Renan Gonçalves

Sistema Autônomo de Controle de Acesso Patrimonial por RFID

São José - SC

Abril / 2016

Renan Gonçalves

Sistema Autônomo de Controle de Acesso Patrimonial por RFID

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador:
Prof. M.Sc. Arliones Stevert Hoeller Junior

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

São José - SC

Abril / 2016

Monografia sob o título *"Sistema Autônomo de Controle de Acesso Patrimonial por RFID"*, defendida por Renan Gonçalves e aprovada em 1 de Abril de 2016, em São José, Santa Catarina, pela banca examinadora assim constituída:

Prof. Arliones Stevert Hoeller Junior, M.Sc.
Orientador

Prof. Eraldo Silveira e Silva, Dr.
Avaliador - IFSC

Prof. Clayrton Monteiro Henrique, Esp.
Avaliador - IFSC

“Nossa maior fraqueza está em desistir.
O caminho mais certo de vencer é tentar mais uma vez.
(Thomas Edison)

Agradecimentos

Gostaria de deixar meus mais sinceros agradecimentos ao Instituto Federal de Santa Catarina, campus de São José e a todos os professores que me proporcionaram a oportunidade de realizar este curso, em especial ao professor Arliones Stevert Hoeller Junior que me orientou no desenvolvimento deste trabalho. Aos meus pais e irmãos, que me apoiaram nos momentos difíceis, sendo atenciosos e carinhos, eles foram parte fundamental para a conclusão desta jornada, sem eles essa caminhada certamente seria muito mais árdua. A todos os amigos que pude fazer ao longo dessa jordana acadêmica, em especial João Carlos Warmling e Eduardo Guse grandes amigos, que me ajudaram muito ao longo do curso, mesmo após formados sempre estavam prontos para escutar e esclarecer minhas duvidas. Por fim agradeço a minha namorada e companheira Aline Poltronieri, que sempre esteve do meu lado incentivando e ajudando nos momentos difíceis, esta que muito me ensinou a encarar e enfrentar os problemas independente do tamanho ou quão difíceis eles possam ser.

Resumo

Estudos demostram a dificuldade em controlar manualmente o acesso dos usuários em diversos ambientes. Estes estudos também apresentam parâmetros relevantes para a escolha do sistema de controle automatizado, de modo a atender as especificações das áreas de segurança patrimonial e Tecnologia da Informação e Comunicação (TIC). Atualmente os sistemas de controle de acesso possuem dois modos de operação bem característicos: o online, que pode apresentar lentidão no processamento das requisições de acesso; o offline, que pode operar com suas informações desatualizadas devido à demora do servidor em realizar o sincronismo dos dados. Com base nos modelos citados, buscou-se suprir a problemática implementando um sistema offline sem a necessidade de replicação do banco de dados. Este sistema foi implementando utilizando a memória da *tag* RFID para armazenar dados relevantes à validação do acesso, não sendo necessário a troca constante de informações entre o servidor e o controlador de acesso durante a autenticação de um usuário, assim como não é necessário a replicação dos dados do servidor para cada um dos dispositivos. O sistema conta com entradas e saídas que permitem a integração com outros equipamentos de segurança utilizados para a gestão eficiente dos espaços controlados.

Palavras-chaves: Controle de Acesso, *Radio-Frequency Identification* (RFID), Segurança patrimonial, MIFARE Classic, MFRC522.

Abstract

Studies demonstrate the difficulty to manually control user's access to several environments. These studies also present relevant parameters to the choice of the automated control system to comply with the patrimonial security area's and ICT specifications. Current systems have two classic operation modes: online mode, that may present a delay to process authentication requests; and offline mode, that may operate with outdated information due to the server's synchronization process. Based on the cited models, this study proposes the implementation of an offline system that does not need to be in sync with the server, nor needs to replicate the access control data base. To achieve that, we implemented a system that uses the tag memory to store relevant data to the access validation, eliminates the constant information exchange between server and access controller during the user's access validation, and the need of data replication from the server to each one of the devices. The system has inputs and outputs that can be used to integrate with other devices used in access control systems.

Keywords: Access control, RFID, Patrimonial security, MIFARE Classic, MFRC522.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de abreviaturas e siglas

RFID *Radio-Frequency Identification*

TIC Tecnologia da Informação e Comunicação

IFF *Identify Friend or Foe*

RF Radio Frequência

EPC *Eletronic Product Code*

ISO *International Organization for Standardizatio*

EAN *European Article Number International*

UCC *Uniform Code Council*

IEC *International Engineering Consortium*

ISM *Industrial-Scientific-Medical*

ANATEL Agência Nacional de Telecomunicações

RADAR *Radio Detection and Ranging*

DoS *Denial of Service*

CI Circuito Integrado

UART *Universal Asynchronous Receiver/Transmitter*

FIFO *First in, first out*

EEPROM *Electrically-Erasable Programmable Read-Only Memory*

SO Sistema Operacional

GPIO *general purpose input/output*

SPI *Serial Peripheral Interface*

UID *Unique IDentifier*

NTP *Network Time Protocol*

RTC *Real Time Clock*

1 Introdução

Este trabalho apresenta a implementação de um sistema autônomo de controle de acesso patrimonial utilizando RFID para identificação dos usuários e liberação do acesso. O controle de acesso tem por objetivo restringir o acesso dos usuários aos ambientes controlados, de forma que seja possível determinar quem, e quando, poderá entrar nas dependências monitoradas.

No acesso patrimonial a forma mais comum de controle é a não automatizada, onde são utilizadas chaves mecânicas para liberação do acesso. Este método dificulta o controle e identificação dos usuários que acessam os ambientes (FINKENZELLER; MÜLLER, 2010). Conforme foi demonstrado por (THOMÉ et al., 2012), há uma grande dificuldade em controlar manualmente o acesso de diversos ambientes com grande concentração de usuários. Nesse estudo também foram apresentados os principais parâmetros utilizados na implantação de sistemas de controle de acesso, de modo a atender os requisitos das áreas de segurança patrimonial e TIC. Estes parâmetros envolvem a escolha do tipo de bloqueio, tecnologia de identificação, sistema de gestão e infraestrutura de comunicação.

Uma característica importante na especificação do projeto é no modo de funcionamento do dispositivo. Atualmente dois modelos são comumente utilizados:

- Online: Os sistemas que operam nesse modo possuem por característica principal a comunicação instântanea com os dispositivos controladores, sendo necessário a garantia de comunicação e a velocidade para processamento. Porém, se torna um ponto crítico que pode comprometer a qualidade do serviço;
- Offline: Nesse modelo as informações de acesso são distribuídas para todos os dispositivos controladores, reduzindo o tempo no ato da validação. Um ponto negativo é o fato que a informação pode não estar sempre atualizada em todos os dispositivos simultaneamente, fazendo com que parte do sistema possa operar com informações antigas.

Com base nos modelos citados buscou-se suprir a problemática implementando um sistema offline, sem a necessidade de replicação do banco de dados. O sistema sugerido utilizará a

memória da *tag* para realizar a validação do acesso, não sendo necessário que o controlador de acesso e o servidor troquem informações em cada autenticação, assim como não será necessário a replicação do banco de dados no dispositivo autenticador, pois todas as informações relevantes para a liberação do acesso do usuário estarão armazenadas na própria *tag*.

1.1 Objetivos

O objetivo principal deste trabalho é implementar um sistema autônomo de controle de acesso para restringir o acesso dos usuários aos ambientes controlados. Para a identificação dos usuários e liberação do acesso será utilizada a tecnologia RFID e todas as informações do usuário e suas permissões de acesso necessárias à autenticação estarão gravadas na memória interna da *tag*.

Para alcançar o objetivo principal acima, os seguintes objetivos específicos foram traçados:

- Especificar o mecanismo de controle de acesso;
- Implementar o mecanismo de controlador de acesso;
- Integrar o módulo RFID para a identificação das credenciais;
- Testar o fluxo padrão de uso do sistema;

1.2 Estrutura do documento

O capítulo 2 apresenta um estudo sobre sistemas de controle de acesso, métodos de identificação apresentando os pontos positivos e negativos, seguindo no aprofundamento da tecnologia RFID, dando respaldo para a definição do sistema de controle de acesso e encerrando com a apresentadas das ferramentas de hardware e software utilizadas.

O capítulo 3 apresenta a proposta do sistema a ser desenvolvido. São definidos os parâmetros de funcionamento, definido nos requisitos funcionais e não funcionais, seguido por uma visão geral do sistema com suas entradas e saídas, finalizando com a apresentação dos principais casos de uso.

O capítulo 4 descreve características de hardware e funcionalidades implementadas no software, apresentando o diagrama em blocos do controlador de acesso e a interligação entre os módulos usados no sistema. Nas funcionalidades do software são apresentados os diagramas

de classe e as tabelas criadas para o armazenamento dos registros em banco de dados. Estão descritas cada uma das entradas e saídas usadas no sistema, detalhando seu uso.

Finalmente, o capítulo 5 apresenta os resultados do trabalho, destacando os pontos mais importantes, além de explicitar as dificuldades encontradas na execução deste. O referido capítulo ainda lista tópicos não aprofundados que poderão servir de temas para trabalhos futuros.

2 *Fundamentação Teórica*

Este capítulo tem por objetivo apresentar as teorias e tecnologias em que este trabalho se baseia. Este capítulo baseia, além de mostrar um panorama do sistema de controle de acesso e da tecnologia RFID. No final do capitulo uma seção é destinada a apresentação do RASPBERRYPI, PYTHON, SQLITE, MIFARE Classic, entre outras ferramentas utilizadas no desenvolvimento do sistema.

2.1 Controle de Acesso

Os sistemas de controle de acesso, físicos ou lógicos, têm como objetivo proteger ambientes, equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. O termo controle de acesso, quando aplicado a ambientes físicos, é uma referência à prática de permitir o acesso a uma propriedade, prédio, ou sala, apenas para pessoas autorizadas. O controle físico de acesso pode ser garantido por meio de pessoas (guarda, segurança ou recepcionista); por meios mecânicos como fechaduras e chaves; ou através de meios tecnológicos, como sistemas baseados em senhas ou RFID. (WIKIPEDIA, 2015)

A necessidade de um controle de acesso automatizado surge quando há muitos ambientes e/ou muitos grupos de pessoas que possuem permissões de acesso distintas, aumentando a complexidade do controle. Associam-se a isto outras ações comuns nos dias atuais onde pode-se destacar o acesso de visitantes a áreas restritas, assim como o controle dos horários de entrada e saída evitando que os usuários fiquem nas suas dependências em horários indevidos (THOMÉ et al., 2012).

Neste caso, os responsáveis pela empresa juntamente com a equipe de segurança e a TIC, deverão especificar um sistema de controle de acesso. Estes analisarão as tecnologias e buscarão a melhor solução para atender as necessidade de segurança, condições financeiras e prazo de implantação. O mercado dispõe de muitos sistemas para controle de acesso de alta tecnologia, sendo o ponto principal as tecnologias para identificação do usuário ou sua credencial (THOMÉ

et al., 2012).

2.2 Métodos de identificação

Um usuário pode ser identificado de três maneiras distintas, onde cada técnica utiliza uma tecnologia diferente, com suas complexidades, vantagens e desvantagens.

Sistemas de segurança são, normalmente, compostos por mecanismos para confirmar três fatores:

- O que você sabe? O usuário conhece a credencial que irá liberar o acesso, um exemplo bem comum é a senha;
- O que você possui? O usuário possui uma credencial física que irá utilizar para a liberação do acesso, como exemplo pode ser sitar o bilhete utilizado no sistema de transporte coletivo;
- Quem você é? O usuário é sua própria credencial de acesso, por exemplo o biometria digital.

2.2.1 Senha

A identificação por senha é um mecanismo de autenticação simples, muito usado em sistemas de segurança de baixa complexidade. Este modelo possui um baixo custo de implantação e manutenção. Uma fragilidade desta técnica é que o usuário pode esquecer a senha. Além disso, a senha é de uso pessoal, porém não é possível garantir que o usuário não a repasse a outra pessoa, ou que a senha não seja copiada. Mediante as vulnerabilidades apresentadas, este método de identificação está sujeito a falhas de segurança que podem comprometer a integridade do ambiente controlado.

2.2.2 Biometria

A identificação biométrica (impressão digital, reconhecimento de íris ou facial, entre outras técnicas) necessita de um mecanismo de autenticação de alta complexidade, já que o sistema deverá ler e identificar os padrões do usuário para realizar a autenticação. O modelo mais difundido no mercado é a identificação biométrica por impressão digital. Este modelo possui um elevado custo de implantação do sistema e possui um baixo custo de manutenção.

As técnicas utilizadas para a identificação biométrica possuem características que exigem alto grau de processamento, elevando o tempo de resposta da autenticação, além de serem suscetíveis à falsa identificação.

2.2.3 Dispositivo de identificação

A identificação por cartão possui um mecanismo de autenticação mais elaborado do que o sistema por senhas, sendo que uma forma muito utilizada é a leitura de código de barras. Seus custos de implantação e manutenção não são altos. O uso do código de barras facilita a criação de novas credenciais com baixo custo de confecção, tornando o sistema vulnerável pela facilidade de gerar cópias das credenciais autorizadas.

Outro mecanismo que está ganhando espaço no mercado é a identificação por cartões (RFID), que possui uma maior complexidade na implementação. Ao longo da vida útil do sistema serão necessários pequenos investimentos para a criação de novas credenciais. Esta tecnologia possui mecanismos de segurança que dificultam a confecção de credenciais falsas.

2.3 Identificação por Rádio Frequência (RFID)

A Identificação por Rádio Frequência ou RFID usa o espectro eletromagnético como meio de comunicação para transmissão dos dados. Esta tecnologia está em grande expansão devido à sua ampla aplicabilidade, o que gera um alto volume de negócios, sendo assim alvo de grandes indústrias (GOMES, 2007).

Essa tecnologia é utilizada em sistemas de geolocalização, para a identificação e localização do patrimônio em uma indústria ou até mesmo em uma biblioteca. Utilizado em outras aplicações como identificação bovina e de animais domésticos, contendo os dados do animal e do proprietário. A tecnologia tem sido fortemente aplicada em mercados de identificação e controle de acesso, como sistemas para pagamento de passagem de ônibus e pedágio (GOMES, 2007).

2.3.1 Origem da tecnologia

Na década de 30 o físico Robert Alexander Watson-Watt realizou a descoberta do sistema de *Radio Detection and Ranging* (RADAR), deste modo sendo possível identificar uma aeronave a quilômetros de distância. O sistema foi utilizado durante a segunda guerra mundial pelos alemães, japoneses, americanos e britânicos. Porém, não eram capazes de identificar se as aeronaves eram inimigas ou aliadas que estariam retornando de uma missão. Então, os alemães

descobriram que se ao retornar de uma missão as aeronaves aliadas fizessem uma manobra no ar, causando uma mudança do sinal de rádio refletido de volta, era possível diferenciar aliados de inimigos, constituindo assim o primeiro sistema de RFID passivo (ROBERTI, 2005).

Liderados por Robert Alexander Watson-Watt os britânicos desenvolveram o primeiro sistema ativo. Foram instalados transmissores nos aviões, e ao receber um sinal da estação de radar era transmitido um sinal de volta para a estação. Assim se tornou seguro a identificação de amigos e inimigos, o sistema foi chamado de *Identify Friend or Foe* (IFF) (ROBERTI, 2005).

2.3.2 Componentes básicos dos RFID

O sistema RFID é composto por dois componentes básicos conforme a figura 2.1, o *transponder*[1] ou *tag*[1], que é o objeto a ser identificado, e a unidade de leitura responsável por realizar a identificação da *tag*. Dependendo da concepção e tecnologia a unidade de leitura poderá ler e escrever dados na *tag*. Ao longo deste documento iremos tratar a unidade de leitura contemplando essas funções de leitura e escrita nas *tags* (MICROCHIP, 2004).

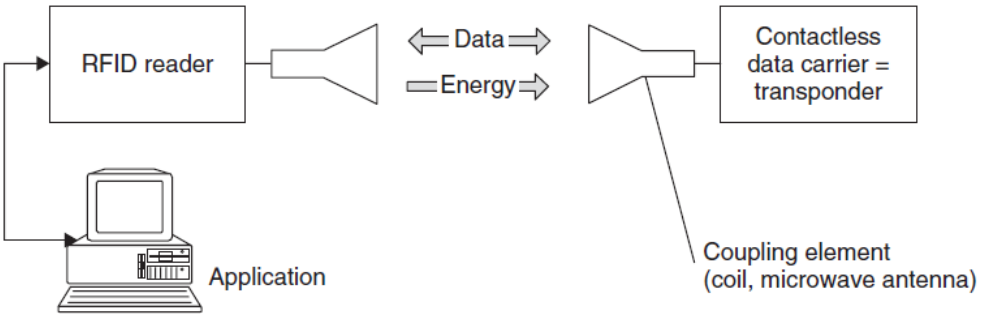

Figura 2.1: Principais componentes do sistema RFID: Leitor e Tag.

Conforme a figura 2.2, a *tag* é composta por um microchip e uma antena, esta podendo ser de diversos formatos e tamanhos. Suas funcionalidades podem variar das mais simples, como os microchips de uso único que possuem dois estados ativo e inativo, onde após ser inativado este deixa de funcionar e a operação é irreversível, passando por outros que permitem a leitura das informações contidas nele, chegando aos mais sofisticados onde é possível realizar leituras e escritas na memória como sendo uma pequena base de dados (INTERMEC, 2007).

[1]Dispositivo de identificação de Radio Frequência (RF).

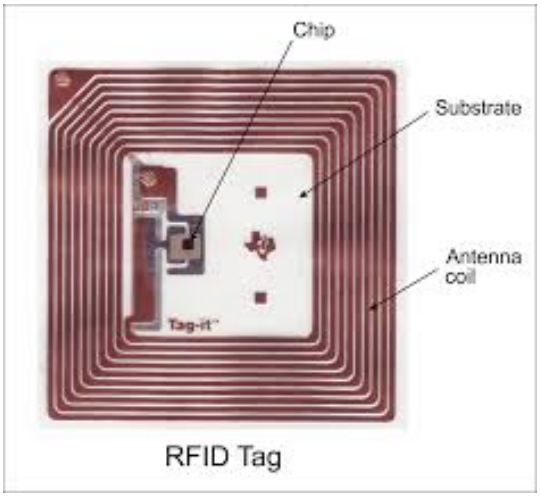

Figura 2.2: Componentes de uma Tag (INTERMEC, 2007).

A construção da *tags* é dinâmica, permitindo que esta possa ser de diversas formas e tamanhos, podendo ser tão pequeno quanto um grão de arroz. Pode ser constituída com materiais que permitem o funcionamento em condições extremas de calor, frio e umidade.

A *tag* possui três possíveis modos de operação, sendo eles:

- Passivo: a energia necessária para alimentação do microchip e todo o processo de comunicação será fornecida pela unidade de leitura, este irá ter seu alcance limitado em alguns poucos metros;
- Ativo: possui uma fonte de energia própria, pode iniciar a transmissão dos dados independente da existência de uma unidade de leitura para receber os dados, pode estabelecer a comunicação com algumas dezenas de metros de distância;
- Semi-ativo: possui uma fonte de energia própria, porém assim como a *tag* passiva depende de um estímulo da unidade de leitura para iniciar a comunicação. Seu alcance é superior a *tag* passiva e inferior a *tag* ativa.

A unidade de leitura é composta por uma antena para envio do sinal RF e por um chip. Este chip é responsável por gerenciar e controlar a comunicação com as *tags*, podendo rejeitar dados duplicados, realizar a correção de erros entre outras funcionalidades. Alguns desses chips podem implementar mecanismos de segurança garantindo a integridade e confidencialidade das informações transmitidas durante o processo de comunicação (INTERMEC, 2007).

2.3.3 Princípios de funcionamento

Sistemas de identificação por rádio-frequência podem operar de diversas maneiras. A seguir serão descritos os dois principais modos de operação. O acoplamento indutivo é muito utilizado em baixa frequência de 100-135KHz e 13,56MHz, o acoplamento reflexivo é utilizado para frequências superiores a 900MHz.

Acoplamento indutivo

Este modelo funciona com um circuito LC ou ressonante, criando um campo magnético de alta frequência. Quando a *tag* se aproxima do campo magnético criado pela unidade de leitura, este campo irá induzir uma corrente no circuito LC da *tag*. Quando a frequência gerada pela unidade de leitura é compatível com a frequência da *tag*, o sistema ressonante irá responder com uma variação (modulação) na frequência. Esta modulação causará uma pequena variação de tensão nos terminais da bobina utilizada pela unidade de leitura (MICROCHIP, 2004).

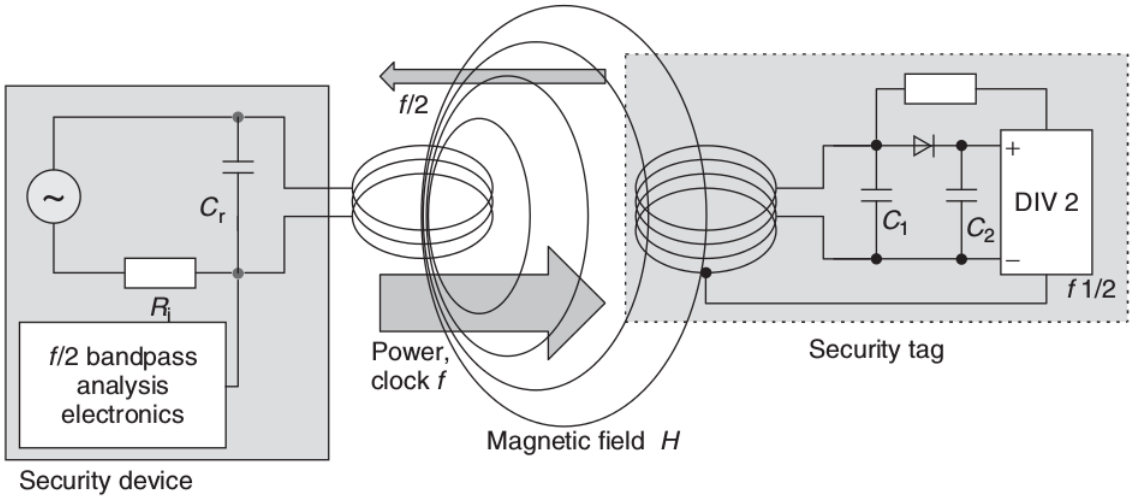

Figura 2.3: Funcionamento da comunicação entre unidade de leitura e *tag* com sistema de acoplamento indutivo (FINKENZELLER; MÜLLER, 2010).

Ao ocorrer o acoplamento da *tag* junto à unidade de leitura, esta sofrerá uma queda de tensão na sua resistência interna como é possível ver na figura 2.4. A *tag* realizará o acoplamento e desacoplamento de uma resistência para que ocorra o efeito de uma modulação de amplitude na tensão da antena da unidade de leitura, assim possibilitando a identificação dos dados transmitidos pela *tag* através da modulação de carga (MICROCHIP, 2004).

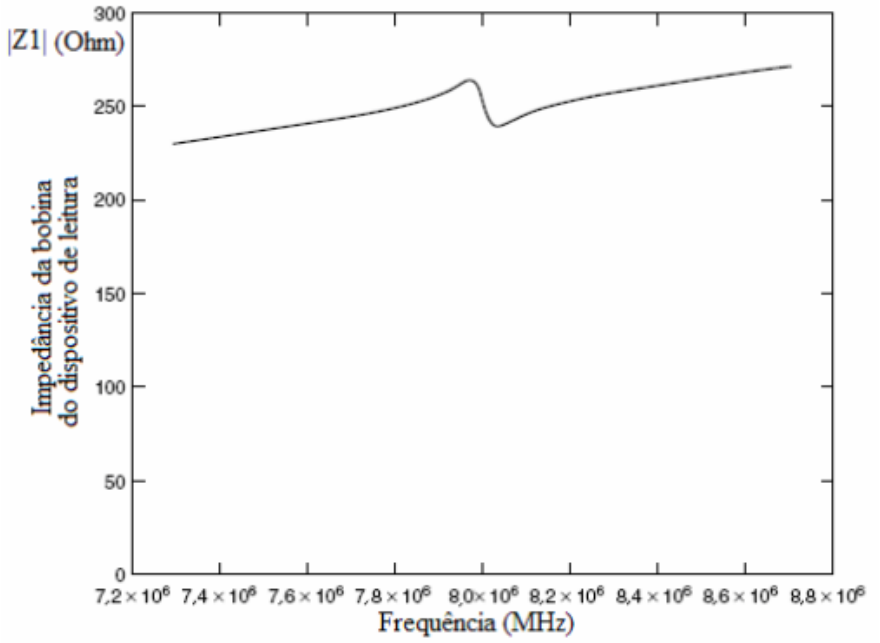

Figura 2.4: Cruzamento da Frequência entre unidade de leitura e tag (FINKENZELLER; MÜLLER, 2010).

Acoplamento reflexivo

A *tag* reflete as ondas enviadas pela unidade de leitura. O sinal refletido permanecerá na mesma frequência. Deste modo o sistema operará no modo *Half-Duplex*, onde cada unidade terá seu tempo de transmissão individual. Para que a *tag* possa enviar as informações para a unidade de leitura, será necessária uma modulação da mensagem a ser transmitida. A modulação ocorre conforme as características da construção da *tag*. Na figura 2.5 é possível observar os três principais componentes. O *microchip* comanda as operações na *tag*, as antenas são utilizadas para reflexão do sinal enviado pela unidade de leitura e o resistor é responsável por realizar a conexão de uma das antenas no circuito. Deste modo, o *microchip* consegue realizar a modulação da mensagem que será enviada para a unidade de leitura (CARRIJO, 2009).

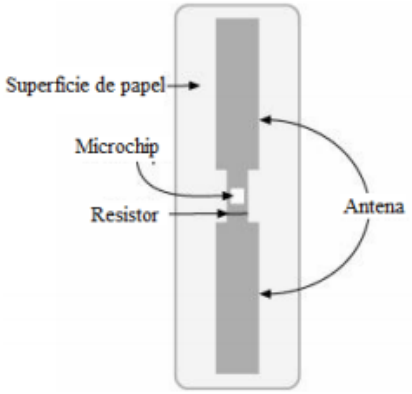

Figura 2.5: Construção da *tag* para acoplamento reflexivo.

2.3.4 Normas e Padrões de RFID

A padronização tem por princípio definir características de operação e funcionamento, permitindo que diversos equipamentos possam operar sem causar interferência uns nos outros. Algumas organizações estão trabalhando em parceria com empresas e estudiosos para padronizar protocolos e regras de uso para o RFID. A ISO, uma organização internacional que engloba 148 países, é uma das grandes organizações envolvidas na padronização, sendo a responsável por aprovar muitas normas técnicas internacionais, exceto as referentes a eletricidade e eletrônica, estas sendo de responsabilidade da *International Engineering Consortium* (IEC). Na tabela 2.1 são apresentados os padrões publicados pela ISO para o RFID (OLIVEIRA; PEREIRA, 2006).

A EPCGlobal é uma divisão da *European Article Number International* (EAN) e do *Uniform Code Council* (UCC), criada com o objetivo de desenvolver, controlar e promover o padrão *Eletronic Product Code* (EPC) ou código eletrônico de produtos. O EPC tem por objetivo definir a arquitetura para o desenvolvimento de aplicações como uma forma de identificação de um produto da linha de produção até a comercialização com um código único. Possibilitando a adoção a nível mundial de um sistema de identificação automática (OLIVEIRA; PEREIRA, 2006).

Sistemas de RF produzem e irradiam ondas eletromagnéticas, deste modo é necessário determinar as faixas do espectro de frequência para as diversas aplicações, evitando a interferência em outros sistemas. Conforme a figura 2.6 e a tabela 2.2, as faixas de frequências utilizadas pelos sistemas de RFID são poucas e são compartilhadas com os sistemas *Industrial-Scientific-Medical* (ISM) (FINKENZELLER; MÜLLER, 2010).

ISO Standard	Título	Status
ISO 11784	RFID para animais – estrutura de código	Publicado em 1996
ISO 11785	RFID para animais – concepção técnica	Publicado em 1996
ISO/IEC 14443	Identificação de cartões – cartões com circuitos integrados sem contato – cartões de proximidade	Publicado em 2000
ISO/IEC 15693	Identificação de cartões – cartões com circuitos integrados sem contato – cartões de vizinhança	Publicado em 2000
ISO/IEC 18001	Tecnologia da Informação – Gerenciamento de Itens de RFID – Perfil de Requisitos de Aplicação	Publicado em 2004
ISO/IEC 18000-1	Parâmetros Gerais para Comunicação por Interface por Ar para Frequências Globalmente Aceitas	Publicado em 2004
ISO/IEC 18000-2	Parâmetros para Comunicação por Interface por Ar abaixo de 135 kHz	Publicado em 2004
ISO/IEC 18000-3	Parâmetros para Comunicação por Interface por Ar em 13,56 MHz	Publicado em 2004
ISO/IEC 18000-4	Parâmetros para Comunicação por Interface por Ar em 2,45 GHz	Em Revisão Final
ISO/IEC 18000-6	Parâmetros para Comunicação por Interface por Ar em 860 a 930 MHz	Publicado em 2004
ISO/IEC 15961	Gerenciamento de Itens de RFID – Protocolo de Dados: Interface de Aplicação	Publicado em 2004
ISO/IEC 15962	Gerenciamento de Itens de RFID – Protocolo: Regras de Codificação de Dados e Funções de Memória Lógica	Publicado em 2004
ISO/IEC 15963	Gerenciamento de Itens de RFID – Identificação única do RF Tag	Em Revisão Final

Tabela 2.1: Padrões ISO para a RFID

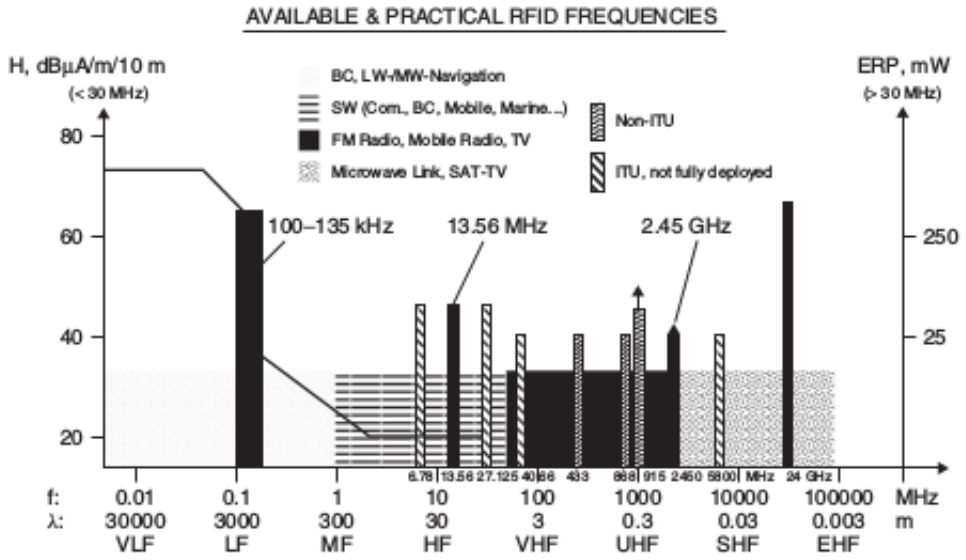

Figura 2.6: Faixas de frequências utilizadas por sistemas RFID (FINKENZELLER; MÜLLER, 2010).

A faixa de 13,56MHz está localizada no meio da faixa de ondas curtas, com alta capacidade de propagação em qualquer período do dia. Esta faixa é muito utilizada em sistemas de rádio e

Distribuição das frequências para sistemas RFID	
Frequência	**Descrição**
9 a 135 kHz	Low Frequency (LF)
6,78 MHz	ISM Frequency
13,56 MHz	High Frequency (HF)
27,125 MHz	High Frequency (HF)
433,92 MHz	Very High Frequency (VHF)
869 MHz	Ultra High Frequency (UHF)
915 MHz	Ultra High Frequency (UHF)
2,45 GHz	Microondas
5,8 GHz	Microondas
24,125 GHz	Super High Frequency (SHF)

Tabela 2.2: Distribuições de frequências para sistemas RFID (OLIVEIRA; PEREIRA, 2006).

telecomunicações, para conexões ponto a ponto, além de diversas outras aplicações ISM.

Na construção de um sistema que utilizará RFID deve ser escolhida a frequência mais apropriada. Definindo o tipo de acoplamento e características da faixa de frequência, essas informações são fundamentais para construção de partes importantes do sistema como o circuito LC e em especial a antena.

No Brasil, a Agência Nacional de Telecomunicações (ANATEL) é o órgão regulador das telecomunicações. Em 2008 entrou em vigor a Resolução nº 506 que trata do regulamento sobre equipamentos de radiocomunicação de radiação restrita, onde está inserido o RFID. O Capítulo I trata dos objetivos e definições, complementado no artigo 2º inciso XIV onde é descrita a definição de RFID ou similares:

> ”XIV - Sistema de Identificação por Radiofrequência (RFID) ou similar: sistema, composto por dispositivo transceptor, que recebe e envia sinais de radiofrequências, quando excitado por um equipamento transceptor interrogador, que tem a capacidade de efetuar a leitura, escrita ou modificação das informações contidas no dispositivo;”(ANATEL, 2008).

2.3.5 Segurança

Para prover a segurança é importante que se identifique as possíveis ameaças, para isso existem alguns questionamentos: De quais ameaças o sistema deve ser protegido? Quem são os invasores em potencial? Por quanto tempo o sistema deve resistir ao ataque? Perguntas essas que são de extrema importância para a implementação dos mecanismos de segurança e, em caso de invasão, o sistema deve estar preparado para reagir. Os questionamentos são fundamentais

para definir o nível de segurança necessário e o custo para a implementação (REZENDE, 2011).

A boa implementação de técnicas de segurança e criptografia são fundamentais para manter a integridade e privacidade das informações. Não é possível garantir 100% da segurança, mas devem ser atingidos níveis de equilíbrio entre o que é possível e o que é aceitável. É importante que sistemas e pessoas ajam de maneira a dificultar as ações dos invasores e/ou coletores de dados. Por parte dos sistemas já estão disponíveis algoritmos e protocolos, de modo a promover um elevado grau de proteção. É de extrema importância que esses mecanismos sejam implementados por especialistas para que seja possível tirar o melhor proveito das ferramentas (REZENDE, 2011).

Assim como outros sistemas de telecomunicações ou tecnologia da informação, o RFID também enfrenta potenciais riscos. Na imagem 2.7 é possível observar uma gama de ataques que um sistema RFID está sujeito. Estes podem ser destinados à unidade de leitura ou à interface RF entre o leitor e a *tag* (FINKENZELLER; MÜLLER, 2010).

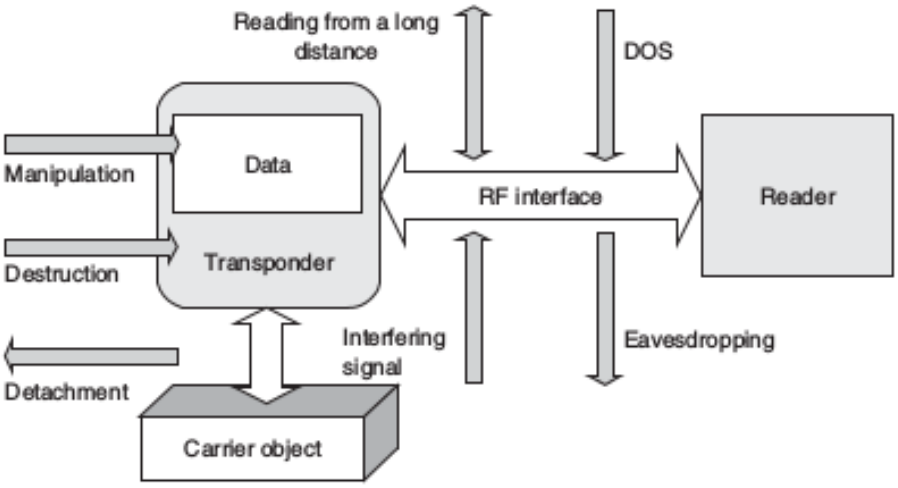

Figura 2.7: Ataques Básicos na RFID (FINKENZELLER; MÜLLER, 2010).

Algumas das formas de violação que podem ser aplicadas nas *tags* e/ou à unidade de leitura (PINTO; ANTUNES; SANTOS, 2011):

- *Cloning*: É a realização de uma cópia física ou variação da *tag* que possa ser entendida como válida por um sistema de autenticação;
- *Spoofing*: É uma variação do *Cloning* onde não é realizada uma cópia física da *tag* e sim a emulação através de campos magnéticos;
- *Eavesdropping*: É uma técnica para captura de informações secretas através de leitores especiais. Geralmente as informações capturadas serão posteriormente utilizadas em

combinação com a *Man-in-the-middle*.

- *Man-in-the-middle*: Consiste em passar-se por uma leitora legítima com a finalidade de recolher informações ou manipular os dados da *tag*, podendo até inserir códigos maliciosos;
- *Code Injection Attack*: Injeção de código maligno em conjunto das *tags* manipuladas para realizar a exploração de vulnerabilidades do sistema de modo a levá-lo a um pane;
- *Denial of Service* (DoS): Com a emulação de *tags*, sobrecarrega o sistema de modo a deixá-lo indisponível.

2.3.6 Vantagens e Desvantagens do emprego de RFID

Desvantagens:

Os sistemas RFID possuem um alto custo quando comparados aos sistemas de código de barras, e este é o principal obstáculo para seu uso em aplicações de logística Outro problema enfrentado pela tecnologia é a aplicação em materiais metálicos e condutivos, já que estes afetam o alcance de transmissão. Os consumidores veem a aplicação desta tecnologia em produtos de consumo como sendo uma invasão de privacidade. Para esse caso existem técnicas de bloqueio do RFID quando o consumidor sai da loja, mas ainda estão com custos elevados.

Vantagens:

Principal vantagem do uso da tecnologia RFID é a facilidade de identificação da *tag*. A tecnologia permite que seja realizada a leitura sem que seja necessário o contato ou uma visada direta, sendo assim a *tag* pode ser aplicada internamente nos produtos ou em suas embalagens.

A tecnologia RFID possui outras vantagens, como o armazenamento de informações e um baixíssimo tempo de resposta, podendo ser inferior a 100 ms. Dessa forma, essa tecnologia torna-se uma boa opção para processos produtivos e para o controle de acessos, onde é necessário ler os dados da tag em movimento, permitindo que o produto carregue seu histórico, facilitando a contagem de estoques e agilizando a autenticação de pessoas.

2.4 Ferramentas Utilizadas

Nesta seção estão descritas as ferramentas utilizadas para o desenvolvimento do projeto. Foram utilizadas algumas ferramentas *Open Source*, mantidas por comunidades sem fins lucrativos. A escolha das ferramentas foi baseada em suas características e capacidade em atender as necessidades do projeto, assim como a quantidade de documentação disponibilizada nas comunidades virtuais.

2.4.1 Leitor de RFID

O módulo RFID utilizado consiste em um Circuito Integrado (CI) MFRC522 que possibilita a leitura e escrita da *tag*. Ele suporta ISO/IEC 14443A no modelo , operando em frequência de 13,56MHz em comunicação sem contato. O MFRC522 possui um sistema robusto e eficiente para a demodulação e decodificação da *tag* RFID, podendo operar a uma velocidade de 848kBd nas operações de leitura e escrita (NXP, 2014).

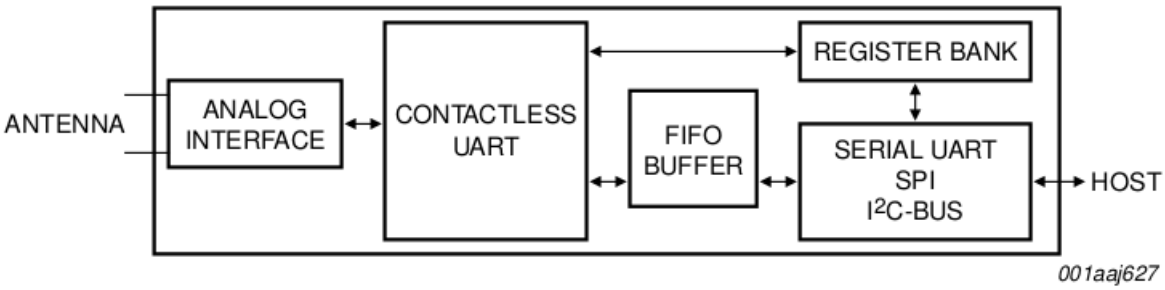

Figura 2.8: Diagrama de Blocos do CI MFRC522 (NXP, 2014).

A figura 2.8 apresenta o diagrama de blocos do MFRC522. Nele é possível observar de maneira sucinta o funcionamento do CI. A antena recebe o sinal analógico e encaminha para a interface analógica, que fará a modulação e demodulação dos sinais. O módulo *Universal Asynchronous Receiver/Transmitter* (UART) sem contato gerencia os requerimentos dos protocolos de comunicação com a *tag*. O *buffer First in, first out* (FIFO) garante a transferência rápida dos dados entre o UART sem contato e o *host*, através do protocolo escolhido (NXP, 2014).

2.4.2 Cartão RFID

O MIFARE Classic é desenvolvido pela NXP e está no mercado desde 1994. É um cartão inteligente sem contato e está em conformidade com a ISO/IEC 14443A. Este cartão consiste ba-

sicamente em uma antena, um chip de processamento com uma memória *Electrically-Erasable Programmable Read-Only Memory* (EEPROM) de 1k (MF1 S50) ou 4K (MF1 S70) dependendo do modelo. Possui um mecanismo de criptografia (Crypto1) com duas chaves permitindo o uso em múltiplas aplicações com hierarquia de chave (NXP, 2011).

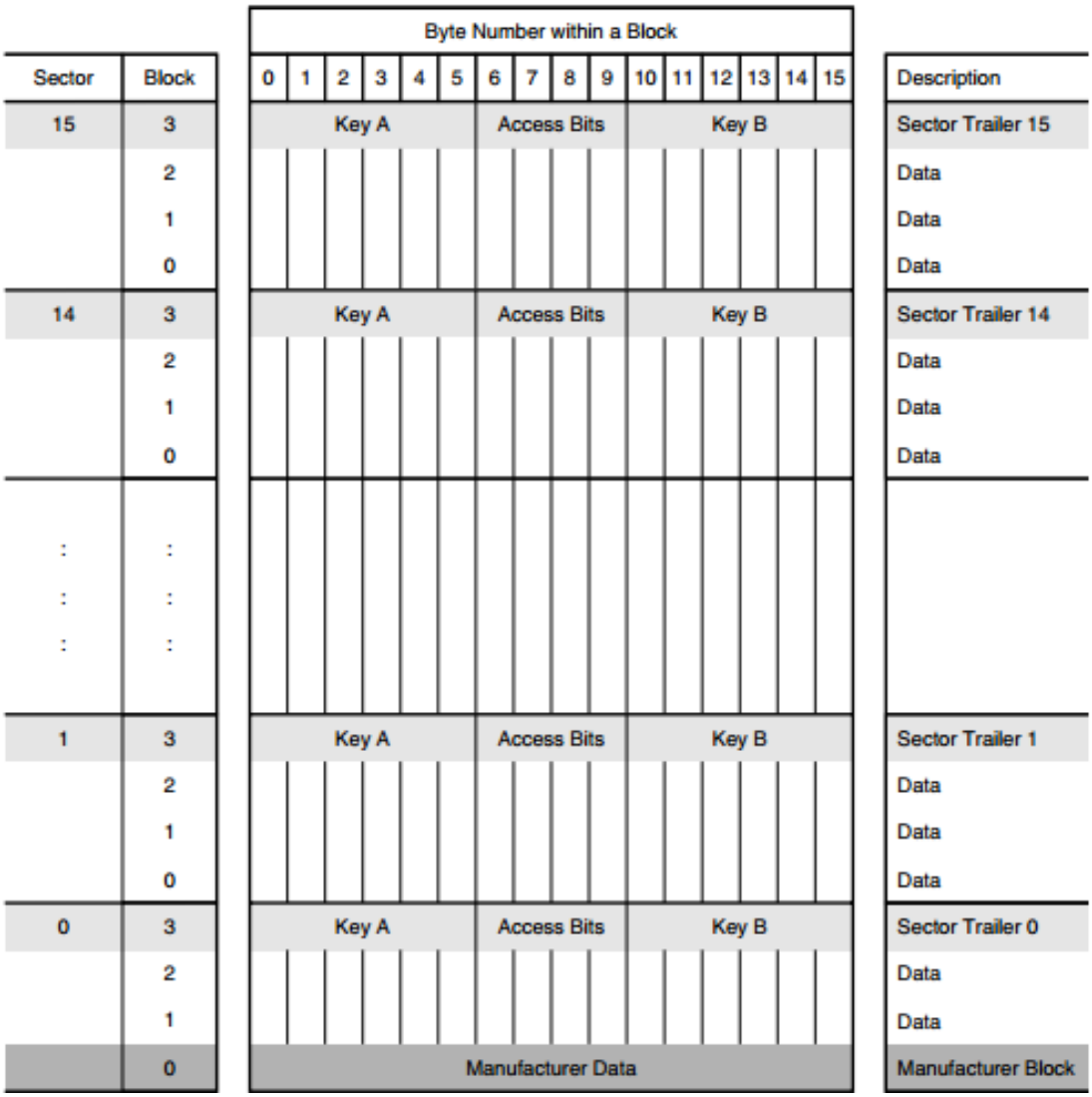

Figura 2.9: Organização da memória MIFARE Classic MF1S50 (NXP, 2011).

Para o desenvolvimento do sistema foi utilizado o MIFARE Classic EV1 com 1k byte de memória, organizada em 16 setores de 4 blocos, sendo que cada bloco contém 16 bytes. O bloco 0 do setor 0 é reservado para informações do fabricante, no bloco 3 de cada setor serão armazenadas as chaves de criptografia, conforme demostrado na figura 2.9 (NXP, 2011).

2.4.3 Modelo de criptografia do MIFARE Classic

Os cartões MIFARE Classic utilizam o algoritmo criptográfico proprietário Crypto-1 desenvolvido pela NXP Semicondutores (SOUZA, 2011). O algoritmo é executado em hardware com o objetivo de obter o melhor desempenho. O mecanismo de criptografia utiliza chaves simétricas de 48 bits.

A comunicação entre a leitor e *tag* inicia quando a *tag* entra no campo magnético criado pela leitora elas trocam algumas mensagens verificando compatibilidades. Finalizando essa etapa de sincronismo a leitora envia uma mensagem para a *tag* solicitando autenticação em uma bloco específico. Na figura 2.10 é apresentado o processo de autenticação de uma *tag* MIFARE Classic. A processo de autenticação ocorre quando a leitora solicita para autenticar em um bloco específico, este processo é realizada em 3 passos:

- A *tag* lê a chave secreta e verifica as condições de acesso ao bloco requisitado pela leitora. Então a *tag* envia um desafio nonce[2] nC para a leitora;
- A partir desta mensagem a comunicação é criptografada. A leitora envia a resposta rL ao desafio da *tag* e um desafio nonce nL que deverá ser resolvido pela *tag*.
- Se a resposta da leitora estiver correta a *tag* termina a autenticação enviando a resposta rC ao desafio da leitora. A resposta enviada pela *tag* será validada pela leitora.

Finalizando essa processo de autenticação será realizada a transição dos dados.

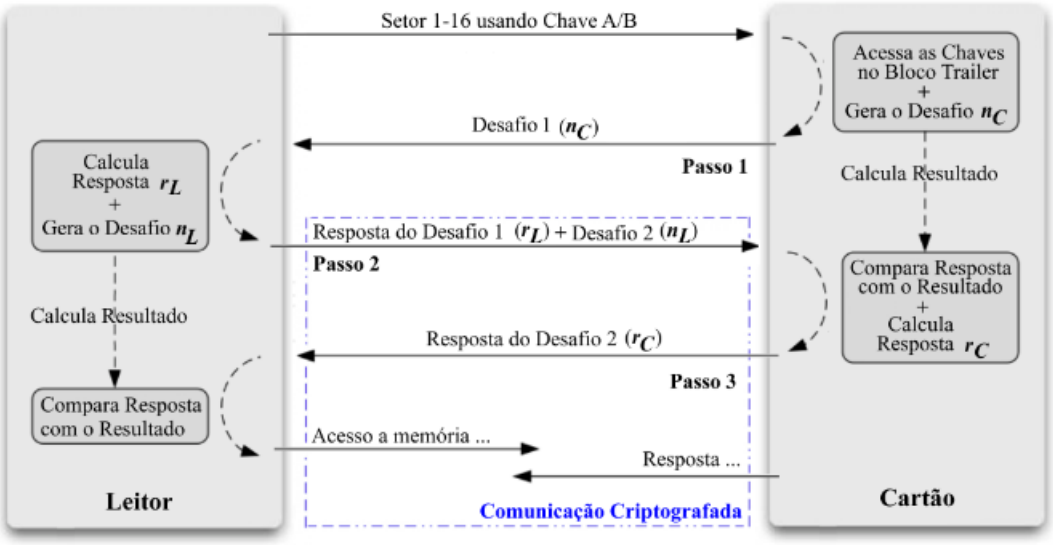

Figura 2.10: Autenticação Mifare Classic (SOUZA, 2011).

[2]Usado uma única vez - Do inglês, *number used once*.

2.4.4 RASPBERRYPI

O RASPBERRYPI é um pequeno computador. Seu hardware é integrado em uma única placa. Para realizar as primeiras operações com este equipamento basicamente é necessário conectar um mouse, teclado, ligar a uma televisão ou monitor e a uma fonte de energia apropriada. Ele foi desenvolvido pela Fundação RASPBERRYPI, com sede no Reino Unido, com o objetivo de promover a educação de crianças e adultos na área de Ciência da Computação (FUNDATION RASPBERRY PI, 2016). Sendo este um projeto com uma finalidade educacional, há grande disponibilidade de material de apoio para o desenvolvimento.

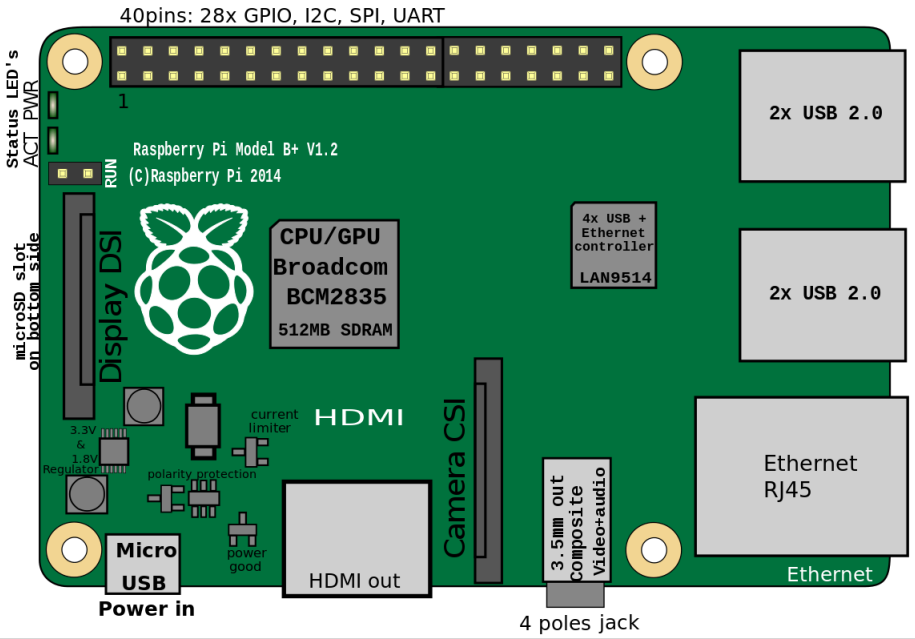

Figura 2.11: RASPBERRYPI B+ V1.2 RFID (FUNDATION RASPBERRY PI, 2016).

Foi utilizado o RASPBERRYPI 1 Model B+ v1.2, consumindo entre 700-1000 mA, dependendo dos periféricos que estão conectados. Ele possui um hardware bem compacto (85mm x 56mm x 21mm), conta com 512MB de memória e um processador ARM de 700 MHz para gerenciamento de suas 28 GPIO, 4 USB 2.0, Micro SD, Ethernet, HDMI, Câmera, áudio (FUNDATION RASPBERRY PI, 2016).

2.4.5 Linux embarcado para RASPBERRYPI

Como visto na seção anterior, o RASPBERRYPI precisa de alguns periféricos de entrada e saída de dados (mouse, teclado e monitor),sendo recomendado um Sistema Operacional (SO), como o Windows, Linux e Mac para facilitar a integração com os periféricos. A fundação

RASPBERRYPI disponibiliza em seu site 3 versões do Raspbian (Raspbian Jessie Lite, Raspbian Jessie e Raspbian Wheezy), que são baseados no Debian. Para o desenvolvimento deste trabalho foi utilizada a versão Raspbian GNU/Linux 7 (wheezy). Ainda no site da fundação, estão disponíveis outras versões desenvolvidas por terceiros (ubuntu, windows 10, OSMC, OpemELEC, PiNet e RISC OS Open), mas alguns desses são compatíveis apenas com a versão mais recente, o RASPBERRYPI2 (FUNDATION RASPBERRY PI, 2016).

2.4.6 Linguagem de Programação *Phyton*

Para o projeto foi utilizada a versão 2.7.3 do PYTHON, uma linguagem de programação com seu projeto de código aberto (licença compatível com a General Public License [GPL]), mais permissiva, autorizando o uso do PYTHONem projeto de produtos proprietários. O desenvolvimento da linguagem é comunitário e gerenciado pela *Python Software Foundation*, instituição sem fins lucrativos (BORGES, 2010).

A linguagem PYTHONé de programação clara e sucinta. Um programa em PYTHONpode ser escrito de maneira estruturada, funcional ou orientada a objeto, tornando-se uma linguagem multi-paradigma. O PYTHONé uma linguagem robusta com estruturas de alto nível, possui listas, dicionários, data/hora, além dos módulos de terceiros que podem ser adicionados. Também possui recursos que são encontrados em linguagens modernas, como persistência, metaclasses e unidades de teste. (BORGES, 2010).

A figura 2.12 ilustra o processo onde o código fonte é transformado em bytecode, que é um formato binário com instruções para a máquina virtual PYTHONou interpretador, o que possibilita a portabilidade do programa para outros SO ou até mesmo plataformas 32 bits e 64 bits (BORGES, 2010).

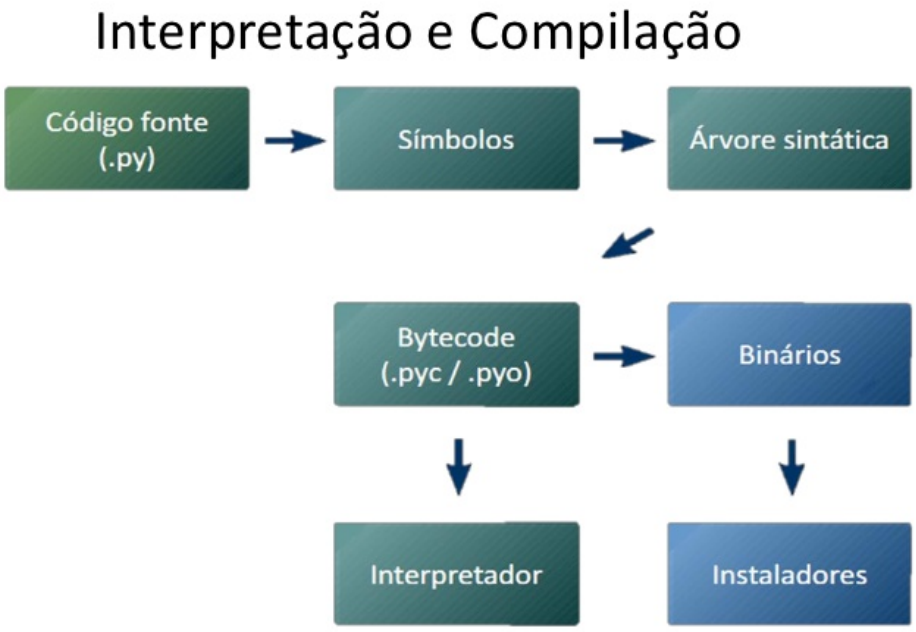

Figura 2.12: Diagrama de Bloco Interpretação e compilação PYTHON

2.4.7 Banco de Dados SQLITE

No desenvolvimento do sistema foi utilizada a versão 3.7.13 do SQLITE, um banco de dados auto-suficiente de linguagem SQL que não necessita de um processo servidor separado. É um banco de dados comum, com várias tabelas, índices, *triggers* e *views*, tudo em apenas um arquivo. O formato do arquivo do banco de dados é multi-plataforma, compatível com plataforma 32 bits e 64 bits, podendo ser usado por sistemas de grande ou pequeno porte. O SQLITEpossui uma biblioteca compacta, podendo ser usando em equipamentos com memória restrita como celulares e MP3 Players. Mesmo com restrição de memória consegue operar com bom desempenho (SQLITE, 2016).

2.4.8 NTP

O modelo de dispositivo utilizado não possui *Real Time Clock* (RTC) interno para persistência do horário em caso de desligamento, portanto nessa versão o controlador necessita ajustar o relógio ao iniciar o sistema. Para realizar o ajuste do relógio foi utilizada a versão 4.2.6p5 do ntpd, um serviço dedicado a manter atualizado o relógio do dispositivo, este realiza constantes verificações para mantendo o dispositivo com data e hora sincronizados com o servidor central.

3 O Sistema Proposto

O controle de acesso mais comum são as chaves mecânicas utilizadas na grande maioria das portas, este sistema não é automatizado, dificultando o controle e gerenciamento dos acessos. Neste capítulo será apresentado a proposta do sistema de controle de acesso automatizado, tendo como objetivos manter os ambientes físicos bloqueados, sendo que a liberação é mediante a autenticação por *tag* RFID.

3.1 Visão Geral

Conforme representado na figura 3.1, os sistemas de controle de acesso automatizados comumente operam de duas maneiras: Online, é necessário que em cada requisição de acesso o controlador troque mensagens instântaneas com o servidor para fazer a validação do acesso; Offline, o servidor deve realizar uma cópia do banco de dados e enviar para os controladores de acesso, permitindo que processem as requisições de acesso, neste modelo as informações podem não ser atualizada em todos os dispositivos simultaneamente.

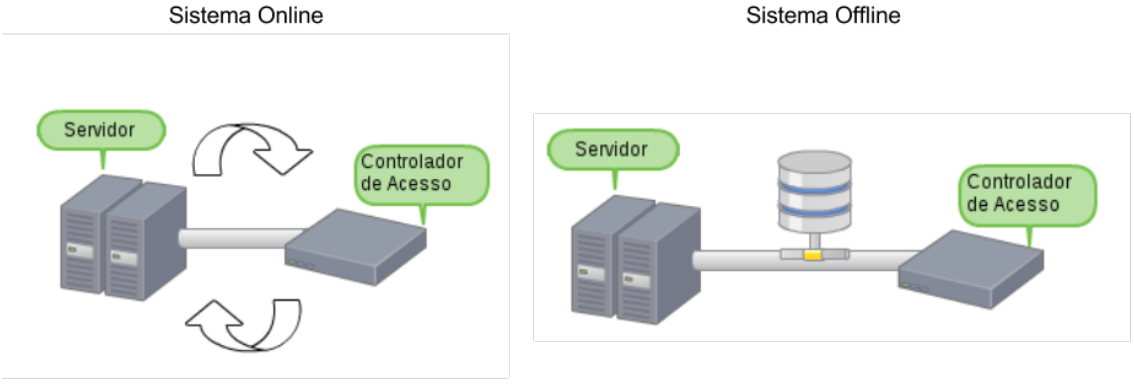

Figura 3.1: Representação dos modelos de sistema de controle de acesso (Online e Offline).

O sistema implementado deve opera em modo offline, onde cada dispositivo toma suas próprias decisões. Este processo de descentralização da autenticação do usuário não necessita

da replicação do banco de dados. Para isso o sistema utiliza a memória da *tag* RFID, onde serão armazenadas as informações de acesso do usuário.

O figura 3.2 apresenta o diagrama em blocos de algumas interfaces necessárias para o sistema de controle de acesso patrimonial. Este possui uma interface de comunicação destinada a configurações, a interface de comunicação RFID para as interação com as *tag*, entrada e saída de comando para controle dos ambientes e interação com outros sistemas supervisórios. A partir destas premissas do sistema serão apresentadas nas seções a seguir detalhes da proposta do sistema.

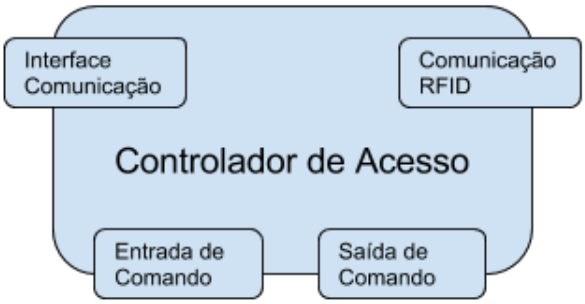

Figura 3.2: Diagrama em Blocos Visão Geral Controlador de Acesso.

3.2 Objetivos

O objetivo principal deste trabalho é implementar um sistema autônomo de controle de acesso patrimonial, para restringir o acesso dos usuários aos ambientes controlados. Para a identificação dos usuários e liberação do acesso será utilizada a tecnologia RFID, as informações do usuário, permissões de acesso e demais dados necessários para à autenticação estarão gravadas na memória interna da *tag*.

Para alcançar o objetivo principal acima, os seguintes objetivos específicos foram traçados:

- Especificar o mecanismo de controle de acesso;
- Implementar o mecanismo de controlador de acesso;
- Testar o fluxo padrão de uso do sistema;

3.3 Requisitos do Sistema

Nesta sessão são apresentados os requisitos funcionais e não funcionais do projeto, utilizados ao longo do desenvolvimento.

Requisitos funcionais:

- **RF1:** Implementar controle de acesso com RFID de modo offline, armazenando na memória da *tag* as permissões de acesso;
- **RF2:** Configurar *tag* do usuário com permissões de acesso, nível de usuário, zona de tempo e validade;
- **RF3:** Inativar *tag* do usuário para que o mesmo tenha sua solicitação de acesso negada;
- **RF4:** Liberar o acesso de usuários previamente cadastrados e sem restrições;
- **RF5:** Bloquear o acesso de usuários não cadastrados ou irregulares;
- **RF6:** Indicar ao usuário se foi liberada ou negada a solicitação de acesso;
- **RF7:** Monitorar estado da porta identificando aberta, fechada ou se houve um arrombamento;
- **RF8:** Registrar log dos acessos de entrada e saída dos usuários em cada um dos dispositivos;
- **RF9:** Visualizar registros de log;
- **RF10:** Liberar ambiente através de acionamento de alta prioridade para integração com sistema de incêndio;

Requisitos não funcionais:

- **RNF1:** Segurança: os dados no RFID devem ser criptografados;
- **RNF2:** Segurança: Se houver comunicação em rede no sistema, esta deve ser segura;
- **RNF3:** Acesso: permissões de acesso devem ser gravadas na *tag*;

3.4 Modelo de Domínio

A figura 3.3 apresenta uma visão geral do sistema e seus principais componentes. Podemos dividí-lo em dois grandes blocos: o controlador, que será instalado junto à porta ou catraca para comandar a abertura; e servidor, onde é instalada a aplicação para gerenciamento, permitindo a realização dos cadastros e auditoria com o auxílio dos registros de acessos.

O controlador é composto por uma unidade central de controle e suas interfaces. O sistema dispõem de uma interface de comunicação com o servidor, permitindo o sincronismo do log de acesso. A SPI - Leitor faz a comunicação com a unidade de leitura RFID, responsável por fazer a comunicação com a *tag*. Estão disponíveis alguns pinos de entrada e saída (I/O), como por exemplo a de emergência que permite a liberação do acesso imediatamente quando acionada. Os I/O - Sensor_Porta e I/O - Acionador, são utilizadas respectivamente para monitorar o estado do equipamento a ser controlado (porta ou catraca) e comandar a liberação do dispositivo controlado. I/O - Sensor_Porta é de extrema importância para garantir a integridade do ambiente controlado. Eventualmente, se uma porta for aberta sem um registro de autenticação, a unidade de controle irá acionar a I/O - Alarme para que a equipe de gerência possa tomar as medidas cabíveis.

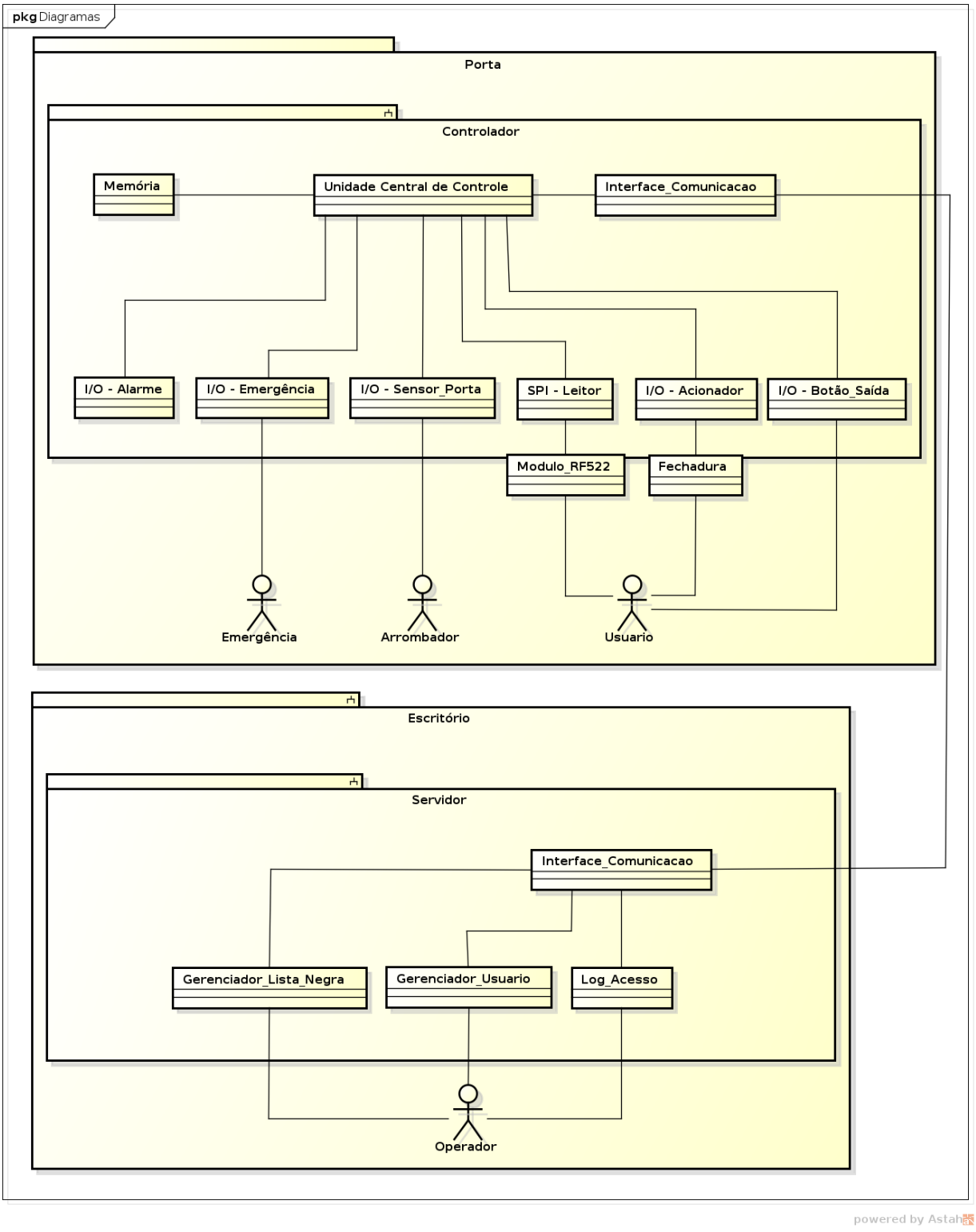

Figura 3.3: Modelo de Domínio.

No servidor roda uma interface de comando, permitindo a atualização da unidade de controle, gravar as permissões de acesso na *tag*, atualização da lista negra e visualização dos registos de acesso.

3.5 Casos de Uso

Nesta sessão são descritas as operações que o sistema realiza, como cadastro de dispositivos, cadastro de usuário, liberação de acesso entre outras funcionalidades.

Identificação do usuário

O usuário aproximará o cartão da unidade de leitura. Deste modo serão lidas as informações armazenadas na *tag* e processadas. Será constatado que a credencial identificada possui ou não a autorização de acesso, a unidade de controle envia a mensagem de acionamento (liberar ou negar) para a I/O - Acionamento. Em seguida, a unidade de controle realizará o registro do resultado da solicitação de acesso na memória do controlador de acesso.

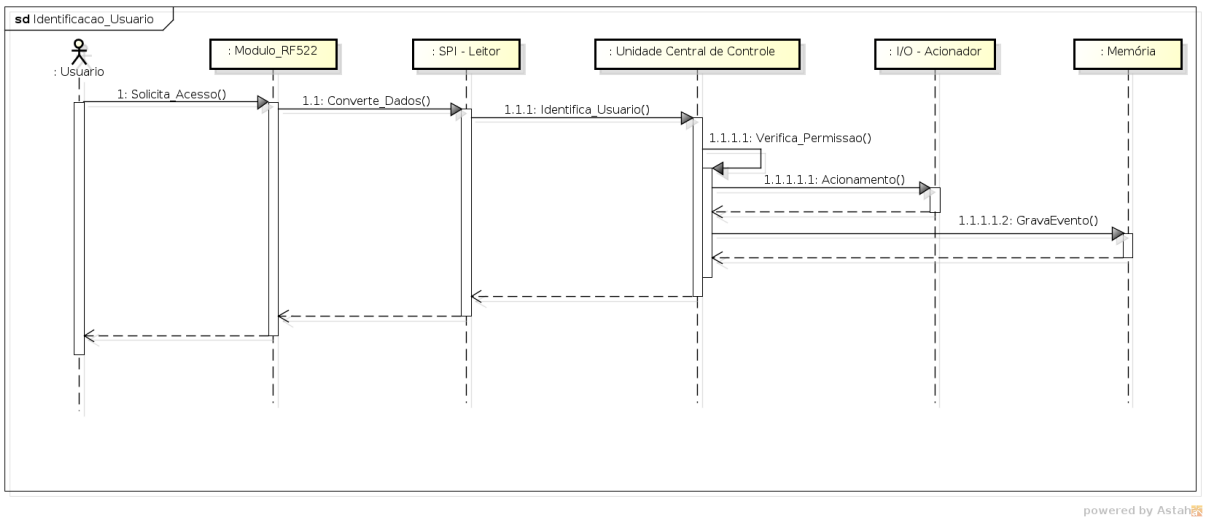

Figura 3.4: Identificação do Usuário.

Botão de Saída

Quando acionada a I/O - Acionador a unidade de controle irá enviar a mensagem de abertura para a I/O - Acionamento, de modo a permitir o livre acesso do usuário por um tempo padrão de dois segundos. Em seguida será registrado na memória a liberação do acesso.

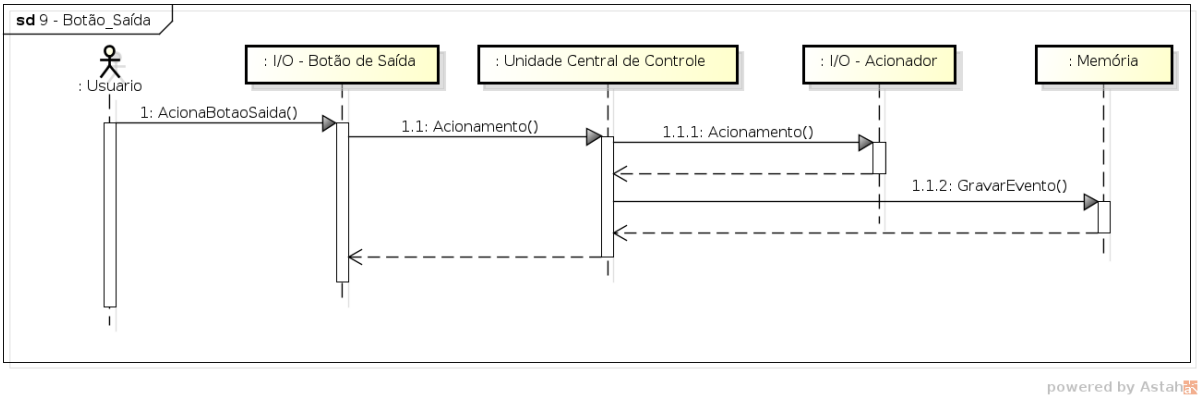

Figura 3.5: Botão de Saída.

Acionamento da emergência

Quando acionada a I/O - Emergência a unidade de controle irá enviar a mensagem de abertura para a I/O - Acionamento, de modo a permitir o livre acesso dos usuários. Em seguida será registrado na memória a liberação do acesso.

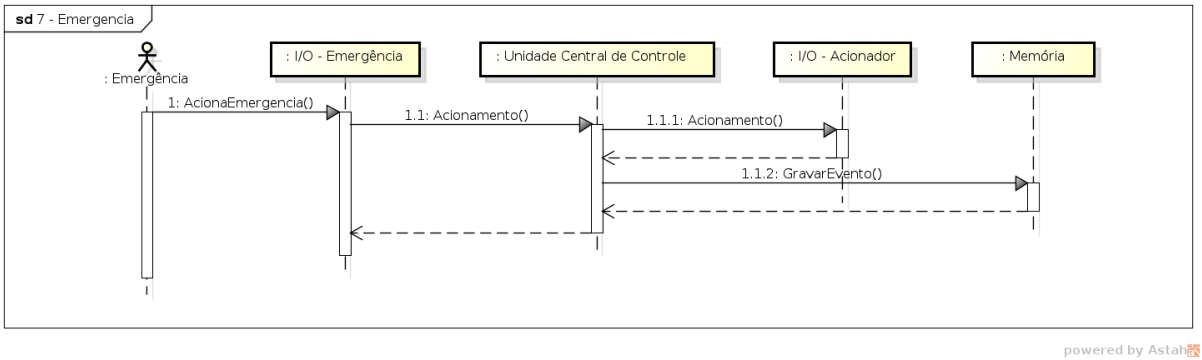

Figura 3.6: Acionamento de Emergência.

Abertura forçada

O arrombador irá acionar a I/O - Sensor, a unidade de controle consultará seus registros de modo a identificar se houve a autenticação de um usuário. Caso não tenha ocorrido uma liberação a unidade de controle deverá acionar a I/O - Alarme indicando que houve uma abertura forçada do ambiente e realizar o registro na memória.

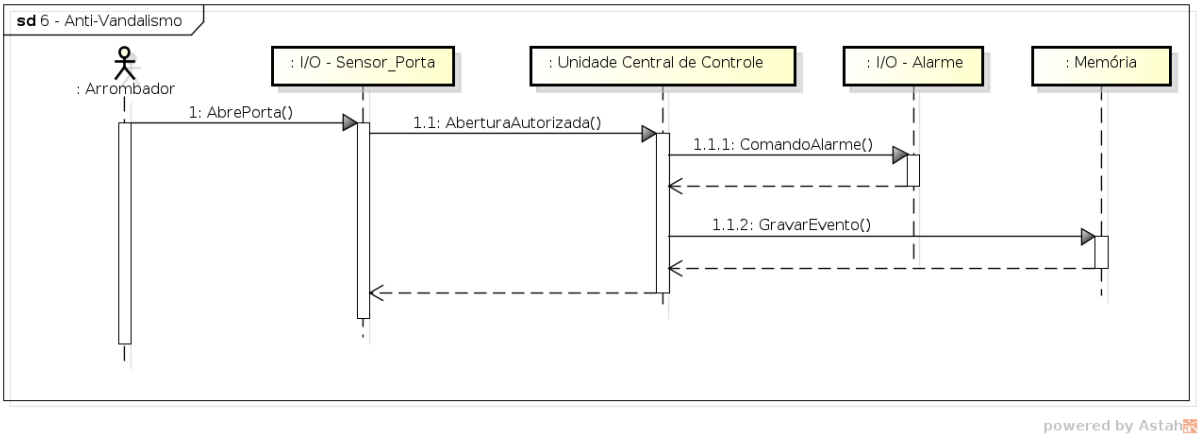

Figura 3.7: Abertura Forçada da Porta.

3.6 Fechamento

Este capítulo apresentou a proposta do sistema. Foram definidos os requisitos funcionais e não funcionais, relevantes para a implementação de um sistema de controle de acesso patrimonial. Foi apresentada a modelagem do sistema demostrando uma visão geral, sendo apresentados os casos de uso do sistema. A partir das definições macro do sistema, foi realizada à implementação, que é apresentada no capítulo seguinte como um protótipo funcional, detalhando questões técnicas quanto ao funcionamento do sistema.

4 *Implementação do Sistema*

Este capítulo tem por objetivo apresentar o desenvolvimento do trabalho. São apresentadas as características técnicas da implementação, dificuldades encontradas e soluções aplicadas. É realizada uma análise confrontando os casos de uso e requisitos com o que foi desenvolvido para validar a implementação.

4.1 Hardware do Controlador de Acesso

Conforme apresentado na seção 2.4, o sistema foi desenvolvido utilizando o RASPBERRYPI. Foram utilizadas as interfaces *ethernet* para comunicação com a rede de dados, a *Serial Peripheral Interface* (SPI) para a comunicação com o módulo MFRC522 e as *general purpose input/output* (GPIO) para as entradas e saídas de comandos, conforme apresentado na figura 4.1

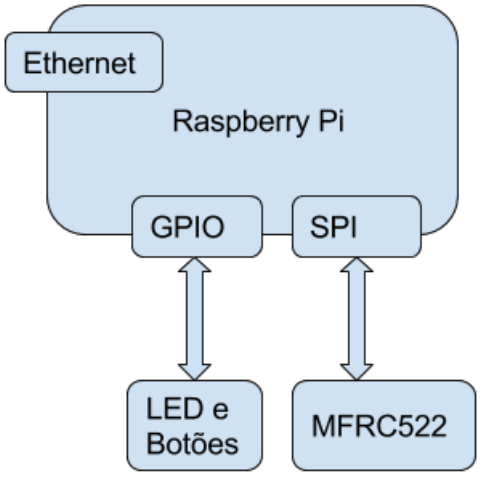

Figura 4.1: Diagrama de Bloco do Controlador de Acesso.

4.2 Software do Controlador de Acesso

Nesta seção estão descritas as características de funcionamento do sistema, no qual o software implementado e embarcado no RASPBERRYPI é responsável pelo funcionamento do controlador de acesso. O sistema foi modelado conforme apresentado nas figurar 4.3, 4.4 e 4.4.

4.2.1 Banco de Dados

Conforme especificado nos requisitos funcionais descrito na seção 3.3 o dispositivo possui um banco de dados SQLITE, nele são armazenadas algumas informações importantes para o funcionamento do sistema e segurança dos ambientes controlados. A figura 4.2 demostra as tabelas do banco de dados embarcado no dispositivo. Na tabela Dispositivo, são armazenadas características e informações do dispositivo, na tabela LogAcesso, são armazenados os registros de acesso atendendo a especificação do RF8 e na tabela ListaNegra, são armazenados os UID das *tag* que não devem ter acesso, contemplando os especificações descritas nos requisitos RF3 e RF5. A tabela ListaNegra, será utilizada também no caso de um usuário perder a *tag*. Como os dados estão gravados nela, essa é uma saída para evitar que seja usada indevidamente por outros usuários.

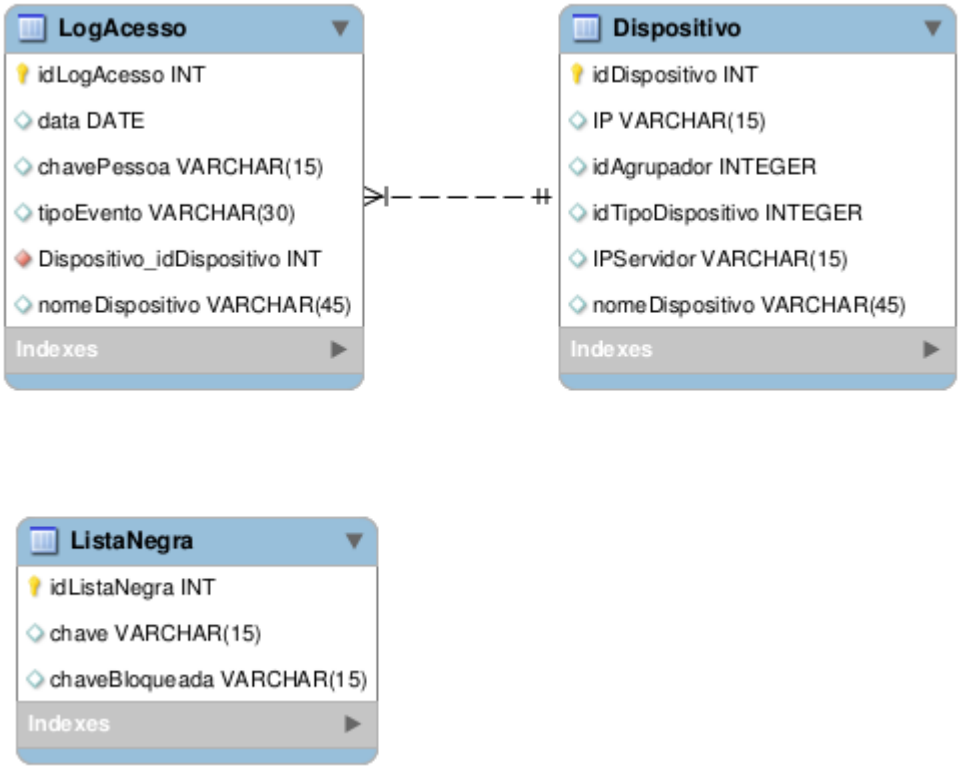

Figura 4.2: Diagrama do Banco de Dados do Dispositivo.

A figura 4.3 apresenta o diagrama das classes do banco de dados, permitindo a conexão e operações em cada uma das tabelas.

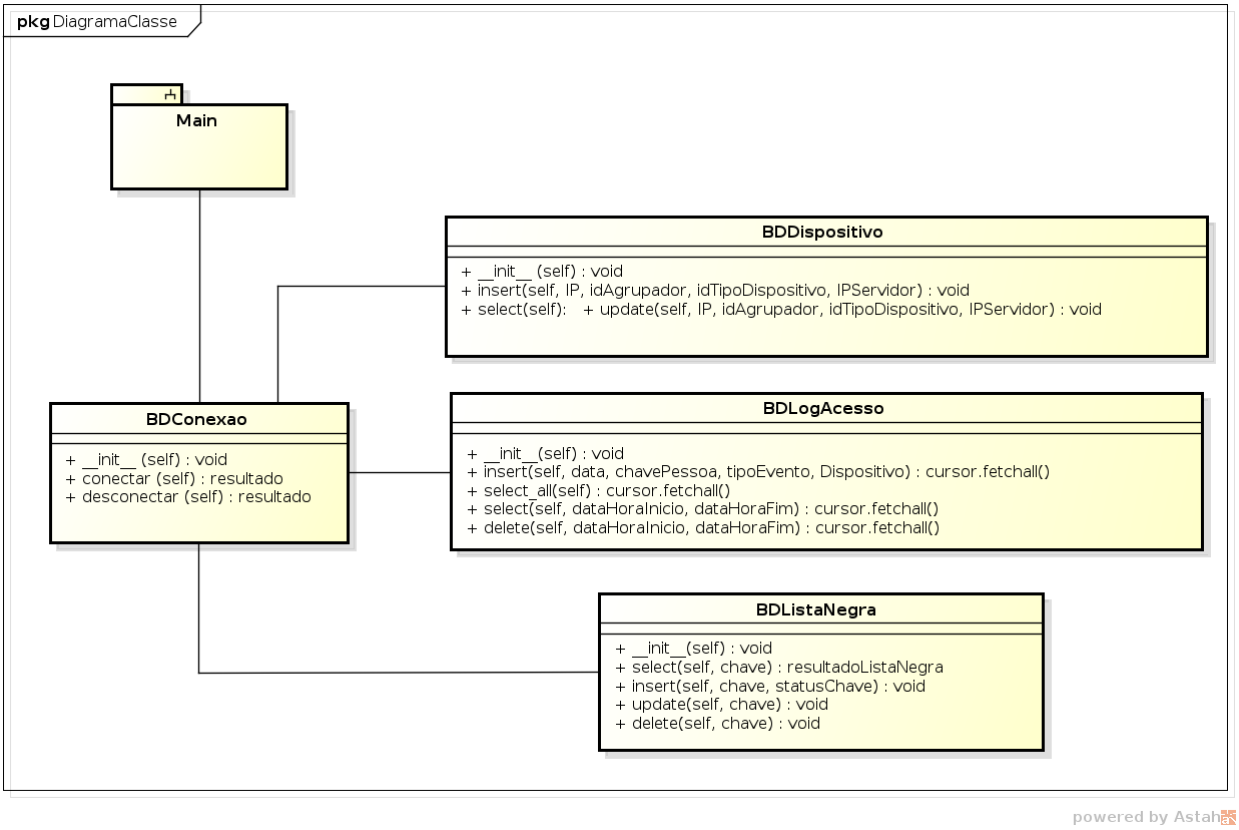

Figura 4.3: Diagrama das Classes do banco de dados.

4.2.2 I/O do sistema

O controlador de acesso desenvolvido possui algumas entradas e saídas de comando, destinadas ao controle e segurança dos ambientes. Quando uma entrada é acionada o sistema realiza o acionamento da saída adequada, a seguir serão apresentadas cada uma das entradas e saídas do sistema. A figura 4.4 apresentado o diagrama das classes criado para a manipulação da GPIO do sistema.

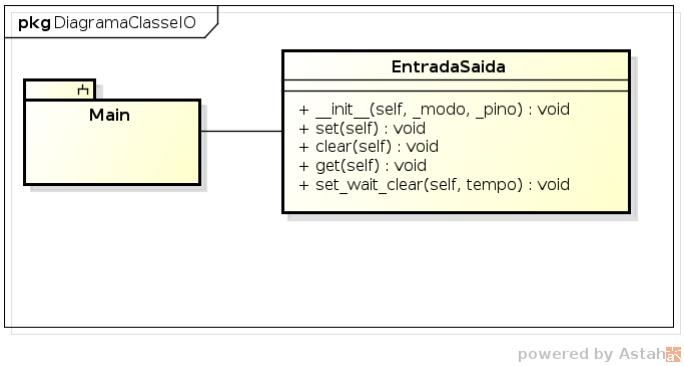

Figura 4.4: Diagrama das Classes das Entradas e Saídas

As tabelas 4.1 e 4.2 apresentam a lista dos componentes utilizados como referencia para montagem do circuito de acionamento das entradas e saídas do sistema.

Componentes Entrada de Acionamento	
Item	**Descrição**
I/O - Emergência	Botão NA (Normalmente Aberto)
I/O - Sensor_Porta	Botão NF (Normalmente Fechado)
I/O - Botão_Saída	Botão NA (Normalmente Aberto)

Tabela 4.1: Lista de Componentes Utilizados nas Entradas de Acionamento do Sistema.

Componentes Saída de Acionamento	
Item	**Descrição**
R1	Resistor 2.2 $K\Omega$
Q1	Transistor BC548
D1	Diodo 1N4148
Relé	Relé SRD-05VCD-SL-C

Tabela 4.2: Lista de Componentes para Acionamento das Saídas do Sistema.

Estão disponíveis duas saídas destinadas para acionamento de equipamento interligados ao sistema de controle de acesso. A I/O - Acionador é destinado para comandar a abertura e fechamento da porta, sendo ligada a um relé conforme apresentado na figura 4.5, chaveando a fonte de energia da fechadura. A I/O - Alarme é usada em casos de emergência, acionando um sistema de segurança supervisório.

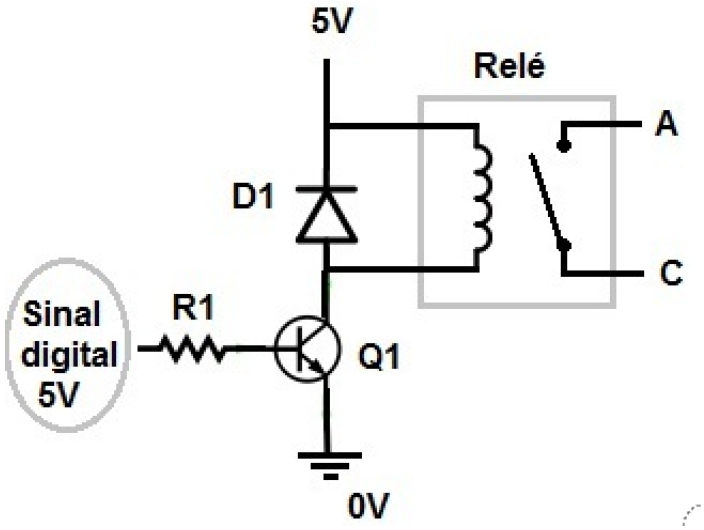

Figura 4.5: Circuito do Rele.

O sistema possui a entrada I/O - Botão_Saída que é destinado à liberação interna da porta. Quando acionada, registra um evento no banco de dados do dispositivo e aciona a I/O - Acionador, destravando a porta. Na figura 4.6 é apresentado o registro deste evento, com o número de identificação do evento, data e hora da liberação do acesso, código da chave padrão do sistema, tipo do evento e o nome do dispositivo.

```
1676|2016-03-08 01:02:09.079865|000000|Abertura Botao de Saida.|Porta Principal
1677|2016-03-08 01:14:21.160330|000000|Abertura Botao de Saida.|Porta Principal
```

Figura 4.6: Evento Abertura Botão de Saída.

Conforme o RF10, quando acionada a I/O - Emergência disponível no controlador de acesso será realizada a abertura da porta e acionamento da saída de alarme. Também serão registrados no banco de dados os eventos de liberação e acionamento de emergência, conforme apresentado na figura 4.7. O sistema mantém as saídas Alarme e Acionamento acionadas até que seja efetuada uma liberação de acesso, podendo ser com o botão de saída ou com a autenticação de um usuário por RFID.

```
1812|2016-03-08 18:51:58.439071|000000|Entrada Emergencia Acionado|Porta Principal
1813|2016-03-08 18:51:58.481151|000000|Saida de Alarme Acionado.|Porta Principal
1814|2016-03-08 18:51:58.517771|000000|Porta Destravada|Porta Principal
```

Figura 4.7: Evento de Abertura de Emergência.

A I/O - Sensor_Porta é utilizada para monitoramento do estado da porta. Quando acionado, o sistema interpreta como uma abertura forçada. O sistema irá acionar saída de alarme e registrar os eventos no banco de dados. Conforme a figura 4.8, serão registrados os eventos de Porta

Arrombada e Saída de Alarme Acionada. Esta funcionalidade atende parcialmente ao RF7, que solicitava que fosse possível identificar quando a porta foi aberta e fechada.

```
1819|2016-03-08 18:53:59.034432|000000|Porta Arrombada.|Porta Principal
1820|2016-03-08 18:53:59.079976|000000|Saida de Alarme Acionado.|Porta Principal
```

Figura 4.8: Evento de Abertura Forçada.

4.2.3 Configurações Remotas do Sistema

O sistema foi desenvolvido com possibilidade de realizar algumas configurações remotamente. Para efetuar as configurações foi desenvolvida uma interface de comando, conforme apresentada no figura 4.9.

```
 SocketCliente -- Selecione uma opção.
0 - Encerrar conexão.
1 - Config. Dispositivo.
2 - Inserir cartão na ListaNegra.
3 - Remover cartão da listaNegra.
4 - Obter LogAcesso.
5 - Gravar permissão de acesso.
Insira o número correspondente a operação desejada:
```

Figura 4.9: Interface de Configurações Remotas.

Permitindo realizar as definições básicas para do funcionamento do dispositivo, como o tipo de dispositivo definindo ele como catraca ou porta. Também são configurados os agrupadores, são identificadores dos dispositivos, de modo que dispositivos que controlem os acessos aos mesmos ambientes podem ser identificados com o mesmo agrupador, visto que a permissão do acesso do usuários é para o ambiente e não ao dispositivos em si.

Com o sistema em funcionamento, outras operações são importantes para o gerenciamento do sistema e podem ser realizadas pela interface de configurações remota. O dispositivo possui um banco de dados permitindo inserir e remover chaves da lista negra, que serão consultadas ao longo do processo de validação de uma RFID o qual é apresentado na subseção 4.2.5.

Para que uma *tag* RFID tenha acesso também é necessário que ela possua uma permissão ativa e válida. A definição dessas informações será realizada remotamente com o auxilio da interface de configurações. Na subseção 4.2.4 são apresentados com detalhes como os dados são armazenados na memória da *tag*.

Para a realização de auditoria do sistema é possível visualizar remotamente os registros de acesso que encontram-se no banco de dados, conforme apresentado na figura 4.10.

```
1828|2016-03-08 21:29:16.515923|000000|Entrada Emergencia Acionado|Porta Principal
1829|2016-03-08 21:29:16.514988|000000|Entrada Emergencia Acionado|Porta Principal
1830|2016-03-08 21:29:16.601569|000000|Saida de Alarme Acionado.|Porta Principal
1831|2016-03-08 21:29:16.637350|000000|Porta Destravada|Porta Principal
1832|2016-03-08 21:29:47.524306|1895616021|Acesso Negado Cartao MIFARE.|Porta Principal
1833|2016-03-08 21:29:56.692891|1412718521|Abertura Cartao MIFARE.|Porta Principal
1834|2016-03-15 01:06:53.169840|000000|Abertura Botao de Saida.|Porta Principal
1835|2016-03-15 01:07:53.139690|000000|Entrada Emergencia Acionado|Porta Principal
1836|2016-03-15 01:07:53.173739|000000|Saida de Alarme Acionado.|Porta Principal
1837|2016-03-15 01:07:54.174247|000000|Porta Destravada|Porta Principal
1838|2016-03-15 01:07:57.220833|000000|Entrada Emergencia Acionado|Porta Principal
1839|2016-03-15 01:07:57.255400|000000|Saida de Alarme Acionado.|Porta Principal
1840|2016-03-15 01:07:57.298197|000000|Porta Destravada|Porta Principal
1841|2016-03-15 01:07:59.985734|000000|Porta Arrombada.|Porta Principal
1842|2016-03-15 01:08:00.059134|000000|Saida de Alarme Acionado.|Porta Principal
1843|2016-03-15 01:08:04.378349|000000|Abertura Botao de Saida.|Porta Principal
1844|2016-03-15 01:08:05.042565|000000|Abertura Botao de Saida.|Porta Principal
1845|2016-03-15 01:08:19.074193|64831951|Negado, usuario da Lista Negra|Porta Principal
1846|2016-03-15 01:08:26.957471|1412718521|Abertura Cartao MIFARE.|Porta Principal
1847|2016-03-15 01:08:34.877761|1895616021|Acesso Negado Cartao MIFARE.|Porta Principal
1848|2016-03-15 01:08:41.136834|14116217421|Acesso Negado Cartao MIFARE.|Porta Principal
```

Figura 4.10: Visualização do Log de Acesso Remotamente.

A figura 4.11 apresentado o diagrama das classes e seus métodos implementado para realização operações solicitadas pelo cliente.

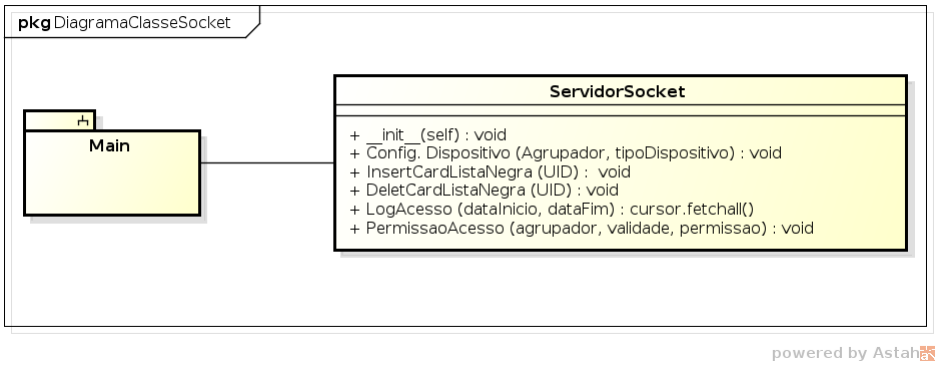

Figura 4.11: Diagrama da Classe da Conexão Socket.

4.2.4 Gravação das Permissões de Acesso na *tag*

A permissão de acesso dos usuários é gravada na memória da *tag*. No setor 0, os blocos 1 e 2 são reservados para armazenamento de informações do usuário. No bloco 1 os *bytes* 0, 1 e 2 são usados para o armazenamento a validade das permissões gravadas na *tag*. Na sequência, o *byte* 3 define o nível de permissão do usuário, podendo ser supervisor ou usuário comum. Nos demais setores serão armazenadas as permissões de acesso para cada um dos 34 agrupadores.

Para cada agrupador são utilizados 21 *bytes*, sendo que cada 3 bytes representam um dia da semana iniciando por segunda-feira. Cada *bit* dos 3 *bytes* representam uma hora do dia. Na tabela 4.3 é apresentado a permissão de um dia da semana, com liberação das 8:00 até as 17:59.

Faixa de horário e permissões																								
	Byte 1								*Byte 2*								*Byte 3*							
Horário	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	23	22	21	20	19	18	17	16
Permissão	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1

Tabela 4.3: Tabela demostração da memória da *tag* da um dia.

Na tabela 4.4 é apresentado em decimal a permissão de acesso de um usuário que possui acesso das 8:00 até as 17:59 de segunda-feira até sexta-feira.

Faixa de horário e permissões em *byte*																					
	Segunda			Terça			Quarta			Quinta			Sexta			Sábado			Domingo		
Byte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Permissão	0	255	3	0	255	3	0	255	3	0	255	3	0	255	3	0	0	0	0	0	0

Tabela 4.4: Tabela demostração da memória da *tag* de um agrupador.

A classe MFRC522 integra uma biblioteca disponibilizada publicamente (GóMEZ, 2014). A Figura 4.12 apresenta os principais métodos utilizados desta classe, sendo estes abstraídos pela classe RFID. A classe RFID apresenta as operações específicas utilizadas pelo sistema, proporcionando isolamento e facilitando a adaptação do sistema para emprego de outros modelos de leitoras.

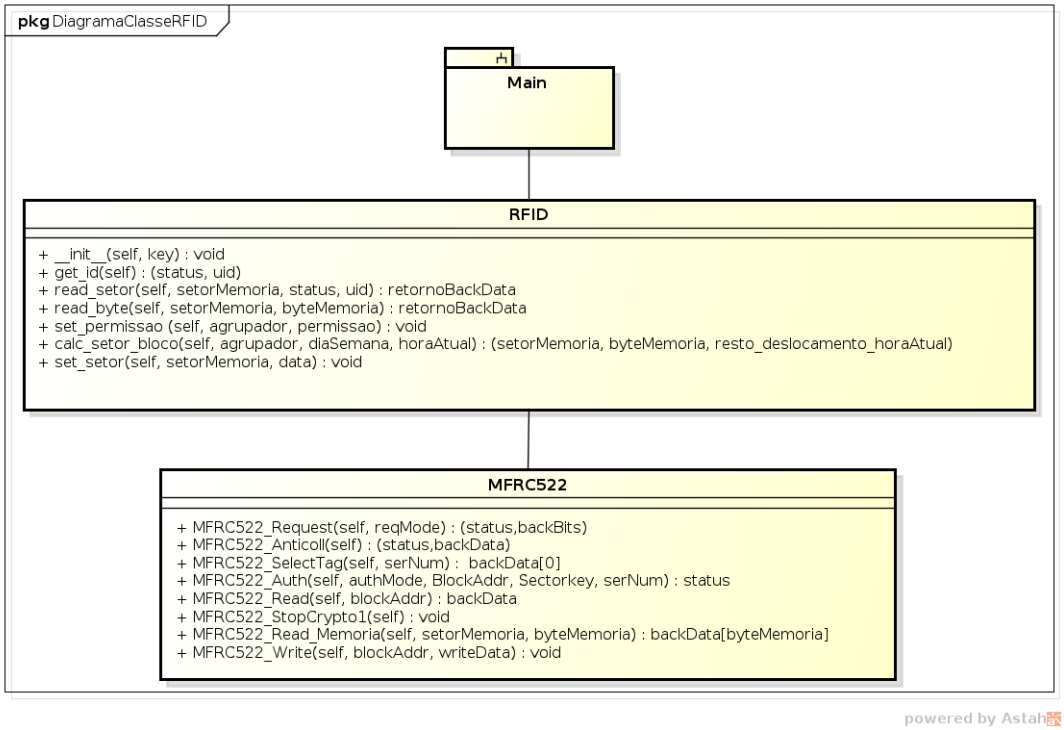

Figura 4.12: Diagrama de Classe RFID.

4.2.5 Mecanismo de Validação do Acesso por *tag*

Conforme apresentado ao longo do trabalho, o sistema realiza a validação das permissões de acesso consultando a memória da *tag*. Na figura 4.13 está representado o fluxo do processo de validação da permissão.

Para realizar o processo de validação da permissão de acesso, o sistema calcula com base no horário e agrupador qual é o setor, bloco e byte que está armazenada a permissão do usuário para aquele instante. Na sequencia o sistema aguarda o usuário aproximar a *tag* para iniciar a leitura dos dados.

Quando o sistema detecta a *tag* é iniciado o processo para identificação do *Unique IDentifier* (UID) seguido pela leitura do *byte* correspondente à permissão desejada e validade das permissões, neste processo o sistema tentará até 3 vezes realizar a leitura de cada uma das duas informações.

Após obter as informações necessárias para a validação do acesso, o sistema realizará os procedimentos de validação, iniciando com a verificação do UID na lista negra. Quando não encontrado o sistema continua os procedimentos, seguindo com a verificação da permissão e validade. Quando atendido, o sistema registra o evento de acesso liberado e realiza a abertura da porta.

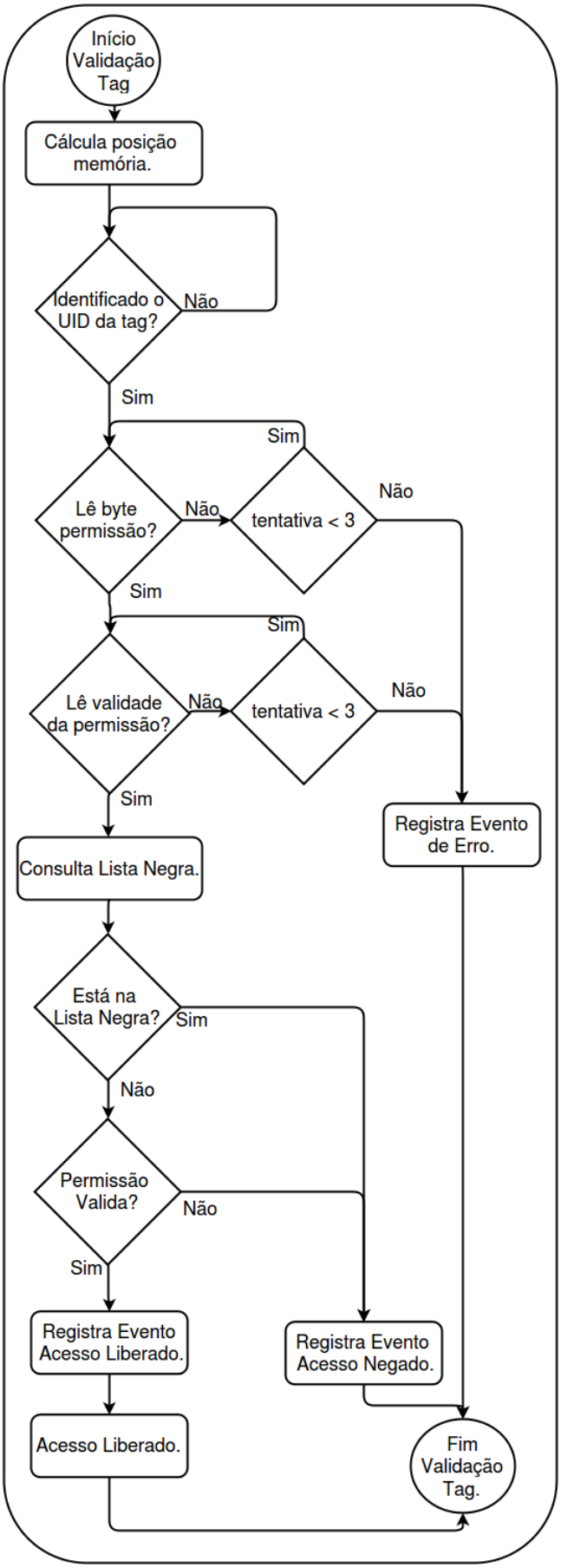

Figura 4.13: Validação Permissão de Acesso do Usuário.

5 *Conclusão*

Este trabalho apresentou a implementação de um sistema de controle de acesso por RFID, tendo como foco a identificação das permissões de acesso a partir da leitura dos dados armazenados na memória da *tag* RFID e registrando o log de todos os acessos em banco de dados.

Ao longo do desenvolvimento do sistema foi possível alcançar a validação das funcionalidades, atingindo os objetivos propostos. O controlador de acesso permite o gerenciamento de um ambiente, proporcionando que os usuários realizem o acesso utilizando uma *tag* RFID, a validação do acesso é realizada a partir da leitura dos dados armazenados em sua memória. Quando é realizado a identificação de uma *tag* ou efetuado um acionamento no dispositivo esses eventos são registrados em banco de dados.

São sugestões para trabalhos futuros os seguintes temas não abordados por este:

1. Implementação de um software para gerenciamento dos dados, permitindo o gerenciamento de vário dispositivos;
2. Desenvolvimento de uma biblioteca de integração entre a unidade de controle e o software de gerenciamento;
3. Implementação de um sistema com um módulo RFID compatível com outras versões do MIFARE e NFC;
4. Realização de testes de desempenho;

Referências Bibliográficas

INTERMEC. *Fundamentos da RFID: Entendendo e usando a identificação por radiofrequência*. [S.l.], 2007. Último acesso em 23 de junho de 2015.

FINKENZELLER, K.; MÜLLER, D. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Wiley, 2010. ISBN 9781119991878. Disponível em: <https://books.google.com.br/books?id=jAszZEQYa9wC>.

NXP. *MFRC522 Standard 3V MIFARE reader solution*. 2014. `http://www.nxp.com/documents/data_sheet/MFRC522.pdf`. Último acesso em 25 de janeiro de 2016.

NXP. *MIFARE Classic 1K - Mainstream contactless smart card IC for fast and easy solution development*. 2011. `http://www.nxp.com/documents/data_sheet/MF1S50YYX_V1.pdf`. Último acesso em 26 de janeiro de 2016.

SOUZA, W. B. de. *Cartão MIFARE classic ataques e medidas de contorno*. Dissertação (Mestrado) — Universidade de São Paulo, 2011.

FUNDATION RASPBERRY PI. *Raspberry Pi*. 2016. `https://www.raspberrypi.org/products/model-b-plus/`. Último acesso em 27 de janeiro de 2016.

OLIVEIRA, A. de S.; PEREIRA, M. F. *Estudo da tecnologia de identificação por radiofrequência - RFID*. 2006.

THOMÉ, M. L. et al. *Controle de acesso físico nas empresas*. 2012.

WIKIPEDIA. *Controle de Acesso — Wikipédia, a enciclopédia livre*. 2015. `https://pt.wikipedia.org/wiki/Controle_de_acesso`. Último acesso em 25 de maio de 2015.

GOMES, H. M. C. *Construção de um sistema de RFID com fins de localização especiais*. Dissertação (Mestrado) — Universidade de Aveiro, 2007.

ROBERTI, M. *The history of RFID technology*. 2005. `http://www.rfidjournal.com/articles/view?1338/`.

MICROCHIP. *microID®125 kHz RFID System Design Guide*. [S.l.], 2004. Último acesso em 23 de junho de 2015.

CARRIJO, G. D. *Estudo de antenas para etiquetas do sistema de identificação por radiofrequência*. 2009.

ANATEL. *Republica o regulamento sobre equipamentos de radiocomunicação de radiação restrita.* [S.l.], 2008. Último acesso em 20 de junho de 2015.

REZENDE, P. A. D. *Criptografia e segurança na informática*. 2011.

PINTO, F.; ANTUNES, J.; SANTOS, L. *Estudo teórico sobre a segurança em sistemas RFID*. 2011.

BORGES, L. E. *Python para Desenvolvedores*. Wiley, 2010. ISBN 978-85-909451-1-6. Disponível em: <https://ark4n.files.wordpress.com/2010/01/python_para_desenvolvedores_2ed.pdf>.

SQLITE. *About SQLite*. 2016. `http://www.sqlite.org/about.html`. Último acesso em 27 de janeiro de 2016.

GóMEZ, M. *MFRC522-python*. 2014. Disponível em: <https://github.com/mxgxw/MFRC522-python>. Acesso em: 01/12/2015.