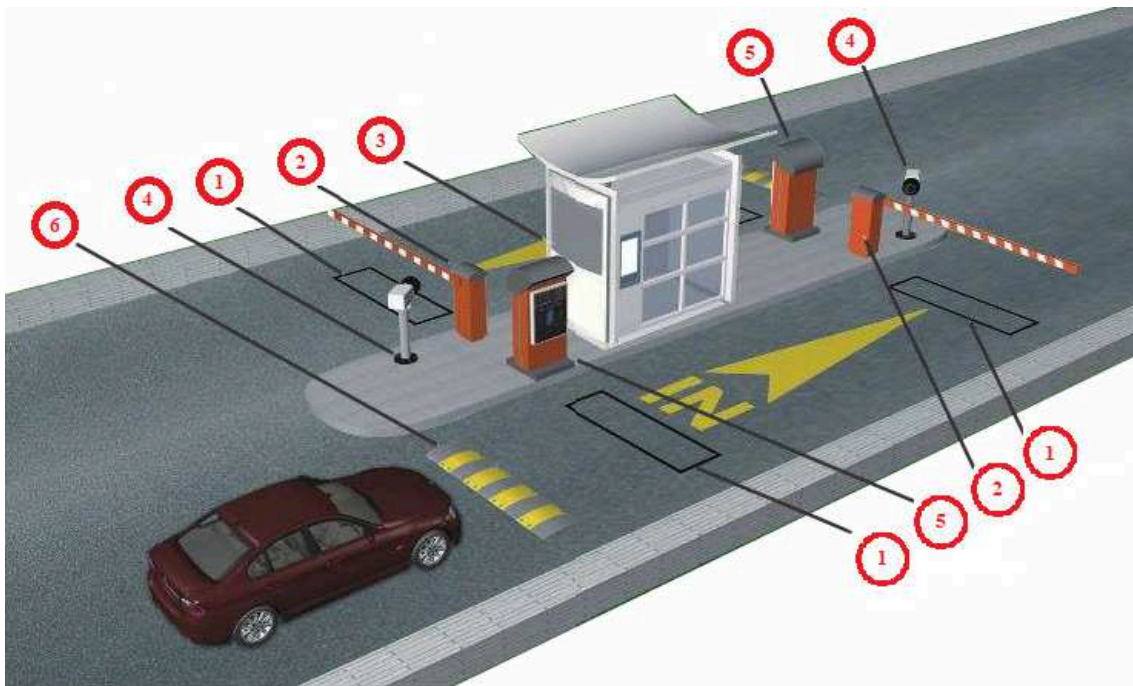


Fonte – SegConect (2013)

4.3.10 – Esquemática do projeto

A seguir será mostrado, na figura 56, uma exemplificação de como é distribuído os componentes fisicamente.

Figura 56 - Esquema físico do projeto



Fonte - CHD Newabel (2014)

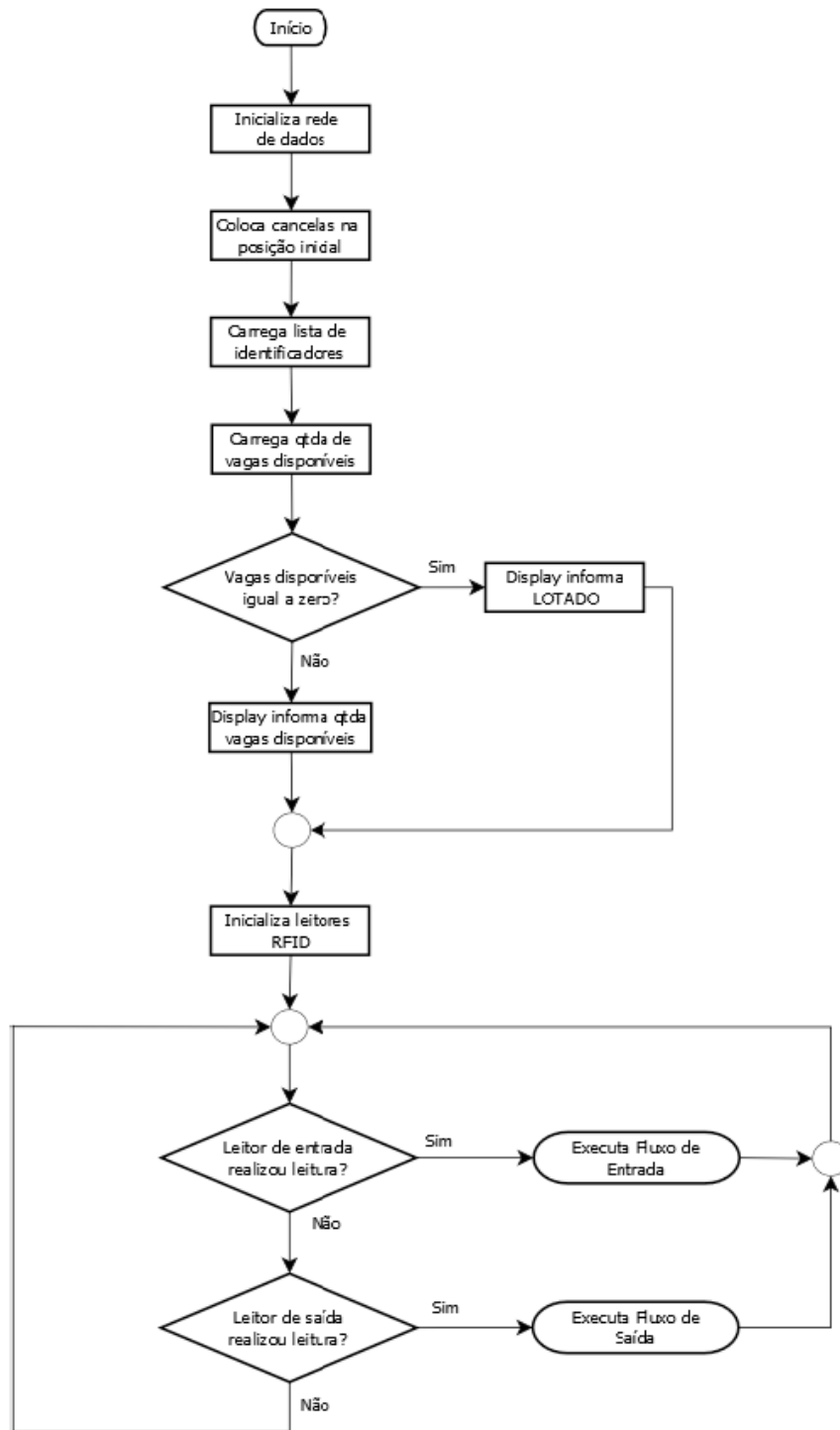
Onde:

- 1 – Laços indutivos
- 2 – Cancelas eletrônicas
- 3 – Cabine de comando
- 4 – Câmeras de vigilâncias
- 5 – Receptores e leitores
- 6 – Redutor de velocidade

4.3.11 – Fluxogramas do sistema de controle de acesso

Na Figura 57 é apresentado o fluxograma do processo de inicialização do sistema. Primeiramente é inicializada a rede de dados através da associação de um IP em conjunto com o módulo guarita. Em seguida são configurados os servo-motores e ajustados para a posição inicial, cancelas fechadas. Após a lista com os identificadores é carregada em um vetor e a quantidade de vagas disponíveis é lida de um arquivo e armazenada em uma variável. Se não houver vagas disponíveis o display informa lotação máxima, caso contrário é apresentado no display a quantidade de vagas disponíveis. Posteriormente os leitores RFID são inicializados e os receptores entram em um laço infinito no qual é realizada a monitoração do leitor RFID de entrada, se o módulo guarita recebe o identificador ele executa o fluxograma do procedimento de entrada, caso contrário ele monitora o leitor RFID de saída, se o módulo guarita receber o identificador ele executa o fluxograma do procedimento de saída, caso contrário volta a monitorar o leitor de entrada e assim sucessivamente.

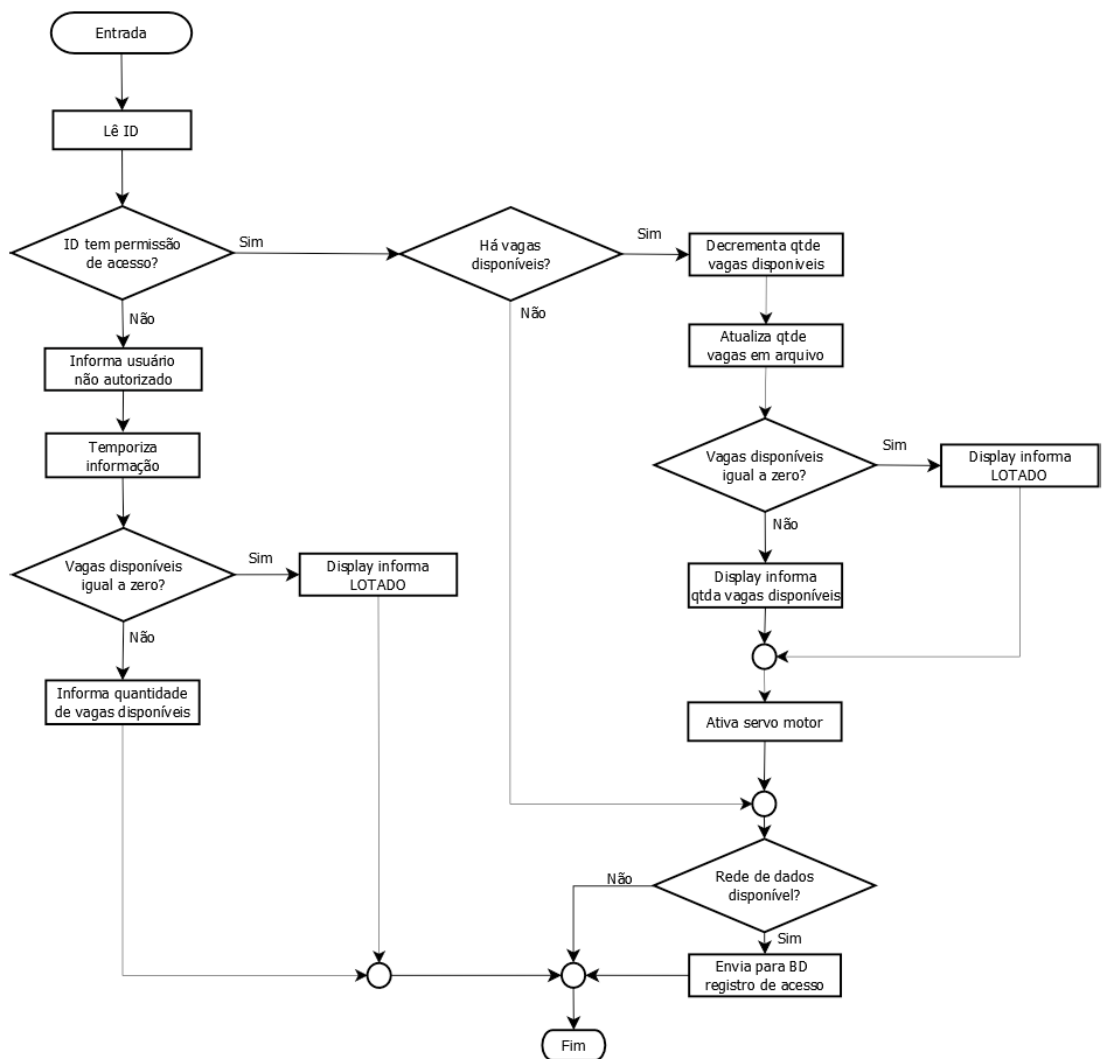
Figura 57 - Fluxograma do processo de inicialização



Fonte – UFSC (2012)

Na Figura 58 é apresentado o fluxograma do processo a ser seguido pelo sistema quando o usuário efetuar uma tentativa de acesso. Assim que a etiqueta se aproxima do leitor RFID, o código de identificação é enviado ao microcontrolador. Este verifica se a informação recebida consta na lista de identificadores. Caso a identificação não seja encontrada, o Servo motor não é acionado e por alguns segundos o display informa que o identificador não possui autorização de acesso. Após finalizar o tempo configurado, o display volta a apresentar a quantidade de vagas disponíveis ou a informação de lotação máxima.

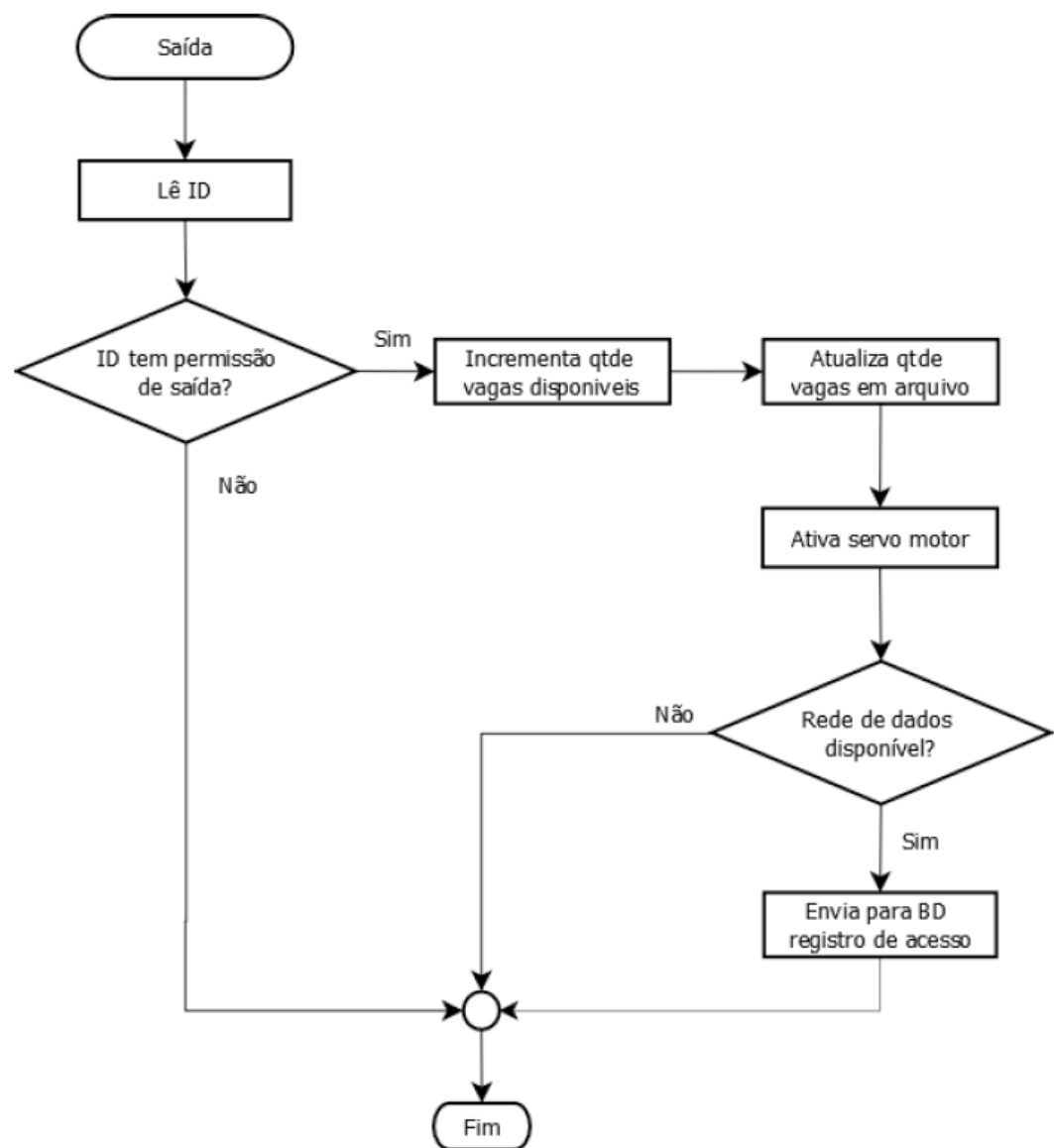
Figura 58 - Fluxograma do procedimento de entrada



Fonte – UFSC (2012)

O procedimento executado na saída dos veículos é bastante simples. Inicialmente é verificado se o identificador possui permissão de saída, caso negativo nenhuma ação é adotada. Se o identificador possuir permissão de saída o número de vagas disponíveis é incrementado, o Servo motor é acionado e é realizada a inserção de um registro de saída no banco de dados. Na Figura 59 é apresentado o fluxograma do processo a ser executado pelo sistema na saída de um veículo. O incremento da quantidade de vagas disponíveis é limitado pela capacidade máxima do estacionamento.

Figura 59 - Fluxograma do procedimento de saída



Fonte – UFSC (2012)

4.3.12 – Planilha de custos

A seguir será apresentado na tabela 5, os custos estimados para o projeto.

Tabela 5 - Tabela de valores dos componentes

	Equipamento	Preço unitário	Quantidade utilizada	Preço
	Modulo Guarita	R\$ 750,00	1	R\$ 750,00
	Botoeira	R\$ 170,00	1	R\$ 170,00
	Receptor CTW-4	R\$ 290,00	1	R\$ 290,00
	Leitor LN-101-A	R\$ 170,00	3	R\$ 510,00
Opcional	Leitor Biométrico LNS - P	R\$ 1.150,00	1	R\$ 1.150,00
	Central de laço indutivo	R\$ 500,00	2	R\$ 1.000,00
	Cancela Automática	R\$ 3.000,00	3	R\$ 9.000,00
	Multiconversor	R\$ 550,00	1	R\$ 550,00
	Software	R\$ -	1	R\$ -
*	Tag's	R\$ 1,50	500	R\$ 750,00
	Câmeras (Kit)	R\$ 200,00	-	R\$ 200,00
	Total	R\$ 6.781,50		R\$ 14.370,00

* Será decisão da instituição ceder as tag's ou não

Fonte - Autoria própria (2018)

5 – Conclusão

Conclui-se que o sistema eletrônico de controle de acesso é um recurso muito útil em diversas aplicações, porém é fundamental que seu funcionamento seja integrado com políticas que criem procedimentos funcionais que restrinjam o acesso sem atrapalhar as operações da instituição, ou seja, treinar as pessoas de forma que elas entendam que o sistema é para ajudar garantir a segurança patrimonial da instituição e também a qualidade das operações que sejam confidenciais. Desta forma é fundamental que o projeto técnico seja feito atendendo aos requisitos e conceitos da segurança patrimonial e seguindo as políticas de privacidade dos setores que controlam as áreas envolvidas.

Em locais onde exista uma cultura de segurança das informações, a utilização de sistemas eletrônicos de controle de acesso é fundamental para que o acesso físico aos centros de processamento de dados não seja limitado a utilização de uma chave para abertura de uma fechadura, por exemplo. Se utilizando cartões como chave de identificação todos os eventos são registrados e como o cartão em praticamente todas as organizações funciona também como identificação física dos funcionários (crachás) a responsabilidade de guarda e utilização do mesmo é atribuída a cada indivíduo, e como há registro de todos os eventos é natural que cada um assimile essa responsabilidade e a pratique.

Porém, para o bom funcionamento dos sistemas eletrônicos de controle de acesso não basta apenas uma série de procedimentos, também é necessário que as instalações sejam feitas atendendo todos os requisitos técnicos do projeto para que sistema opere de forma confiável em tempo integral e que as pessoas sejam treinadas de forma adequada para que entendam e pratiquem as políticas adotadas pela instituição.

Nesta dissertação foi apresentado também um estudo sobre a tecnologia de identificação por radiofrequência – RFID – fazendo uma análise de seus componentes básicos e de seus princípios de operação.

A tecnologia RFID está gradativamente substituindo a maioria dos componentes de identificação atuais. Ela pode ser aplicada em diversas soluções, principalmente em cadeias de suprimentos para controles de estoques, no controle de animais e também no controle de acesso, conforme abordado neste projeto.

O projeto foi baseado em equipamentos da empresa Linear HCS que tem o seu ramo de atuação no campo da segurança eletrônica. Todas as conexões e equipamentos foram pesquisados com informações disponibilizadas pela empresa e os valores colhidos são baseados em uma procura de valores em diversos locais, fora considerado os valores médios para o projeto.

Executando-se um projeto como este, poderá notar-se uma extrema melhoria de organização, monitoramento e segurança, que foram as motivações para esta dissertação.

Anexos e apêndices

Programação do protótipo

```
//Bibliotecas
```

```
    #include <SPI.h>
```

```
    #include <MFRC522.h>
```

```
//Pinos
```

```
    #define LED_VERDE 6
```

```
    #define LED_VERMELHO 7
```

```
    #define BUZZER 8
```

```
    #define SS_PIN 10
```

```
    #define RST_PIN 9
```

```
String IDtag = ""; //Variável que armazenará o ID da Tag
```

```
bool Permitido = false; //Variável que verifica a permissão
```

```
//Vetor responsável por armazenar os ID's das Tag's cadastradas
```

```
String TagsCadastradas[] = {"767669ac"};
```

```
MFRC522 LeitorRFID(SS_PIN, RST_PIN); // Cria uma nova instância para o leitor e passa os pinos como parâmetro
```

```
void setup() {
```

```
    Serial.begin(9600);          // Inicializa a comunicação Serial
```

```
    SPI.begin();                // Inicializa comunicação SPI
```

```
    LeitorRFID.PCD_Init();      // Inicializa o leitor RFID
```

```
    pinMode(LED_VERDE, OUTPUT); // Declara o pino do led verde como saída
```

```
    pinMode(LED_VERMELHO, OUTPUT); // Declara o pino do led vermelho como saída
```

```
    pinMode(BUZZER, OUTPUT);    // Declara o pino do buzzer como saída
```

```
    }
```

```
void loop() {
```

```
    Leitura(); //Chama a função responsável por fazer a leitura das Tag's    }
```

```
void Leitura(){
```



```

IDtag = ""; //Inicialmente IDtag deve estar vazia.
// Verifica se existe uma Tag presente
if ( !LeitorRFID.PICC_IsNewCardPresent() || !LeitorRFID.PICC_ReadCardSerial() ) {
    delay(50);
    return;    }

// Pega o ID da Tag através da função LeitorRFID.uid e Armazena o ID na variável
IDtag
for (byte i = 0; i < LeitorRFID.uid.size; i++) {
    IDtag.concat(String(LeitorRFID.uid.uidByte[i], HEX));    }
//Compara o valor do ID lido com os IDs armazenados no vetor TagsCadastradas[]
for (int i = 0; i < (sizeof(TagsCadastradas)/sizeof(String)); i++) {
    if( IDtag.equalsIgnoreCase(TagsCadastradas[i]) ){
        Permitido = true; //Variável Permitido assume valor verdadeiro caso o ID Lido esteja
cadastrado    }    }

    if(Permitido == true) acessoLiberado(); //Se a variável Permitido for verdadeira será
chamada a função acessoLiberado()

    else acessoNegado(); //Se não será chamada a função acessoNegado()

    delay(2000); //aguarda 2 segundos para efetuar uma nova leitura    }

void acessoLiberado(){

    Serial.println("Tag Cadastrada: " + IDtag); //Exibe a mensagem "Tag Cadastrada" e o ID da
tag não cadastrada

    efeitoPermitido(); //Chama a função efeitoPermitido()

    Permitido = false; //Seta a variável Permitido como false novamente    }

void acessoNegado(){

    Serial.println("Tag NAO Cadastrada: " + IDtag); //Exibe a mensagem "Tag NAO
Cadastrada" e o ID da tag cadastrada

    efeitoNegado(); //Chama a função efeitoNegado() }

void efeitoPermitido(){

    int qtd_bips = 2; //definindo a quantidade de bips

    for(int j=0; j<qtd_bips; j++){

        //Ligando o buzzer com uma frequência de 1500 hz e ligando o led verde.

```

```

tone(BUZZER,1500);
digitalWrite(LED_VERDE, HIGH);
delay(100);
//Desligando o buzzer e led verde.
noTone(BUZZER);
digitalWrite(LED_VERDE, LOW);
delay(100); } }
void efeitoNegado(){
int qtd_bips = 1; //definindo a quantidade de bips
for(int j=0; j<qtd_bips; j++){
//Ligando o buzzer com uma frequência de 500 hz e ligando o led vermelho.
tone(BUZZER,500);
digitalWrite(LED_VERMELHO, HIGH);
delay(500);
//Desligando o buzzer e o led vermelho.
noTone(BUZZER);
digitalWrite(LED_VERMELHO, LOW);
delay(500); } }

```

A seguir será explicado a utilidade de todas as opções listadas sobre o software Linear HCS.

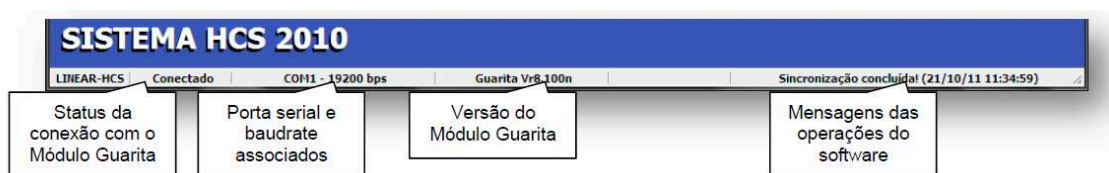
BLOQUEIO DOS MENUS

Com o objetivo de proteger o software de utilização não autorizada, todas as opções de configuração e comunicação com o Módulo Guarita são bloqueadas por **senha**.

BARRA DE STATUS

Quando conectado, a barra de status do software exibe algumas informações importantes, como segue abaixo na figura 60:

Figura 60 - Barra de status



Fonte - Linear HCS (2012)

MONITORAMENTO ON-LINE

O **Monitoramento on-line**, mostrado na figura 61, exibe em tempo real qualquer acionamento ocorrido ao equipamento, registrando ainda um histórico com os oito eventos anteriores.

Figura 61 - Monitoramento On-line Linear HCS



Fonte - Linear HCS (2012)

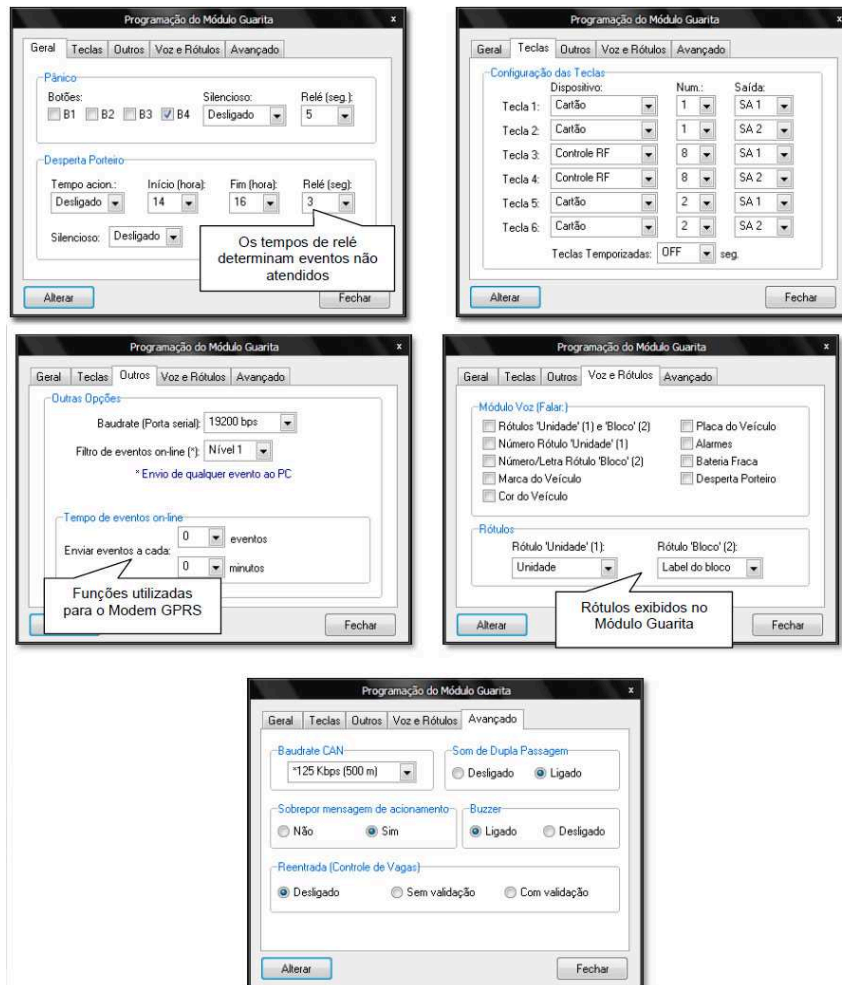
CONFIGURAÇÃO DO MÓDULO GUARITA

Toda configuração do Módulo Guarita 2010 pode ser feita via software, como segue abaixo:

Programação

Clique no menu **Avançado**, **Módulo Guarita** e selecione a opção **Programação**. As telas, na figura 62, serão exibidas.

Figura 62 - Programação do módulo guarita



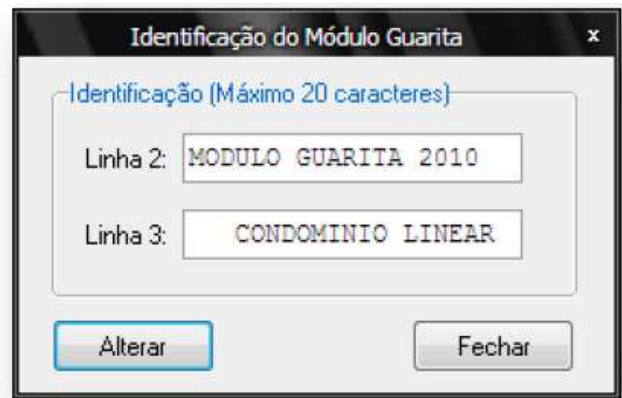
Fonte - Linear HCS (2012)

Confirme as alterações clicando no botão **Alterar**.

Identificação

Para alterar as linhas 2 e 3 do display do Módulo Guarita 2010, clique no menu **Avançado, Módulo Guarita** e selecione a opção **Identificação**. A tela, mostrada na figura 63, será exibida.

Figura 63 - Identificação modulo guarita



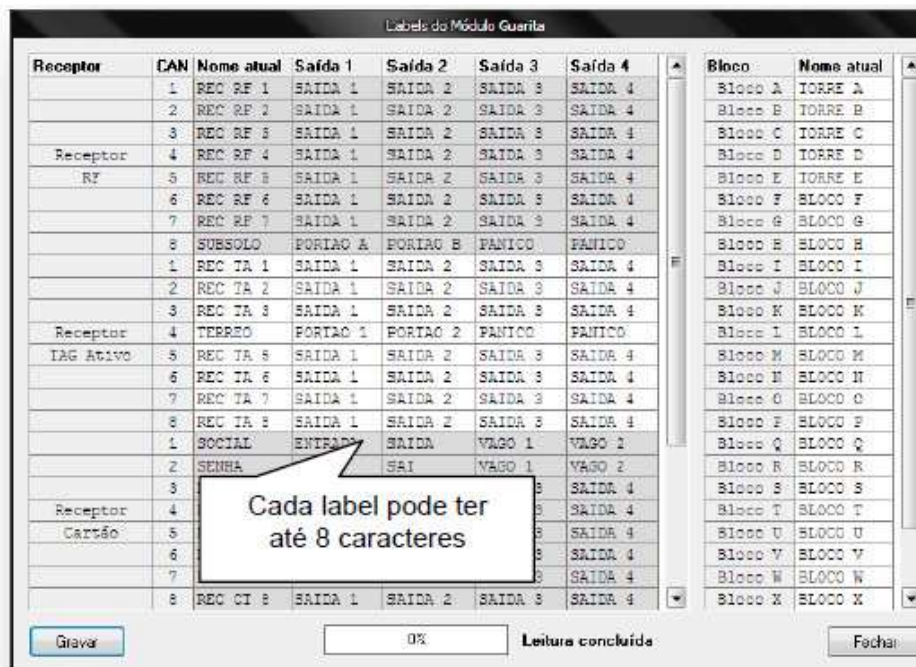
Fonte - Linear HCS (2012)

Confirme as alterações clicando no botão **Alterar**.

Labels

Para alterar os nomes de exibição (*labels*) dos blocos, receptores e saídas, clique no menu **Avançado, Módulo Guarita** e selecione a opção **Labels**. A tela, mostrada na figura 64, será exibida.

Figura 64 - Labels do software Linear HCS



Fonte - Linear HCS (2012)

Confirme as alterações clicando no botão **Gravar**.

Data e Hora

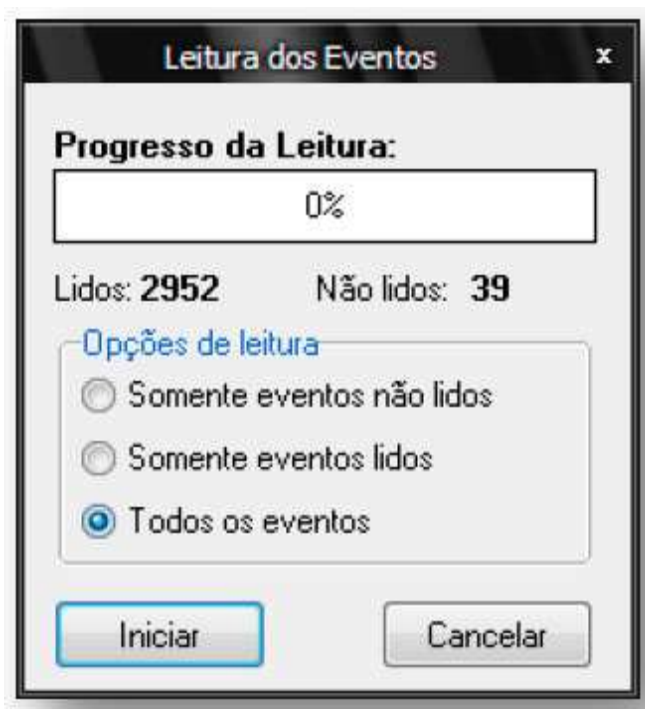
É possível alterar o relógio do Módulo Guarita 2010 a partir do horário do **Windows**. Para tanto, acesse o menu **Avançado, Módulo Guarita**, opção **Alterar Data/Hora**. Confirme a alteração.

EVENTOS

Os eventos gerados ao Módulo Guarita 2010 são armazenados em sua **memória interna**, em aproximadamente 8.100 posições. Sempre que este limite é atingido, o equipamento automaticamente cria uma cópia de toda memória em um **Cartão SD** devidamente instalado, passando então a sobrescrever os eventos mais antigos na memória interna. Se o Cartão SD não estiver presente, apenas a memória interna será gerenciada.

Para salvar uma cópia dos eventos no PC, clique no menu **Leitura** e selecione a opção **Eventos**. A tela, mostrada na figura 65, será exibida:

Figura 65 - Leitura dos eventos



Fonte - Linear HCS (2012)

Selecione uma das opções de leitura e em seguida, clique no botão **Iniciar**. O software solicitará um local no PC para salvar o arquivo de eventos (extensão **EVT**), sugerindo inclusive o nome do arquivo (data e hora). Clique no botão **Salvar** e aguarde o processo de coleta.

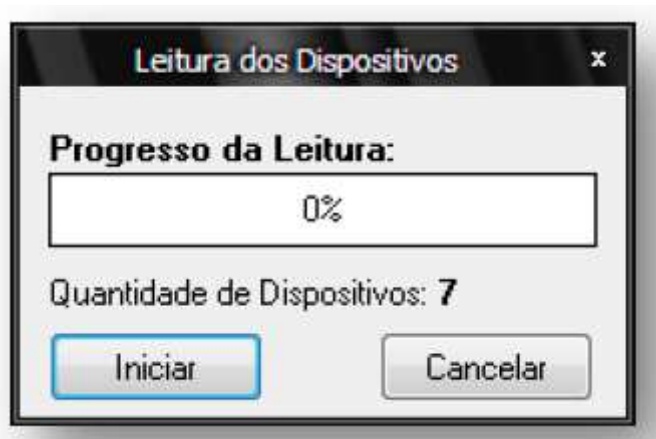
Ao finalizar, será solicitado ao usuário se deseja **visualizar o relatório dos eventos**. Selecione a opção desejada, lembrando que pôr o arquivo já estar salvo no PC, este pode ser visualizado a qualquer momento pelo menu **Relatórios**.

DISPOSITIVOS

Módulo Guarita 2010 permite armazenar até 12.000 dispositivos que incluem Controle Remoto (**RF**), TAG Ativo (**TA**), TAG Passivo (**TP**), Cartão de Proximidade (**CT**) e Senhas de Acesso (**SN**). Cada dispositivo possui informações de unidade e bloco, identificação de 18 caracteres, e dados de veículo (marca, cor e placa).

Para salvar uma cópia dos dispositivos no PC, clique no menu **Leitura** e selecione a opção **Dispositivos**. A tela, mostrada na figura 66, será exibida:

Figura 66 - Leitura dos dispositivos



Fonte - Linear HCS (2012)

Clique no botão **Iniciar**. O software solicitará um local no PC para salvar o arquivo de dispositivos (extensão **DPT**), sugerindo inclusive o nome do arquivo (data e hora). Clique no botão **Salvar** e aguarde o processo de coleta.

Ao finalizar, será solicitado ao usuário se deseja **visualizar o relatório dos dispositivos**. Selecione a opção desejada, lembrando que pelo o arquivo já estar salvo no PC, este pode ser visualizado a qualquer momento pelo menu **Relatórios**.

RELATÓRIO DE EVENTOS

Ao realizar a leitura dos eventos ou recuperar uma leitura salva, pelo menu **Relatórios**, opção **Eventos**, a janela **Visualizar Eventos** é exibida, conforme figura 67:

Figura 67 - Relatório de eventos

The image shows a software window titled "Visualizar Eventos". It has a standard Windows-style title bar with a close button. The window is divided into several sections:

- Tipo de Evento:** A group box containing a list of event types. The "Todos" checkbox is checked. Other unchecked options include "Controle RF", "TAG Ativo", "Cartão", "Senha", "TAG Passivo", "Desperta Porteiro + Mód. Ligado + Muda. Programação", "Pânico", "Clonagem", "Acionamento por Porteiro", and "Backups + Restores".
- Unidade Específica:** A group box with a "Filtrar" checkbox. Below it are two dropdown menus: "Unidade" (set to "0") and "Bloco" (set to "TORRE A (A)").
- Faixa de Data:** A group box with a "Filtrar" checkbox. Below it are two date pickers: "Inicial" (set to "21/10/2011") and "Final" (set to "21/10/2011").
- Outras Opções:** A group box with a "Bateria Fraca" checkbox.

At the bottom of the window, there are two buttons: "Visualizar" (highlighted with a blue border) and "Fechar".

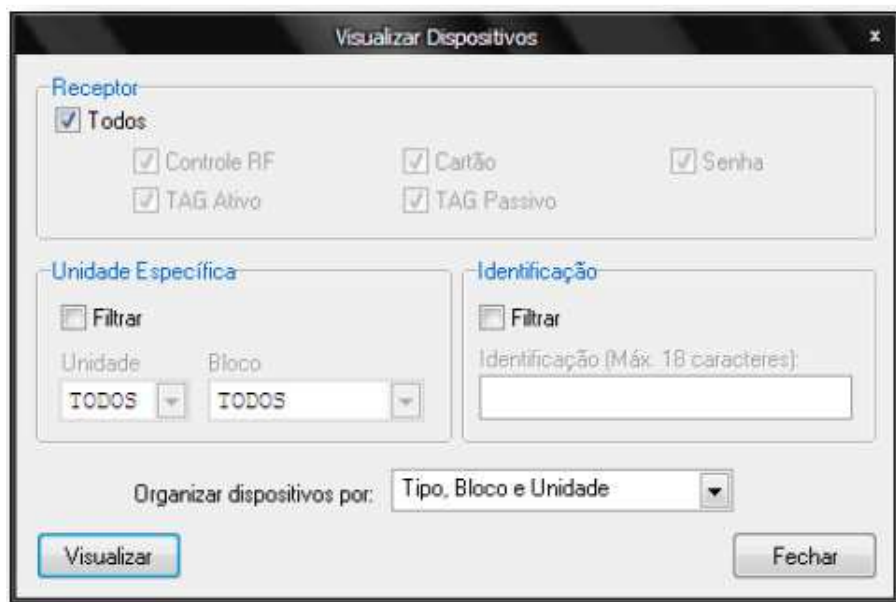
Fonte - Linear HCS (2012)

Após selecionar os filtros desejados, clique no botão **Visualizar**. O relatório será montado e exibido em tela.

RELATÓRIO DE DISPOSITIVOS

Ao realizar a leitura dos dispositivos ou recuperar uma leitura salva, pelo menu **Relatórios**, opção **Dispositivos**, a janela **Visualizar Dispositivos** é exibida, conforme figura 68:

Figura 68 - Relatório de dispositivos



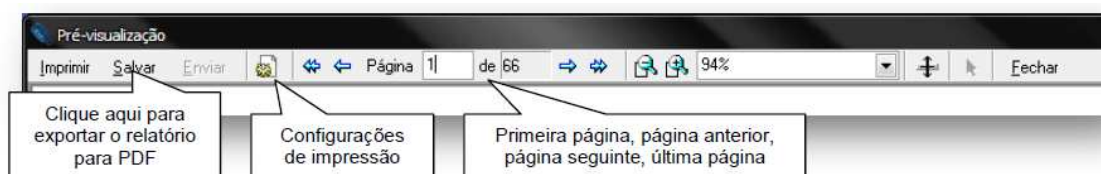
Fonte - Linear HCS (2012)

Após selecionar os filtros desejados, clique no botão **Visualizar**. O relatório será montado e exibido em tela.

PRÉ-VISUALIZAÇÃO

Para os relatórios de eventos e dispositivos, a janela conforme figura 69, será exibida:

Figura 69 - Pré-visualização



Fonte - Linear HCS (2012)

Nesta tela é possível imprimir o relatório ou exportá-lo para **PDF** e **RFP**, que é padrão do software.

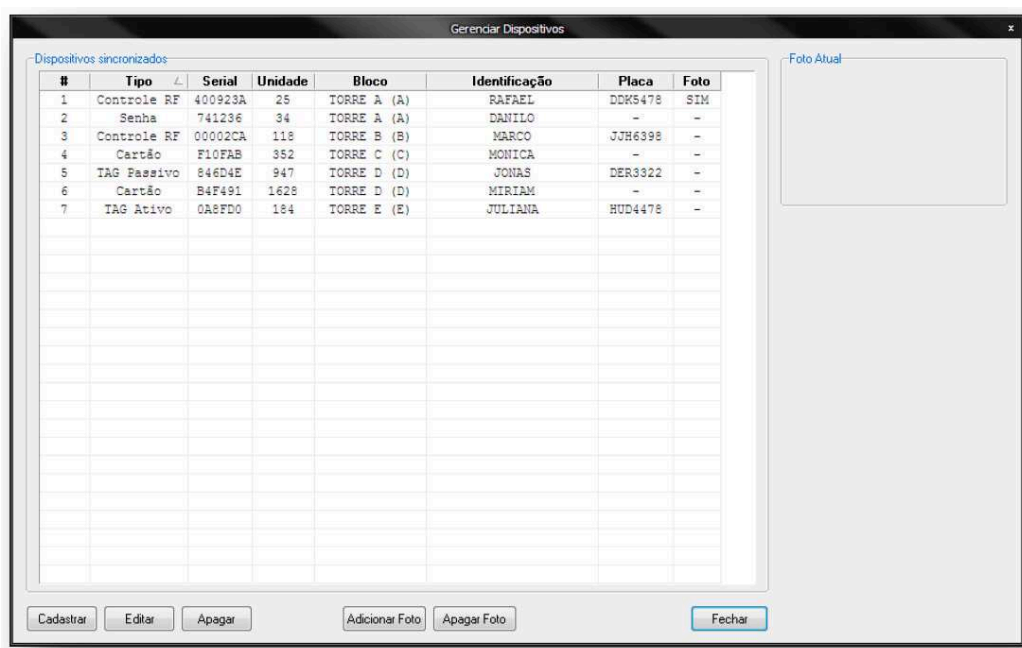
LEITURA COMPLETA

A opção **Leitura completa** disponível no menu **Leitura** pode ser utilizada como backup do Módulo Guarita 2010, ou como uma maneira de fornecer a terceiros acesso aos relatórios de **eventos** e **dispositivos**, sem precisar instalar o software completo.

GERENCIAR DISPOSITIVOS

Pelo software também é possível cadastrar, editar e apagar dispositivos. Para tanto, acesse o menu **Avançado, Avançado II, Gerenciar Dispositivos**. A tela mostrada na figura 70, será exibida:

Figura 70 - Gerenciador de dispositivos



Fonte - Linear HCS (2012)

Cadastrar dispositivo

Para cadastrar um novo dispositivo, clique no botão **Cadastrar**. Verifique que à direita estarão disponíveis os campos para cadastro. Existem três formas para preencher os campos do grupo **Dados do dispositivo**:

1. **Manualmente**, selecionando o **Tipo** de dispositivo e preenchendo os campos **Serial** (ou **Senha**, quando aplicável) e **Contador** (apenas para Controle Remoto).
2. **Via Módulo Guarita 2010**, virando a chave de programação e acionando o dispositivo escolhido na direção do equipamento. Para Controle Remoto, pressione uma vez as teclas B1 e B2 ao mesmo tempo; para Cartão de Proximidade, apenas aproxime o cartão ao equipamento; para TAG Ativo, ligue e desligue a chave do dispositivo. Note que os campos em **Dados do dispositivo** serão preenchidos automaticamente.
3. **Via Leitora de Mesa USB (Desktop Reader)**, clicando no botão **Leitora USB** com este ligado a uma porta USB disponível no PC. Acione o dispositivo escolhido na direção da leitora e verifique que os campos em **Dados do dispositivo** serão preenchidos automaticamente.

Após seguir um dos passos acima, preencha todos os campos em **Dados de cadastro** e por fim clique no botão **Confirmar**. O programa exibirá a mensagem “Dispositivo cadastrado com sucesso!” caso esteja tudo correto; “Memória do Módulo Guarita cheia!” caso o limite de dispositivos seja atingido; “Dispositivo já cadastrado!” caso já houver no equipamento um dispositivo com os mesmos **Dados do dispositivo** associados.

Editar dispositivo

Para editar um dispositivo já cadastrado, selecione-o na lista e clique no botão **Editar**, ou simplesmente clique duas vezes no dispositivo escolhido na lista. O modo de edição será mostrado à esquerda, onde somente os campos do grupo **Dados de cadastro** podem ser alterados.

Confirme a alteração clicando no botão **Confirmar**.

Apagar dispositivo

Para apagar um dispositivo já cadastrado, selecione-o na lista e clique no botão **Apagar**. Uma mensagem de confirmação será exibida, bastando clicar em **Sim** para remover completamente o dispositivo do equipamento.

Adicionar e apagar foto

É possível associar uma foto a cada dispositivo, para ser exibida no **Monitoramento On-line** durante o acionamento. Para tanto, selecione o dispositivo escolhido e clique no botão **Adicionar Foto**. Selecione a imagem no PC (formatos aceitos: **JPG**, **JPEG** e **BMP**) e clique no botão **Abrir**. Recomenda-se escolher fotos com resolução média e tamanho reduzido, por limitações de exibição no software.

Para remover a foto, selecione o dispositivo escolhido e clique no botão **Apagar Foto**. Confirme a exclusão da foto e esta não será mais exibida no Monitoramento On-line.

ATUALIZAÇÃO DOS RECEPTORES

Após cadastrar, editar ou apagar qualquer dispositivo, a atualização dos receptores deve ser executada, para garantir que todas as alterações sejam informadas aos receptores ligados ao Módulo Guarita 2010. Para tanto, ao fechar a janela **Gerenciar Dispositivos**, o programa solicita se o usuário deseja atualizar os receptores. Clique em **Sim** e aguarde o processo de atualização.

Também é possível fazer a atualização via menu **Avançado**, **Avançado II** e opção **Atualizar Receptores**.

BACKUP E RESTORE

O software disponibiliza opções de cópia de todo o Módulo Guarita 2010 (**Backup**) assim como opções para devolução dessas cópias ao equipamento (**Restore**).

Os backups podem ser realizados individualmente ou em conjunto, utilizando a opção **Leitura completa**, descrita anteriormente.

Backup Labels

Esta opção possibilita o backup da **identificação** (linhas 2 e 3 do display) e **labels** do Módulo Guarita 2010. Clique no menu **Leitura** e selecione a opção **Backup Labels**. O programa solicitará um local no PC para salvar o arquivo de **labels** (extensão **STP**), sugerindo inclusive o nome do arquivo (data e hora). Clique no botão **Salvar** e aguarde o processo de coleta.

Backup Recs. Multi.

Esta opção possibilita o backup da **configuração dos Receptores Multifunção** presentes ou não no sistema. Clique no menu **Leitura** e selecione a opção **Backup Recs. Multi**. O programa solicitará um local no PC para salvar o arquivo (extensão **PAR**), sugerindo inclusive o nome do arquivo (data e hora). Clique no botão **Salvar** e aguarde o processo de coleta.

O processo de restore é individual e não é possível enviar ao Módulo Guarita 2010 os eventos salvos. Vale lembrar que nos procedimentos abaixo, as informações serão apagadas e substituídas por novas.

Restore Dispositivos

Esta opção envia os **dispositivos e programação** salvos no PC (arquivo **DPT**) para o Módulo Guarita 2010. Clique no menu **Avançado, Avançado II, Restore** e selecione a opção **Dispositivos**.

Clique no botão **Enviar** e o programa solicitará o **arquivo de dispositivos**. Selecione o arquivo corretamente e clique no botão **Abrir**. Aguarde o progresso do envio e ao finalizar, o programa solicitará a **Atualização dos Receptores**. Em seguida, será solicitada a **Sincronização do Módulo Guarita**.

Restore Labels

Esta opção envia a **identificação** e os **labels** do PC ao Módulo Guarita 2010 (arquivo **STP**). Clique no menu **Avançado, Avançado II, Restore** e selecione a opção **Labels**.

Clique no botão **Enviar** e o programa solicitará o **arquivo de labels**. Selecione o arquivo corretamente e clique no botão **Abrir**. Aguarde o progresso do envio e ao finalizar, o programa solicitará a **Sincronização do Módulo Guarita**.

Restore Recs. Multi.

Esta opção envia a **programação dos Receptores Multifunção**, do PC ao Módulo Guarita 2010 (arquivo **PAR**). Clique no menu **Avançado, Avançado II, Restore** e selecione a opção **Rec. Multi**.

Clique no botão **Enviar** e o programa solicitará o **arquivo de programação**. Selecione o arquivo corretamente e clique no botão **Abrir**. Aguarde o progresso do envio e ao finalizar, o programa solicitará a **Atualização dos Receptores**.

CARTÃO SD

O Módulo Guarita 2010 possui duas interfaces para Cartão SD, uma **interna** e outra **externa**. Ambas funcionam como memória de backup, armazenando todas as informações do Módulo Guarita e separando-as por data e hora da operação. Os backups podem ser realizados **manualmente** (pelo menu do próprio equipamento), ou **automaticamente** (sempre quando a memória interna atinge aproximadamente 8.100 eventos). Eles também podem ser devolvidos ao equipamento via menu, acessando a opção de **Restore**.

Os arquivos salvos no Cartão SD estão **codificados**, por isso só podem ser lidos ou alterados via software. Para tanto, as seguintes opções estão disponíveis:

Cartão SD (Guarita)

Esta opção permite ler o conteúdo do Cartão SD (interno ou externo) **diretamente ligado ao Módulo Guarita**, ideal quando o PC não possui interface para este tipo de cartão. Clique no menu **Leitura** e selecione a opção **Cartão SD (Guarita)**.

Selecione a **posição** do Cartão SD e clique no botão **Selecionar**. Aguarde o carregamento das informações onde o programa listará todos os backups realizados. Selecione a data e hora desejadas, e a opção de coleta (com **Visualizador** ou para **Backup**). Clique no botão **Iniciar** e aguarde. Ao finalizar, será solicitado um local para salvar as informações. Após confirmar, a pasta abrirá automaticamente exibindo todos os arquivos copiados, nos moldes da **Leitura completa**.

Cartão SD (PC)

Esta opção permite ler o conteúdo do Cartão SD ligado **diretamente** ao PC. Acesse o menu **Relatórios** e selecione a opção **Cartão SD (PC)**.

Selecione a **unidade de disco** onde se encontra o Cartão SD e clique no botão **Verificar**. O programa listará todos os backups realizados, bastando selecionar a data e hora desejadas e clicar no botão do relatório que deseja exibir: **Dispositivos** ou **Eventos**. O relatório correspondente será exibido.

Apagar Backup

É possível apagar de **maneira correta** qualquer backup realizado ao Cartão SD. Para tanto, acesse o menu **Configurar, Cartão SD (PC)** e selecione a opção **Apagar Backup**.

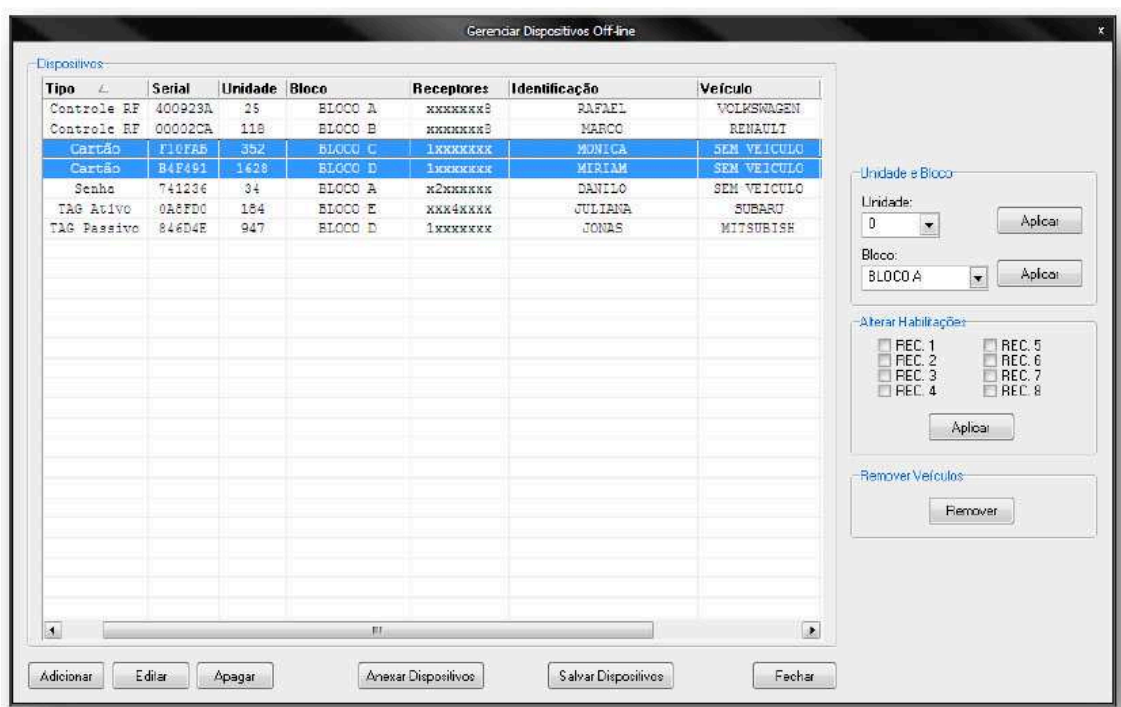
Selecione a **unidade de disco** onde se encontra o Cartão SD e clique no botão **Verificar**. O programa listará todos os backups realizados. Selecione a data e hora desejadas e clique no botão **Apagar**. Confirme a exclusão clicando em **Sim**.

GERENCIAR DISPOSITIVOS OFF-LINE

Em **Gerenciar Dispositivos Off-line**, o usuário tem a opção de cadastrar, editar ou apagar dispositivos **sem comunicação direta** com o Módulo Guarita, podendo executar posteriormente a função **Restore** para gravar as informações no equipamento.

Clique no menu **Configurar** e selecione a opção **Gerenciar Dispositivos Off-line**. A tela, mostrada na figura 71, será exibida.

Figura 71 - Gerenciar dispositivos Off-line



Fonte - Linear HCS (2012)

Utilize o botão **Anexar Dispositivos** para recuperar um arquivo salvo anteriormente. Os botões **Adicionar**, **Editar** e **Apagar** gerenciam individualmente o dispositivo, nos mesmos moldes do **Gerenciar Dispositivos** explanado anteriormente.

À direita estão disponíveis opções para edição em **massa** dos dispositivos. Para selecionar vários ao mesmo tempo, utilize as teclas **SHIFT** ou **CTRL** do teclado.

Ao finalizar as operações, clique no botão **Salvar Dispositivos**.

Selecionando **Computador**, o programa solicitará uma pasta no PC para salvar o arquivo de dispositivos gerado, no formato **DPT**. Selecione a pasta adequada e clique no botão **Salvar**.

Selecionando **Cartão SD**, o programa salvará uma pasta de backup contendo a lista de dispositivos, **diretamente** no cartão SD, bastando apenas efetuar o **Restore** no próprio Módulo Guarita 2010. O backup será exibido no equipamento com o *label* de identificação “GRAVACAO OFF-LINE”.

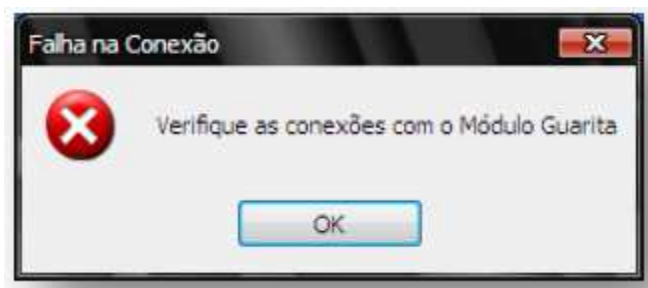
OPÇÕES AVANÇADAS

O software possui ainda algumas funções avançadas, de uso não comum, ideal para técnicos, instaladores ou integradores.

PROBLEMAS E SOLUÇÕES

O problema mais comum que pode ocorrer é com relação à comunicação entre o PC e o Módulo Guarita 2010, conforme a mensagem da figura 72:

Figura 72 - Aviso de erro

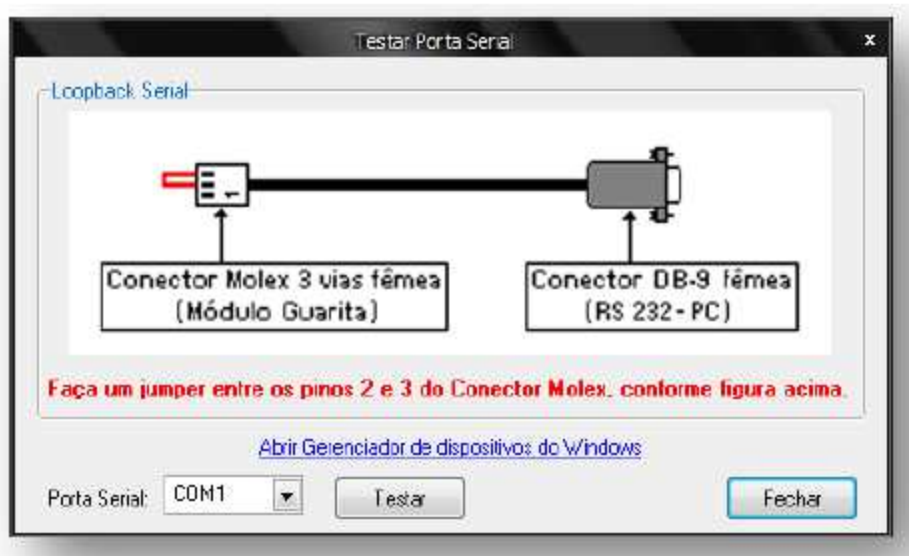


Fonte - Linear HCS (2012)

Neste caso, verifique se o Cabo de Comunicação está bem conectado e caso haja um Conversor Serial-USB entre as conexões, verifique se está funcional e completamente instalado no PC.

É possível verificar a integridade da Porta Serial em um teste simples efetuado via software. Clique no menu **Configurar** e selecione a opção **Testar Porta Serial**. A janela conforme figura 73 será exibida:

Figura 73 - Teste da porta serial



Fonte - Linear HCS (2012)

Desconecte a extremidade do Cabo de Comunicação ligada ao Módulo Guarita e faça um **jumper** (curto) com um fio entre os pinos 2 e 3 do conector, como mostra a figura. Em seguida, selecione a **Porta Serial** correspondente e clique no botão **Testar**. O programa exibirá uma mensagem com o resultado do teste.

Problemas com instabilidade nas operações, como leituras incompletas e erros aleatórios também estão relacionados à conexão. Efetue os testes acima e se possível, faça testes utilizando outro PC.

Referências bibliográficas

FINKENZELLER, K. **RFID HANDBOOK**: fundamentals and applications in contactless smart cards and identification. 3ªed. Chichester: John Wiley & Sons, 2010.

LAHIRI, S. **RFID SOURCE BOOK**. 1ªed. Armonk: IBM, 2005.

DOBKIN, D. **The RF in RFID**: Passive UHF RFID in Practice. 1ªed. Burligton: Elsevier, 2008.

SAUNDERS, S; ARAGON, A. **ANTENNAS and PROPAGATION for WIRELESS COMMUNICATION SYSTEMS**. 2ªed. Chichester: John Wiley & Sons, 2007.

SWEENEY, P. **RFID for DUMMIES**. 1ªed. Indianapolis: Wiley Publishing, 2005.

MANDARINI, M. **SEGURANÇA CORPORATIVA ESTRATEGICA**. 1ªed. Barueri: Manole, 2005.

<http://blog.grupoms.com.br/4-tipos-de-controle-de-acesso-nas-portarias/> - Acessado em 05/08

<https://www.ohub.com.br/ideias/tipos-de-controle-de-acesso-para-empresas/#.WpXOzejwaUI>
- Acessado em 05/08

<http://clicksmart.com.br/blog/conheca-os-principais-tipos-de-controle-de-acesso-a-ambientes/>
- Acessado em 06/08

<https://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm> - Acessado em 06/08

<http://insoft4aps.com.br/noticia/O-que-e-RFID-e-para-que-serve> - Acessado em 06/08

https://pt.wikipedia.org/wiki/Identifica%C3%A7%C3%A3o_por_radiofrequ%C3%Aancia
- Acessado em 06/08

<https://rfidbrasil.com/blog/o-que-e-a-tecnologia-rfid-e-como-ela-pode-ajudar-sua-empresa/> -
Acessado em 13/08/18

<https://www.mandae.com.br/blog/etiquetas-rfid-como-funcionam-e-quais-sao-as-suas-vantagens/> - Acessado em 13/08/18

https://pt.wikipedia.org/wiki/Identifica%C3%A7%C3%A3o_por_radiofrequ%C3%Aancia –
Acessado em 15/08

<http://saladaautomacao.com.br/funcionamento-da-rfid/> - Acessado em 15/08/18

https://pt.wikipedia.org/wiki/SAP_SE - Acessado em 15/08 - Acessado em 15/08

https://pt.wikipedia.org/wiki/Sistema_de_gerenciao_de_armaz%C3%A9m – Acessado em 15/08

https://pt.wikipedia.org/wiki/Sistema_legado - Acessado em 15/08/18

<https://pt.wikipedia.org/wiki/Idempot%C3%Aancia> – Acessado em 15/08

https://en.wikipedia.org/wiki/Received_signal_strength_indication - Acessado em 15/08

https://pt.wikipedia.org/wiki/Rede_por_microondas - Acessado em 15/08

<https://revista.feb.unesp.br/index.php/gepros/article/view/750> Acessado em 25/08

https://pt.wikipedia.org/wiki/Equa%C3%A7%C3%B5es_de_Maxwell#Lei_de_Amp%C3%A8re_com_a_corre%C3%A7%C3%A3o_de_Maxwell – Acessado em 25/08

<https://www.informs-sim.org/wsc04papers/147.pdf> - Acessado em 27/08/18

https://www.gta.ufrj.br/grad/10_1/rfid/historia.html - Acessado em 27/08/18

https://www.gta.ufrj.br/grad/13_1/rfid/cap2_1.html - Acessado em 27/08/18

<https://rfidmoura.wordpress.com/2015/07/21/as-frequencias-de-operacao-das-etiquetas-e-leitores-rfid/> - Acessado em 27/08/18

<http://brasil.rfidjournal.com/perguntas-frequentes> - Acessado em 27/08/18

http://www.teleco.com.br/tutoriais/tutorialrfid/pagina_3.asp - Acessado em 27/08/18

http://www.rfidjournal.net/masterPresentations/rfid_latam2012_brasil/np/rampim_1000_nov29.pdf - Acessado em 27/08/18

<http://www.rfid.ind.br/etiquetas-rfid-onde-comprar> - Acessado em 27/08/18

https://books.google.com.br/books?id=rblmAgAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false - Acessado em 27/08/18

<https://www.elcomhu.com/Electrical/Antennas%20/Antennas%20and%20Propagation%20for%20Wireless%20Communication%20Systems%20%202nd%20Ed.pdf> - Acessado em 27/08/18

<http://fatece.edu.br/arquivos/arquivos%20revistas/perspectiva/volume4/8.pdf> - Acessado em 27/08/18

<http://www.indusmelec.pt/newsletter/24/RFID.pdf> - Acessado em 27/08/18

<https://www.herrtech.com.br/blank> - Acessado em 28/08/18

<https://en.wikipedia.org/wiki/GS1> - Acessado em 28/08/18

<https://www.embarcados.com.br/rfid-etiquetas-com-eletronica-de-ponta/> - acessado em 28/08/18

http://www.professorpetry.com.br/Ensino/Defesas_Pos_Graduacao/Defesa%2038_Karla%20Maria%20Garcia_Sistema%20de%20Controle%20de%20Acesso%20Veicular%20Utilizando%20Tecnologia%20RFID.pdf – Acessado em 29/08/18

<https://pt.wikipedia.org/wiki/Microcontrolador> - Acessado em 05/10/18

<https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf> - Acessado em 05/08/18

<https://en.wikipedia.org/wiki/Buzzer> - Acessado em 05/10/18

https://pt.wikipedia.org/wiki/Diodo_emissor_de_luz - Acessado em 05/10/18

<https://pt.wikipedia.org/wiki/Resistor> - Acessado em 05/10/18

<https://pt.wikipedia.org/wiki/Jumper> - Acessado em 05/10/18

<https://pt.wikipedia.org/wiki/System-on-a-chip> - Acessado em 10/10/18

https://pt.wikipedia.org/wiki/Mem%C3%B3ria_de_acesso_aleat%C3%B3rio – Acessado em 10/10/18

<https://pt.wikipedia.org/wiki/PROM> - Acessado em 10/10/18

<https://pt.wikipedia.org/wiki/BIOS> - Acessado em 10/10/18

https://pt.wikipedia.org/wiki/Sistema_operacional_de_tempo-real - Acessado em 10/10/18

https://pt.wikipedia.org/wiki/Comiss%C3%A3o_Eletrot%C3%A9cnica_Internacional –
Acessado em 10/10/18

<https://en.wikipedia.org/wiki/MIFARE> - Acessado em 10/10/18

<https://en.wikipedia.org/wiki/NTAG> - Acessado em 10/10/18

<http://www.linear-hcs.com.br/txt/prod4.asp> - Acessado em 15/10/18

http://www.linear-hcs.com.br/manuais_hcs/equipamentos/guia_m_guarua_2010_sw_8.104d_29_8_16.pdf -
Acessado em 15/10/18

<http://www.linear-hcs.com.br/txt/prod45.asp> - Acessado em 15/10/18

http://www.linear-hcs.com.br/manuais_hcs/equipamentos/face_sheet_rec_ctw_24_09_14.pdf
- Acessado em 15/10/18

<http://dicas.webautomotivo.com.br/rede-can-o-que-e-e-como-funciona/> - Acessado em
15/10/18

http://linear-hcs.com.br/txt/iframe_prod.asp - Acessado em 15/10/18

<http://www.linear-hcs.com.br/txt/prod47.asp> - Acessado em 15/10/18

http://www.linear-hcs.com.br/manuais_hcs/equipamentos/face_sheet_ln101_a_21_10_14.pdf
- Acessado em 15/10/18

<http://www.linear-hcs.com.br/txt/prod67.asp> - Acessado em 15/10/18

http://www.linear-hcs.com.br/manuais_hcs/manuais_atualizados_05-17/LN5-P_%2030-1-17.pdf – Acessado em 15/10/18

<http://www.almitec.com.br/laco-indutivo-cancela> - Acessado em 15/10/18

<http://www.eletr.ufpr.br/marlio/medidas/seminarios/Rodolfo.pdf> - Acessado em 15/10/18

http://www.repositorio.ufc.br/bitstream/riufc/15545/1/2011_dis_haoliveira.pdf - Acessado em 15/10/18

http://www.linear-hcs.com.br/manuais_hcs/software/manual_software_hcs_2010_v6.x.pdf - Acessado em 17/10/18

<http://www.almitec.com.br/cancela-automatica> - Acessado em 17/10/18

<https://www.significados.com.br/bypass> - Acessado em 18/10/18

<https://produto.mercadolivre.com.br/MLB-985029289-modulo-guarita-linear-hcs-2010-b001-JM> - Acessado em 18/10/18

<https://produto.mercadolivre.com.br/MLB-995047439-botoeira-com-7-botoes-linear-modulo-guarita-panico-portaria-JM> - Acessado em 18/10/18

<https://produto.mercadolivre.com.br/MLB-952693886-receptor-linear-hcs-ctw-4a-ate-4-portoes-extra-autenticaco-JM> - Acessado em 18/10/18

<https://produto.mercadolivre.com.br/MLB-792633590-leitor-rf-id-ln-101-a-125-khz-linear-hcs-original-JM> - Acessado em 18/10/18

https://www.americanas.com.br/produto/19522139/leitor-biometrico-e-cartao-rfid-ln5-p-linear?WT.srch=1&epar=bp_pl_00_go_pla_casaconst_geral_gmv&gclid=CjwKCAjw3qDe

[BRBkEiwAsqeO7muU1AAFiYoj3zfkCkg- 1Z9uu6btAkbC-xthYGz4oQPZIW9-q7mXRoCMx0QAvD BwE&opn=YSMESP&sellerId=19457025000147 - Acessado em 18/10/18](https://produto.mercadolivre.com.br/MLB-876101602-central-de-laco-indutivo-1-canal-produto-novo-com-garantia- JM)

[https://produto.mercadolivre.com.br/MLB-876101602-central-de-laco-indutivo-1-canal-produto-novo-com-garantia- JM - Acessado em 18/10/18](https://produto.mercadolivre.com.br/MLB-876101602-central-de-laco-indutivo-1-canal-produto-novo-com-garantia- JM)

[https://www.inovecerto.com.br/kit-cancela-eletronica-automatica-brasso-1-2-hp-ppa-p2/?afiliadoid=34&utm_source=google&utm_medium=cpc&utm_content=KIT Cancela Elet r%C3%B4nica Autom%C3%A1tica Brasso - 1/2 HP - _PPA&utm_campaign=&gclid=CjwKCAjw3qDeBRBkEiwAsqeO7nYzf6AeDx8fBXqNoegv vZ-SB5EvZK4Te7iq3-eKBbK65_0XBq05nxoCU6UQAvD BwE - Acessado em 18/10/18](https://www.inovecerto.com.br/kit-cancela-eletronica-automatica-brasso-1-2-hp-ppa-p2/?afiliadoid=34&utm_source=google&utm_medium=cpc&utm_content=KIT Cancela Elet r%C3%B4nica Autom%C3%A1tica Brasso - 1/2 HP - _PPA&utm_campaign=&gclid=CjwKCAjw3qDeBRBkEiwAsqeO7nYzf6AeDx8fBXqNoegv vZ-SB5EvZK4Te7iq3-eKBbK65_0XBq05nxoCU6UQAvD BwE)

[https://produto.mercadolivre.com.br/MLB-870731166-receptor-hcs-multifunco-linear- JM - Acessado em 18/10/18](https://produto.mercadolivre.com.br/MLB-870731166-receptor-hcs-multifunco-linear- JM)

[https://produto.mercadolivre.com.br/MLB-1064866482-100-tag-chaveiro-rfid-aproximaco-125khz-em4100-diversas-cor- JM - Acessado em 18/10/18](https://produto.mercadolivre.com.br/MLB-1064866482-100-tag-chaveiro-rfid-aproximaco-125khz-em4100-diversas-cor- JM)