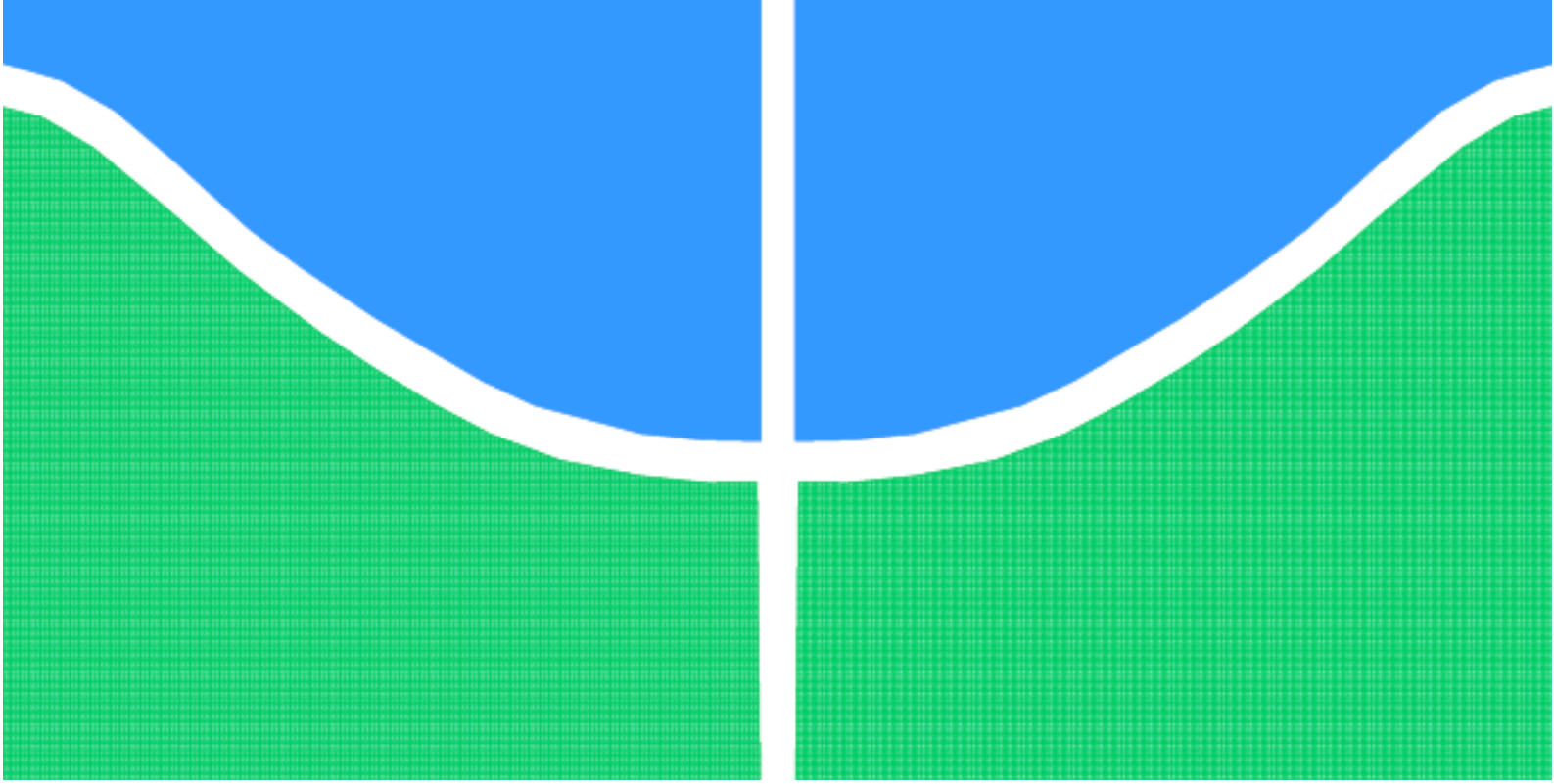

PROJETO DE GRADUAÇÃO

RFID – Identificação por radiofreqüência movendo-se para o futuro

Por

Caio Santi Passaretti

Brasília, 10 de junho de 2008

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

PROJETO DE GRADUAÇÃO

RFID – Identificação por radiofreqüência movendo-se para o futuro

Por
Caio Santi Passaretti

Monografia de graduação submetida ao Departamento de Engenharia Elétrica da Faculdade de Tecnologia da Universidade de Brasília, como requisito parcial para obtenção do grau de Engenheiro Eletricista.

Banca Examinadora

Marco Antonio Brasil Terada (Orientador) _____

Antonio José Martins Soares _____

Franklin da Costa Silva _____

Brasília, 10 de junho de 2008

Dedicatória

Ao meu pai Sérgio, minha mãe Marlinda e minha irmã Kim, que sempre estiveram ao meu lado, me apoiando e me incentivando em todos os momentos.

Agradecimentos

Agradeço a toda minha família, que tanto me apóia, me estimula a crescer como profissional e como pessoa e que me oferece condições para que eu alcance meus objetivos; aos Srs. Vicente Shinoda e Ricardo Catón que, com todo conhecimento que possuem acerca do assunto deste trabalho, colaboraram com muitas informações importantes; ao Dr. Dilno Pereira Lopes – Diretor da Diretoria de Telecomunicações – DITEL - do Gabinete Civil da Presidência da República, que viabilizou a elaboração do presente trabalho quando possibilitou o acesso às informações do Projeto implantado naquelas instalações; ao Bruno, com quem sempre pude contar, sendo sempre muito prestativo e provando que a distância não desfaz uma verdadeira amizade; aos demais amigos, que tantas experiências boas me proporcionaram ao longo da vida acadêmica; e aos professores que me deram conhecimentos necessários para a realização deste trabalho.

RESUMO

Este trabalho apresenta um estudo da tecnologia de RFID (Identificação por radiofreqüência) através de uma abordagem mais sistêmica e prática, na qual o sistema é discutido a nível de arquitetura, de componentes, tais como tags, leitores e servidores, padronizações e aplicabilidade. Também há um estudo aprofundado dos *smart cards*, sendo demonstradas descrições e comparações entre seus tipos. Da mesma forma, é apresentado um estudo dos desafios a serem transpostos para que a tecnologia evolua do estágio atual. O trabalho é complementado com um estudo de caso, onde é analisada a aplicação do RFID na Presidência da República Federativa do Brasil.

ABSTRACT

This work shows a systemic and practical study of RFID (Radiofrequency identification) technology, in which the system is discussed in architecture, components (like tags, readers and servers), standardizations and applications level. It has also a deep study about smart cards, being demonstrated features and comparisons between the types. In addiction, it is showed a study about the RFID technology future. The work is complemented with a case study, where is analyzed the RFID application at the Presidência da República Federativa do Brasil.

Índice

Índice de Ilustrações

Lista de Abreviaturas e Siglas

3DES – Triple Data Encryption Standard
AAR – Association of American Railroads
AES – Advanced Encryption Standard
AIDC – Automatic Identification and Data Capture
ALE – Acquisition Logistics Engineering
ANATEL – Agência Nacional de Telecomunicações
API – Application Programming Interface
Auto-ID – Automatic Identification
CCD – Charge-Coupled Device
CEN – European Committee for Standardization
CEPT – European Conference of Postal and Telecommunications Administrations
CFTV – Circuito Fechado de Televisão
CHCP – Cargo Handling Cooperative Program
CNH – Carteira Nacional de Habilitação
COSIPA – Companhia Siderúrgica Paulista
CSN – Companhia Siderúrgica Nacional
DITEL – Diretoria de Telecomunicações
DoD – United States Department of Defense
EAI – Enterprise Application Integration
EAN – European Article Number
EAS – Electronic Article Surveillance
EEPROM - Electrically-Erasable Programmable Read-Only Memory
EPC – Electronic Product Code
ERO – European Radiocommunications Office
ETSI – European Telecommunications Standards Institute
FAAP – Fundação Armando Álvares Penteado
FCC – Federal Communications Commission
HF – High Frequency
IEC – International Electrotechnical Commission
IFF – Identifier Friend or Foe
ISBN – International Standard Book Number
ISM – Industry, Scientific and Medical Radio Bands
ISO – International Organization for Standardization
ITU – International Telecommunication Union
LASL – Los Alamos Scientific Laboratory
LF – Low Frequency
MAPA – Ministério da Agricultura, Pecuária e Abastecimento
MCAS – Módulo de Controle de Acesso
MCFTV – Módulo de Circuito Fechado de Televisão
MIT – Massachusetts Institute of Technology
MPHPT – Ministry of Public Management, Home Affairs, Posts and Telecommunications
NPU – Numerical Processor Unit
OFTA – Office of the Telecommunications Authority
ONS – Object Name Service

PC – Personal Computer
PLC – Programmable Logic Controller
PML – Product Markup Language
RAM – Random Access Memory
RF – Radio Frequency
RFID – Radio Frequency Identification
RO – Read Only
ROM – Read Only Memory
RTLS – Real Time Location System
RW – Re-Writable
SAC – Standardization Administration of China
SINIAV – Sistema Nacional de Identificação Automática de Veículos
SIS – Sistema Integrado de Supervisão
SISBOV – Sistema Brasileiro de Identificação e Certificação de Origem Bovina e Bubalina
SOA – Service-Oriented Architecture
TI – Tecnologia da Informação
USB – Universal Serial Bus
UHF – Ultra High Frequency
UnB – Universidade de Brasília
U.S.FDA – United States Food and Drug Administration
USFHA – United States Federal Highway Administration
UPC – Universal Product Code
UPCC – Uniform Product Code Council
WLAN – Wireless Local Area Network
WORM – Write Once Read Many

CAPÍTULO 1

Introdução

1.1 Objetivo do estudo da tecnologia

O objetivo do estudo dos sistemas de RFID é elucidar a visão da importância dessa tecnologia hoje e nos próximos anos. Tendo em vista a agilidade, a segurança e os benefícios que podem ser obtidos, o uso do RFID tende a ser mundialmente expandido. Se for levada em consideração a aplicabilidade da tecnologia na vida cotidiana, verificar-se-á que praticamente tudo poderá ser facilitado com seu uso, como, por exemplo, o RFID substituindo as chaves de casa, do carro, do escritório, o controle remoto do portão da garagem, extinguindo a necessidade de parar na cabine de pedágio, auxiliando no controle da quantidade e da validade de produtos na despensa, ou na geladeira, elaborando e enviando, automaticamente, a lista de compras ao supermercado, assim que algum produto é retirado de um armário ou prateleira de casa, dentre várias outras facilidades. Tamanhas são as vantagens trazidas pelo o RFID, que grandes *players* do mercado, como *Wal-Mart*, *DoD* (*U.S. Department of Defense*), *U.S. FDA* (*Food and Drug Administration*), e outros, estão adotando essa tecnologia, fazendo com que ela se mantenha muito distante da obsolescência, sendo constantemente atualizada e desenvolvida.

1.2 Estrutura do trabalho

O presente trabalho apresenta, inicialmente, um histórico da tecnologia de RFID, bem como sua evolução ao longo dos anos. Em seguida é detalhada a arquitetura e os componentes do sistema, tais como tags, leitores, *middleware* e software de aplicação, as freqüências de operação, as padronizações existentes para o RFID e é feita uma comparação com outro sistema de identificação: o Barcode, ou código de barras.

No capítulo 6 é realizada uma análise de algumas das diversas aplicações onde o uso do RFID se traduz em grandes vantagens, como no transporte urbano, na cadeia de suprimentos, na segurança, no monitoramento animal, na automação de bibliotecas e nos sistemas de pedágio.

O capítulo 7 descreve os smart cards a nível de características, classificação e aplicações.

No capítulo 8 é apresentado um estudo de caso, da aplicação do RFID na Presidência da República Federativa do Brasil.

Por fim, nos capítulos 9 e 10 são apresentados os desafios para o sucesso do RFID no mundo e a conclusão do trabalho, contendo a opinião do autor sobre uma visão de futuro da tecnologia.

CAPÍTULO 2

História do RFID

2.1 Histórico

O surgimento da tecnologia da identificação por rádio freqüência remete à época da Segunda Guerra Mundial, onde alemães, japoneses, americanos e britânicos utilizavam radares para alertar suas bases da aproximação de aeronaves, enquanto estas estivessem a quilômetros de distância. O problema que eles encontravam era que não existiam métodos de identificar quais aviões eram do inimigo e quais eram de sua própria frota, que poderiam estar retornando de uma missão. Posteriormente, os alemães descobriram que se o piloto girasse seu avião quando retornasse à base, ele mudaria o sinal de rádio refletido, que fora emitido pelo equipamento de radar. Assim, este pode ser considerado como sendo o primeiro sistema de RFID passivo, pois se conseguia a identificação da aeronave (se alemã ou não) através de RF.

Posteriormente, o mesmo inventor do sistema de radar, Watson-Watt, participou de um projeto secreto, no qual desenvolveu o primeiro sistema de identificação ativo de aliado ou inimigo. A solução por ele encontrada foi colocar um transmissor em cada avião britânico. Quando os aviões recebiam os sinais das estações de radar no solo, distribuíam o sinal de retorno, o que identificava a aeronave como aliada. E este é o conceito básico de funcionamento de um sistema de RFID [1].

2.2 Evolução

Parte-se da época da Segunda Guerra Mundial, época na qual se considera que foi originada a tecnologia RFID. Os anos seguintes, da década de 50, foram marcados pela exploração das técnicas de RFID com sucessivos desenvolvimentos técnicos de rádio e radar. Alguns dos importantes artigos que foram publicados foram de F.L. Vernon's, "Applications of the Microwave Homodyne", e D.B. Harris's, "Radio Transmission Systems with Modulatable Passive Responders". Nessa época estavam sendo exploradas várias tecnologias relacionadas ao RFID. Um exemplo é o exército americano, que começara a implementar uma tecnologia de identificação de aeronaves por rádio-freqüência, chamada Identification Friend or Foe, ou IFF [2].

A década de 60 foi o prelúdio da explosão do RFID, que viria posteriormente, nos anos setenta. R.F. Harrington efetuou uma grande pesquisa no campo da teoria eletromagnética relacionada com o RFID e a descreveu em dois documentos denominados "Field Measurements Using Active Scatterers" e "Theory of Loaded Scatterers". Inventores e invenções no campo de RFID também começaram a surgir, como, por exemplo, as descobertas sobre ativação remota de dispositivos, publicadas por Robert Richardson's em "Remotely Activated Radio Frequency Powered Devices", o desenvolvimento das comunicações por antenas, publicadas por Otto Rittenback's em "Communication by Radar Beams", o aprofundamento das técnicas de transmissão de dados passiva, publicadas por J.H. Vogelman's em "Passive Data Transmission Techniques Utilizing Radar Beams" e as pesquisas de J.P. Vinding's sobre a comunicação entre dispositivos em um sistema de identificação, em "Interrogator-Responder Identification System". Algumas atividades comerciais também começaram

a surgir nessa década. As empresas Sensormatic e a Checkpoint foram fundadas para desenvolver equipamentos de segurança patrimonial eletrônica (EAS – Electronic Article Surveillance) para evitar roubos e para outras aplicações em segurança. Tais sistemas eram simples. Eram sistemas de 1-bit, ou seja, eles só poderiam detectar a presença de tags RFID, mas não identificá-los. Posteriormente o EAS se tornou a primeira aplicação comercializada em larga escala do RFID [2].

A década de 70 foi um período de intenso desenvolvimento na tecnologia de RFID. Empresas, inventores, universidades, fundações de pesquisa e laboratórios do governo estavam trabalhando ativamente na tecnologia de RFID. Com isso, pode-se notar perceptíveis avanços na tecnologia nesse período. Em 1975 o Los Alamos Scientific Laboratory (LASL) apresentou para a comunidade um importante estudo sobre RFID, intitulado "Short-Range Radio-Telemetry for Electronic Identification Using Modulated Backscatter", escrito por Alfred Koelle, Steven Depp e Robert Freyman. Grandes empresas como Raytheon, RCA e Fairchild começaram a desenvolver sistemas de identificação eletrônica também. Em 1978 era criado um transponder passivo que operava em freqüências de microondas. Este desenvolvimento sinalizou o começo prático do uso das etiquetas, completamente passivas e com amplitude operacional de até dez metros. No mesmo ano alguns órgãos governamentais começaram a demonstrar interesse na tecnologia também. As autoridades dos portos de New York e de New Jersey testaram sistemas construídos pela General Electric, Westinghouse, Philips e Glenayre e os resultados foram favoráveis. A Administração Federal de Rodovias dos Estados Unidos (USFHA) convocou uma conferência para discutir a possibilidade da tecnologia de identificação eletrônica em veículos e em aplicações de transporte também. Daí surgiu a primeira aplicação com sucesso para utilização no transporte comercial, que foi uma estação de pedágio, com restrições de uso nos horários de grandes movimentos. Uma grande quantidade de pequenas empresas focadas na tecnologia de RFID também começaram a surgir no fim dos anos 70. Nessa época, muitas das pesquisas em princípios eletrônicos e eletromagnéticos de ondas de rádio-freqüência foram finalizadas e pesquisas em tecnologia da informação, em computadores, fundamental para o desenvolvimento de clientes RFID, e redes haviam começado, como evidência da criação do PC e da ARPANET, que viria a se tornar a Internet [2][1].

A década de 80 foi marcada por várias implantações da tecnologia RFID. Ainda sem a definição dos padrões, é marcada por diferentes interesses em várias partes do mundo.

Na Europa os maiores interessados trabalharam em sistemas utilizando RFID no controle de animais (com alcance limitado) em diversas outras aplicações industriais e empresariais. Entretanto, teve destaque a aplicação da tecnologia de RFID no controle de passagens e praças de pedágio de estradas na Itália, França, Espanha, Portugal e Noruega.

Nos Estados Unidos, os maiores interessados nesta tecnologia desenvolveram aplicações para transportes, controle de acesso e, com menos ênfase, para o controle de animais. A Associação Americana de Ferrovias (AAR) e o Programa de Cooperativas de Manipulação de Containers (CHCP) se tornaram ativos nas iniciativas para o crescimento da tecnologia de RFID, com o objetivo de identificar vagões de trem por

RFID. As aplicações no setor de transporte começaram a crescer no fim da década de 80. A primeira aplicação no mundo foi implementada na Noruega, em 1987, seguido por Dallas, em 1989. As autoridades dos Portos de New York e de New Jersey implementaram um projeto para ônibus que transitavam no Túnel Lincoln. Todos os sistemas de RFID instalados na década de 80 eram sistemas proprietários. Não havia interoperabilidade entre eles e a pequena competição na indústria de RFID resultava na manutenção de altos custos, o que impedia uma maior expansão da indústria [2].

Os anos 90 foram extremamente significantes para a RFID, pois finalmente ela começou a se tornar uma aplicação importante no mundo dos negócios e da tecnologia. Em meados da década, os sistemas de RFID já podiam ser aplicados em rodovias de velocidade elevada, significando que motoristas poderiam passar pelos pedágios sem terem de parar. Isso fez com que sistemas de RFID em pedágios se tornassem amplamente utilizados nos Estados Unidos. Agências regionais de pedágio, utilizando a tecnologia RFID, começaram a integrar seus sistemas, habilitando os motoristas a pagar diversos pedágios, em diferentes rodovias, pontes e túneis com uma mesma conta. Tem-se como exemplos a E-Z Pass Interagency Group, localizada no nordeste dos Estados Unidos, um projeto na área de Houston, outro projeto interligando as praças de pedágio no Kansas e em Oklahoma, bem como um projeto na Georgia. Ainda na década de 90 a Texas Instruments criou um sistema chamado TIRIS. Esse sistema desenvolveu novas aplicações para o RFID tais como o pagamento de combustível, como o ExxonMobil's Speedpass, e sistemas de acesso de veículos. Nos anos 90 muitas empresas nos Estados Unidos e Europa se envolveram com o RFID, como Philips, MIkron, Alcatel e Bosch. A expansão dos PC's e da Internet deixou a indústria com somente o problema do custo elevado dos tags para superar, para tornar os sistemas RFID viáveis comercialmente. Mas avanços na tecnologia de materiais durante a década de 90, muitos deles relacionados com trabalhos de fabricantes de semicondutores como IBM, Intel, AMD e Motorola, finalmente elevaram a relação custo-benefício dos tags. Isso viabilizou a implantação de muitos projetos. Projetos que antes eram completamente inviáveis financeiramente se tornaram implantáveis. Testes em larga escala com "smart labels", ou etiquetas inteligentes, começaram no fim da década. Mas ainda havia um impeditivo para um crescimento maior e uma padronização da tecnologia: a maioria dos sistemas de RFID no mercado ainda era de sistemas proprietários. Algumas organizações de padronização trabalharam na publicação de normas, incluindo a *European Conference of Postal and Telecommunications Administrations* (CEPT) e a *International Organizatios of Standards* (ISO). O *Auto-ID Center*, no M.I.T. (*Massachussets Institute of Technology*), foi criado em 1999 exatamente com esse propósito. Atualmente, todas essas organizações estão trabalhando em padrões para a tecnologia RFID, particularmente para aplicações na cadeia de suprimentos e no gerenciamento de estoques [2][1].

Na mesma década, em muitos outros países do mundo, estavam aparecendo aplicações que utilizavam a tecnologia de RFID. Dos países que iniciaram o uso de aplicações utilizando rádio-freqüência, podemos citar: Austrália, China, Hong Kong, Filipinas, Argentina, México, Brasil, Canadá, Japão e Cingapura.

O século 21 começou com a significativa redução dos custos dos tags, chegando a valores como U$ 0,05. As implicações que isso tem para as distribuidoras de produtos e para as redes de varejo chamaram a atenção da indústria. O ano de 2003,

especialmente, foi muito movimentado para o RFID. Nesse ano *Wal-Mart* e *DoD* (*U.S. Department of Defense*), a maior rede de varejo e a maior cadeia de suprimentos do mundo, respectivamente, incentivaram o RFID obrigando seus fornecedores a adotarem a tecnologia até o final de 2005. A magnitude combinada dessas operações constituiu um enorme mercado para o RFID. Outras redes de varejo e muitos fabricantes, como Target, Proctor & Gamble e Gillete seguiram a implantação da tecnologia. Além disso, em 2003, o *Auto-ID Center* foi incorporado a *EPCglobal*, uma *joint-venture* entre o *Uniform Product Code Council* (UPCC), controladores do *UPC Bar Code Symbol*, e a *EAN* (*European Article Numbering*). A tecnologia do EPC foi adotada por *Wal-Mart*, *DoD* e pela indústria de RFID. Isso significou que finalmente o RFID teria uma plataforma comum, permitindo o maior crescimento da tecnologia. Os padrões desenvolvidos pelo EPC foram adotados pela ISO em 2006, dando à indústria de RFID uma única fonte para guiar seus desenvolvimentos. A convergência de todos os padrões para um irá servir para aumentar a competição entre as diversas empresas do mercado, reduzir os custos e rapidamente consolidar a tecnologia de RFID. Atualmente, um grande número de aplicações para o RFID chega a um número cada vez maior de empresas [2][1].

CAPÍTULO 3

Tecnologia de RFID

3.1 Descrição

RFID (*Radio Frequency IDentification*) é uma tecnologia que utiliza ondas de radiofreqüência para transferir dados entre um leitor e um item móvel, para identificação, categorização, rastreamento, etc. A quantidade de objetos identificáveis pelo RFID inclui praticamente tudo que há no planeta. Sendo assim, o RFID é um exemplo de tecnologia de Auto-ID (*Automatic IDentification*), através da qual um objeto físico pode ser identificado automaticamente. O RFID é rápido, confiável e não necessita de visada nem de contato entre o leitor e o objeto a ser lido. O sistema de RFID consiste, basicamente, de tags (uma etiqueta que é aplicada ao produto para que ele seja identificado), leitores e softwares – esse assunto é melhor detalhado na seção 3.4. A operação básica do RFID é ilustrada pela figura 3.1 e, na figura 3.2, é mostrado um esquema do funcionamento:

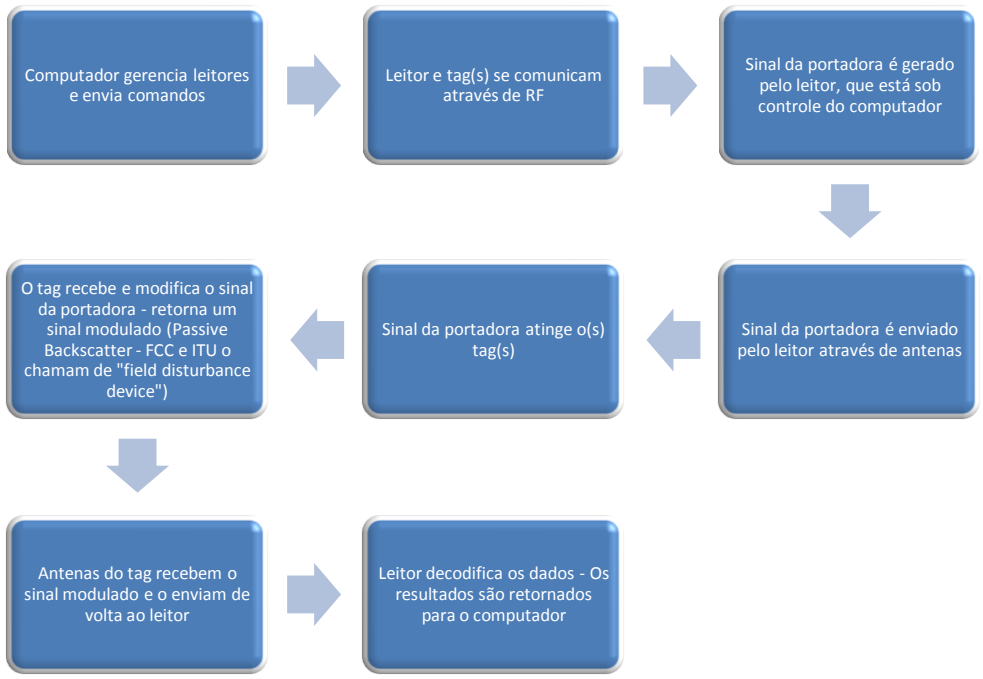

Figura 3.1 – Operação básica do RFID

O tag, ou transponder, é um dispositivo que possui nele gravadas informações, sejam elas 1 bit, ou *n* bit. No caso de *n* bit, o tag pode portar informações do objeto a ser monitorado, da mesma forma que uma carteira de identidade traz informações acerca de uma pessoa. Eles são dividido em três grupos: Ativos, Passivos e Semi-Passivos, classificação essa que será detalhada na seção 3.4.2 deste trabalho. Os sistemas RFID também são divididos de acordo com sua freqüência de operação, que vai desde LF (sendo utilizadas as freqüências 125kHz e 134kHz), até freqüências de Microondas (chegando a utilizar a freqüência 5,8GHz), conforme será visto na seção 3.5.

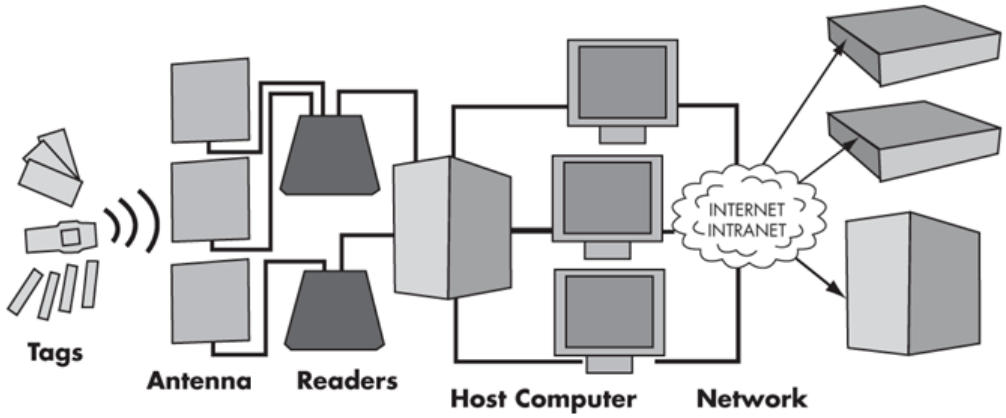

Figura 3.2 – Esquema de funcionamento do sistema de RFID [3]

3.2 Composição de um sistema de RFID

3.2.1 Arquitetura de um sistema RFID

Um sistema de RFID pode ser dividido em dois grupos, de acordo com as características dos equipamentos que o compõe: um que compreende os meios físicos, ao qual pertencem os tags, os leitores, os sensores e a infra-estrutura de comunicação, e outro que compreende tudo que envolve Tecnologia da Informação, ao qual pertencem o *Middleware* e os demais sistemas de tratamento das informações obtidas no processo de leitura.

Um sistema RFID consiste, principalmente, em tags, leitores e *Middleware*. Tags são os dispositivos que carregam uma informação que será lida pela leitora. A leitora é exatamente esse dispositivo que colhe as informações contidas nos tags e as passa ao *Middleware*. O *Middleware* é o software responsável pela comunicação do meio físico com o software de gerenciamento do sistema. Portanto ele recebe as informações da leitora e as repassa ao software do sistema. Ambos os componentes serão detalhados posteriormente. Há também a infra-estrutura de comunicação e eventuais sensores que possam estar acoplados ao sistema. A arquitetura do sistema RFID, com tais componentes, é indicada nas figuras 3.3 e 3.4.

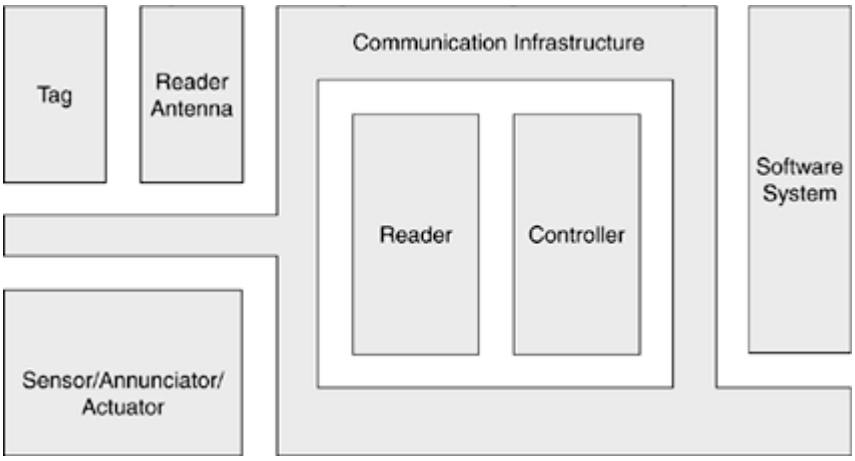

Figura 3.3 – Arquitetura do sistema de RFID [1]

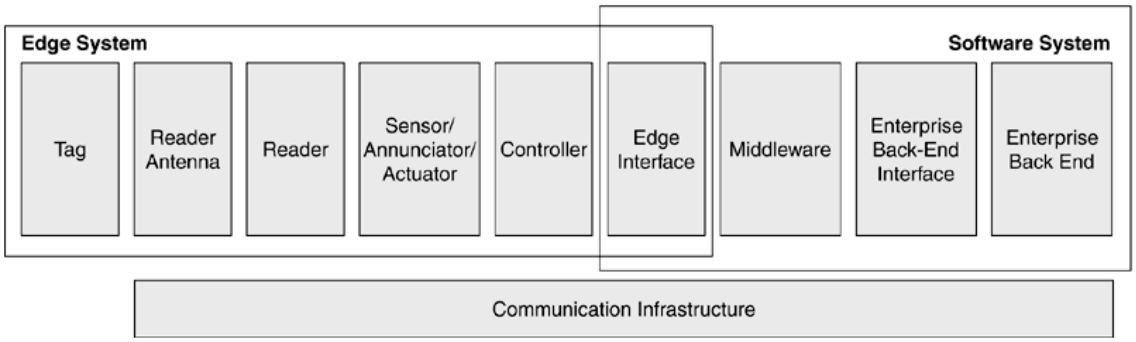

Figura 3.4 – Componentes do sistema de RFID [1]

3.2.2 Tags

A função principal de um tag RFID é armazenar dados e transmiti-los aos leitores. Basicamente, um tag consiste de um chip e uma antena, encapsulados em um invólucro, como mostra a figura 3.5. Geralmente o chip contém uma memória, onde os dados podem ser gravados, lidos e, algumas vezes, dependendo do tipo do tag, escritos. Alguns tags são alimentados, ou seja, também contém uma bateria, que é o que diferencia um tag ativo de um tag passivo. Outra característica muito importante que define qual tipo de tag se utilizar em determinada aplicação é o alcance de leitura. O alcance de leitura depende de vários fatores, como mostra a figura 3.6.

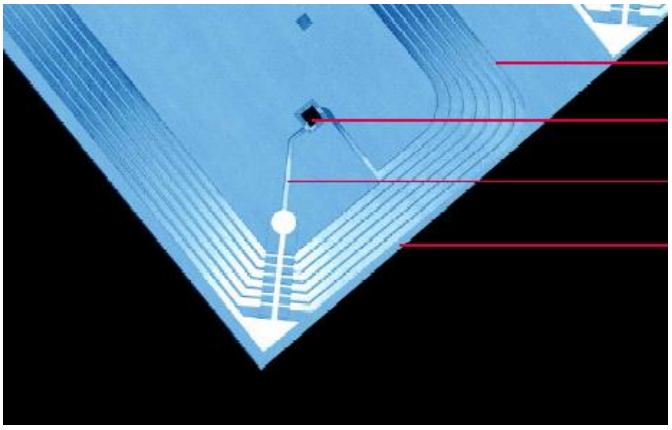

Figura 3.5 – Composição básica de um tag passivo

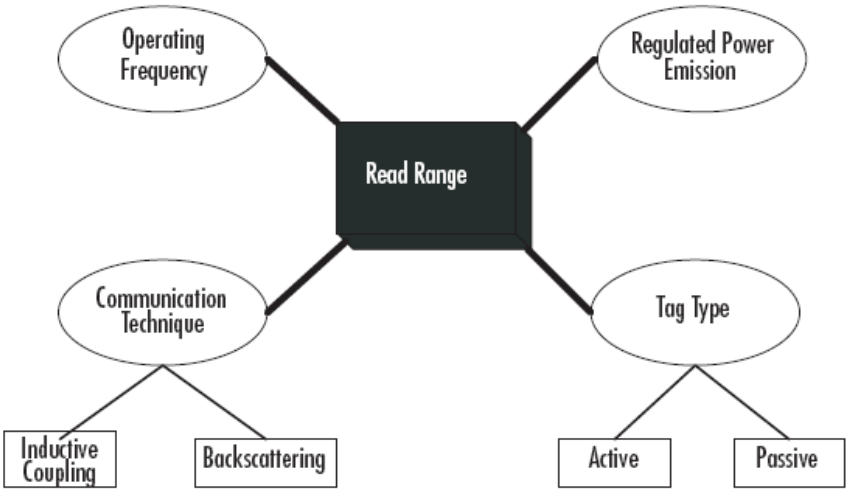

Figura 3.6– Parâmetros que influenciam no alcance de leitura [4]

3.2.2.1 Tags Ativos

Um tag ativo, como os das figuras 3.7 e 3.8, é um tag que possui uma fonte de energia, como uma bateria, e pode iniciar uma comunicação enviando seu próprio sinal. Ele não necessita da potência do leitor para excitar seu circuito, ou criar seu sinal. Bem como não necessita de uma excitação provinda do leitor para que funcione.

Figura 3.7 – Tag Ativo [1]

Figura 3.8 – Diferentes formatos de Tags Ativos

Características

As principais características de um tag ativo são as seguintes:

- **Operação:** Devido à fonte própria de energia possuída pelos tags ativos, há a possibilidade do tag permanecer ligado o tempo todo, ou ficar desligado até que receba algum sinal, economizando energia. Porém, para algumas aplicações que se faz necessário, um tag que estiver operando todo o tempo pode enviar sua localização em intervalos pré-determinados, permitindo sua rastreabilidade.

- **Tamanho:** Devido a suas fontes de energia (baterias), tags ativos, em sua maioria, têm um tamanho grande. Um tamanho típico é (3,8 x 7,6) x 1,3 cm. No entanto esse tamanho tem diminuído a cada dia, devido aos avanços da tecnologia, miniaturizando-os para algo em torno do tamanho de uma moeda [4].

- **Alcance de leitura:** Mais uma vez, devido à fonte própria de energia para alimentação de seu circuito e geração dos sinais, ele pode ser lido a uma distância muito grande. Alguns tags ativos possuem a capacidade de enviar um sinal à distância de 1km. Entretanto, devido a padrões e normas, a maioria dos tags tem

alcance de dezenas de metros. Há aplicações em que um tag ativo é vinculado a um dispositivo de GPS para determinar a exata localização de um objeto.

- **Vida útil:** Apesar de durar muito tempo, algo em torno de 5-10 anos, a bateria tem uma vida útil, o que acarreta na troca do tag ou das baterias do tag após determinados períodos de tempo.

- **Memória:** A capacidade de memória de um tag varia muito. Mas, por, geralmente, ser maior do que os outros tipos de tag, possuindo, assim, mais espaço para componentes, normalmente tem uma maior armazenamento de memória do que os demais.

Aplicações

Devido ao maior alcance de leitura de um tag ativo, ele pode ser utilizado no rastreamento de, por exemplo, vagões de trem e contêineres, que exigem grandes distâncias de leitura. Por causa da habilidade de poder iniciar a comunicação, eles podem ser divididos em dois grupos:

- ***Active transponders*:** Os tags pertencentes a essa categoria só são ativados quando eles recebem um sinal do leitor. Esse modo de operação prolonga a vida da bateria. Normalmente esses tags são utilizados em aplicações como sistemas de coleta de pedágio ou de controle de acesso, nos quais o tag apenas estará ativo quando se aproximar de um leitor

- ***Beacons*:** Os tags que são denominados de *beacons* emitem um sinal em intervalos de tempo pré-determinados. Os *beacons* são muito utilizados em sistemas de localização em tempo real (RTLS), nos quais, por um sistema de triangulação de leitores, sabe-se exatamente a posição do tag em um determinado espaço.

A grande maioria dos tags ativos é utilizada em aplicações que operam na faixa de freqüência UHF e em freqüências de Microondas (como 455MHz, 2,45GHz e 5,8GHz) e tem distância de leitura que varia de 20 a 100m [4].

Vantagens / Desvantagens

As principais vantagens da utilização dos tags ativos é, sem dúvida, a distância necessária para que a leitura seja efetuada com sucesso. Enquanto que nos outros tipos de tags ela se restringe a poucos metros, no caso dos tags ativos ela varia de vários metros, chegando até a quilômetros, apesar de restrita, por normas, a algumas centenas de metros. Outra vantagem é, por ser auto-alimentado, a maior capacidade de processamento, bem como de armazenamento de dados. Da mesma forma que a bateria interna representa uma grande vantagem, ela significa uma desvantagem, visto que há a necessidade da sua substituição quando finda sua carga, ou da troca do tag, já que muitas vezes se torna inviável o processo de substituição da bateria.

3.2.2.2 Tags Passivos

Este tipo de tag RFID não possui uma fonte de alimentação (uma bateria, por exemplo) incorporada em sua estrutura. Ele utiliza a energia emitida pelo leitor para energizar o seu circuito e transmitir os dados nele contidos. Exemplos de tags passivos são mostrados na figura 3.9.

Figura 3.9 – Exemplos de tags passivos [1]

Características

Nas comunicações tag-leitor, supondo os tags passivos, a comunicação sempre é iniciada pelo leitor. A presença de um leitor é condição sinequanon para que o tag transmita os dados nele contidos. A estrutura de funcionamento de um tag passivo é, basicamente, demonstrada na figura 3.10, a seguir:

Figura 3.10 – Estrutura de funcionamento de um tag passivo

Esse tipo de tag é, normalmente, menor do que um tag ativo ou semi-passivo. Por não possuir bateria interna e por necessitar de energia suficiente provinda do leitor para por seu circuito em funcionamento, ele precisa estar dentro da zona de atuação do leitor; logo, sua distância de leitura varia de menos que 3cm a algo em torno de 9m [1]. Ele é, também, geralmente, mais barato do que os demais tipos de tag, devido, principalmente, a sua simplicidade.

Aplicações

Um tag passivo é simples em sua construção e não tem partes móveis. Como resultado, este tipo de tag tem uma vida útil extremamente longa e é, geralmente, resistente a várias condições adversas de ambiente. Por exemplo, alguns tags passivos podem conviver com substâncias químicas corrosivas, como ácidos, ou com temperaturas elevadas de mais de 200°C, dentre outros [1]. Por isso, dependendo da necessidade da aplicação, ele pode ser utilizado em condições extremas. As aplicações ideais para os tags passivos são as que requerem pequenas distâncias para leitura.

Uma das grandes aplicações dos tags passivos, que pode até ser considerado como uma subdivisão destes, é o *Contactless Smart Card*, que será detalhado posteriormente. Trata-se de um tipo especial de tag passivo, no formato de um cartão, amplamente utilizado nos mais variados tipos de aplicações, como, por exemplo, no controle de acesso, onde os dados armazenados no cartão são lidos quando ele estiver próximo ao leitor. É importante ressaltar que o cartão não precisa estar em contato físico com o leitor para que a leitura seja efetuada.

Vantagens / Desvantagens

As principais vantagens dos tags passivos se referem ao seu custo extremamente baixo, permitindo que seja aplicado em várias situações. Outras vantagens dizem respeito à resistência à condições adversas, conforme foi citado anteriormente e à vida útil extremamente longa, visto que não possuem bateria interna; logo, não há a necessidade de substituição da mesma. Da mesma forma que a bateria interna se traduz como uma vantagem aos tags passivos, ela significa uma grande desvantagem: a curta distância de leitura. Essa desvantagem é o que inviabiliza muitos dos projetos envolvendo esse tipo de tag.

Um tag passivo é composto, essencialmente, pelos seguintes componentes, conforme figura 3.11:

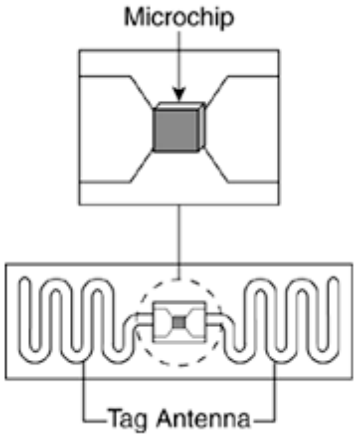

Figura 3.11 – Composição de um tag passivo [1]

- **Microchip:** É responsável por armazenar as informações, além de converter a energia AC recebida através do sinal da antena do leitor para DC, alimentando, assim, os demais componentes; modular o sinal recebido, embutindo nele as informações contidas no tag; e enviar de volta tal sinal ao leitor

- **Antena:** É utilizada para direcionar a energia do sinal recebido do leitor, para energizar o tag, bem como para enviar e receber os dados do leitor. Essa antena é fisicamente ligada ao microchip. Sua geometria é fundamental para operação do tag. Infinitas variações no seu desenho são possíveis, especialmente para UHF. Seu comprimento é diretamente proporcional ao comprimento de onda referente à freqüência de operação do tag. Exemplos de antenas em diversos tipos de tags passivos são mostrados na figura 3.12.

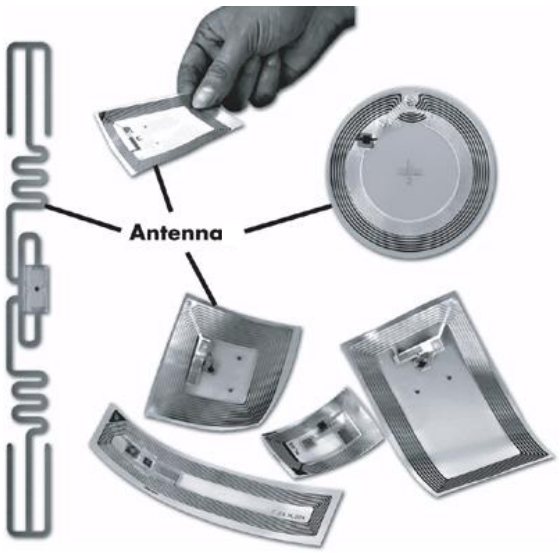

Figura 3.12 – Exemplos de antenas em tags passivos [3]

3.2.2.3 Tags Semi-Passivos

Um tag semi-passivo, ou semi-ativo, como alguns preferem, é um tag que possui sua própria fonte de energia, como uma bateria, porém não tem a iniciativa da comunicação com o leitor, mas sim, responde ao sinal enviado por este. Em outras palavras, o sinal do leitor "liga" o tag. Um tag semi-passivo utiliza sua bateria para colocar o circuito em funcionamento. As principais características de um tag semi-passivo são:

- **Operação:** Devido à capacidade do tag semi-passivo transmitir um sinal de resposta apenas se ele receber algum tipo de contato do leitor, seu princípio de operação é praticamente o mesmo de um tag passivo

- **Tamanho e Alcance:** Devido à bateria interna, tanto o tamanho como o alcance são naturalmente maiores do que de um tag passivo

- **Vida útil:** Um tag semi-passivo tem uma vida útil menor que a de um tag passivo, devido à bateria

- **Memória:** A capacidade de memória de um tag semi-passivo varia, mas pode ser bem maior do que de um tag passivo, devido ao seu maior tamanho, que permite uma maior alocação do espaço interno com componentes de memória

Em suma, um tag semi-passivo, como o da figura 3.13, utiliza uma bateria para que seu circuito funcione, mas não tem a iniciativa da comunicação com o leitor, pois ele usa a energia vinda do sinal do mesmo para preparar a resposta.

Figura 3.13 – Exemplos de tags semi-passivos [1]

Sendo assim, pode-se traçar uma linha entre os tipos de tags existentes. Em uma ponta da linha constam os tags passivos, que não possuem bateria interna e não iniciam a comunicação. Na parte intermediária da linha constam os tags semi-passivos, que

possuem bateria interna, mas não a iniciativa da comunicação. E no outro extremo da linha os tags ativos, que possuem bateria interna e a iniciativa da comunicação.

3.2.2.4 Comparação entre tags passivos, semi-passivos e ativos

A comparação entre as principais características dos três tipos de tags existentes (Passivos, Semi-Passivos e Ativos) pode ser resumida através da tabela a seguir:

Tipos de tags			
Características	***Passivos***	***Semi-Passivos***	***Ativos***
Fonte de Alimentação	Sem fonte própria. Recebe energia gerada pelo leitor	Possui fonte de energia própria (bateria)	Possui fonte de energia própria (bateria)
Comunicação	Comunicação deve ser iniciada pelo leitor	Comunicação deve ser iniciada pelo leitor	Pode ou responder ao sinal gerado pelo leitor, ou iniciar a comunicação
Tamanho	Pequeno. Pode ser tão pequeno quanto (0.15mm x 0.15mm) x 0.75µm	Médio	Grande. Geralmente (3,8 x 7,6) x 1,3 cm
Distância da leitura	Curta. Em geral, alguns milímetros, mas pode chegar a alguns metros, dependendo da freqüência de operação	Média. Pode chegar a mais de 100m	Grande. É possível chegar a mais de 1km. Porém algumas normas e padrões limitam esse alcance
Tipo de memória	Read Only(RO), Write Once/Read Many (WORM) ou Read/Write(RW)	Read Only(RO), Write Once/Read Many (WORM) ou Read/Write(RW)	Read Only(RO), Write Once/Read Many (WORM) ou Read/Write(RW)
Capacidade de memória	Normalmente em torno de 128bits, porém alguns tags possuem mais de 64kB	-	Mais de 8MB
Custo	Baixo	Médio	Alto

3.2.3 Leitores

Os leitores atuam como uma ponte entre o tag e o software. Ele possui algumas funções básicas, como ler os dados contidos nos tags, escrever dados nos tags e alimentar os tags passivos. Os leitores compõem o sistema nervoso central do *hardware* de um sistema de RFID. O estabelecimento de uma conexão e o controle de suas operações são as tarefas mais importantes de qualquer dispositivo que busca integração com esse *hardware*. Devido a sua maior complexidade e aos componentes internos, ao contrário dos tags, os leitores não são tão resistentes às condições adversas do ambiente.

Um leitor possui os seguintes componentes, conforme a figura 3.14:

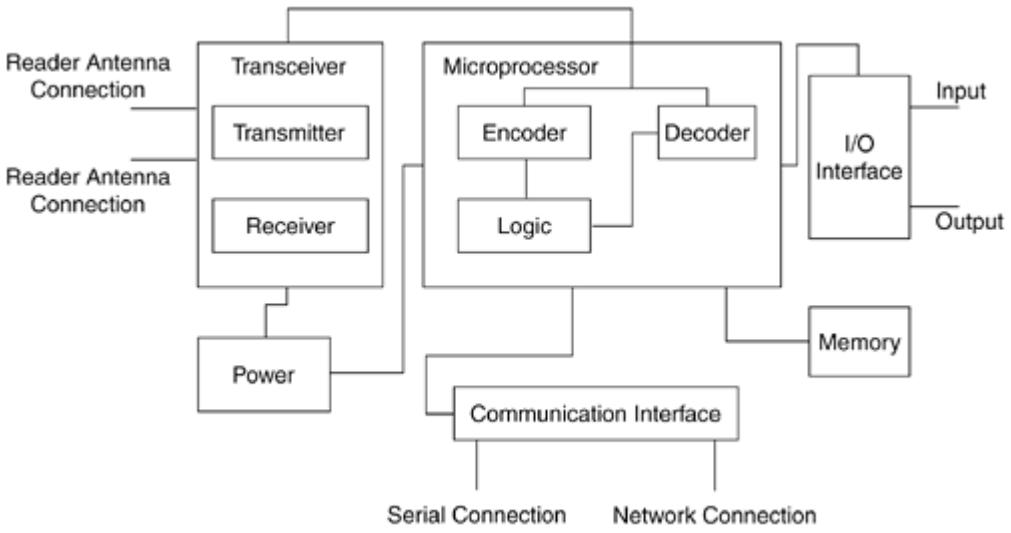

Figura 3.14 – Componentes de um leitor de RFID [1]

- **Transmissor:** O transmissor do leitor é usado para transmitir energia AC e o ciclo de *clock*, por meio da(s) antena(s) do leitor, para os tags, na zona de leitura. Esta é uma parte da unidade transceptora, o componente responsável por enviar o sinal do leitor para o ambiente e receber as respostas dos tags por meio da(s) antena(s) do leitor. As portas de antena de um leitor são conectadas ao seu transceptor. Uma antena de leitura pode ser acoplada a cada porta de antena disponível. Atualmente, alguns leitores podem suportar até quatro portas de antenas [1].

- **Receptor:** Este componente é, também, parte do módulo transceptor. Ele recebe sinais analógicos dos tags, por intermédio da antena, e envia esses sinais para o microprocessador do leitor, onde serão convertidos a sinais digitais equivalentes (representação digital dos dados que o tag transmitiu à antena do leitor).

- **Microprocessador:** Este componente é responsável por implementar o protocolo de leitura para comunicar-se com os tags compatíveis. Ele efetua a decodificação e a análise de erros do sinal analógico recebido do módulo receptor. Além disso, o microprocessador pode conter uma lógica personalizada para efetuar uma filtragem de baixo nível e processar os dados lidos dos tags [1].

- **Memória:** A memória é utilizada para armazenar dados, parâmetros de configuração do leitor e uma lista de leituras de tags, ou seja, um histórico de leituras. Por isso, se a conexão entre o leitor e o controlador, ou o *software* do sistema, cai, nem todos os dados de leitura de tags são perdidos. O limite de leituras que serão armazenadas depende do tamanho da memória disponível. Se a conexão volta a cair, mas agora por um período maior de tempo, e o leitor continuando a ler tags durante esse período, tal limite pode ser excedido e uma parte dos dados armazenados, perdidos, ou seja, substituídos por outras leituras de tags mais atuais [1].

- **Canais de entrada/saída para sensores externos, atuadores e anunciadores (embora esses componentes sejam opcionais em um sistema de RFID, o seu suporte normalmente é provido pelo leitor):** Sensores, atuadores e anunciadores podem ser acoplados aos leitores. Por exemplo, leitores não têm que estar ligados durante todo o tempo. Eles podem ser iniciados e parados automaticamente, se necessário. Para esse fim, pode ser utilizado um sensor, como de movimento, ou de luminosidade. Esse sensor pode, então, através desses eventos externos, como a detecção da presença de um objeto com tag na zona de leitura, ligar ou desligar o leitor. Logo, um sensor pode ser utilizado como um tipo de circuito de disparo do leitor. Isso gera uma economia de energia muito grande, visto que o leitor só estará ligado quando for solicitado.

  Um anunciador é um sinal eletrônico, ou um indicador, como um alarme sonoro, ou um conjunto de luzes que podem expressar o status de diferentes atributos do sistema; por exemplo, se uma luz vermelha se acende, pode significar que os dados da leitura de um tag estejam corrompidos, ou que o tag esteja danificado, da mesma forma que uma luz verde pode indicar que a leitura foi efetuada com sucesso e uma luz amarela pode indicar que haja um problema na conexão entre o leitor e o controlador.

  Um atuador é um dispositivo mecânico para o controle de objetos que se movem. Exemplos de atuadores são o PLC (*Programmable Logic Controller*), braços de um robô, braços mecânicos para um portal de acesso, etc. O PLC é um dos atuadores mais versáteis e é amplamente utilizado em fábricas. Ele torna possível uma ampla gama de ações, como monitorar e controlar uma linha de produção, por exemplo.

  Anunciadores e atuadores podem então serem utilizados para prover alguns tipos de interações externas de um sistema RFID, como alertas áudio-visuais, ou no caso de um erro de leitura, abrir um portal de acesso no caso de uma leitura ter sido efetuada com sucesso, por exemplo [2].

- **Controlador:** Um controlador é um dispositivo que permite a comunicação com uma entidade externa, como, por exemplo, com um *software*, controlar funções do leitor e controlar atuadores e anunciadores associados com esse leitor. O controlador

é o único componente de um sistema de RFID através do qual são possíveis comunicações com o leitor. Uma analogia pode ser feita entre um computador e uma impressora. Para que a impressão seja realizada, o computador dever possuir a interface de comunicação com a impressora. Da mesma forma, para receber os dados armazenados em um tag, um computador precisa usar um controlador. Normalmente fabricantes incorporam esse componente dentro do próprio leitor (como um *firmware*, por exemplo). Entretanto, também é possível que seja vendido como um componente de *hardware* ou de *software* separado, que deve ser comprado junto com o leitor.

- **Interface de comunicação:** Esse componente provê as instruções de comunicação para o leitor, o que lhe permite interagir com outros components externos, por meio do controlador, para transferir os dados que estiverem armazenados, aceitar comandos e enviar de volta as respectivas respostas. O leitor deve ter uma interface para comunicação com a rede, como serial, Ethernet ou Wireless. Leitores mais completos possuem outras funções, como descobrimento automático pelo software (uma espécie de plug-and-play), servidores Web embutidos, o que permite ao leitor aceitar comandos e exibir respostas utilizando um browser Web, etc.

- **Fonte de alimentação:** Este componente fornece a energia para o funcionamento do leitor.

- **Antena:** A antena é o que conduz a comunicação dos dados entre o tag e o leitor. O design da antena e o local onde é colocada são fatores determinantes para a zona de cobertura, o alcance e a eficiência da comunicação. Por exemplo, uma antena com polarização linear perde eficiência na leitura quando a orientação do tag varia aleatoriamente com relação à orientação da antena do leitor. Isso faz, por exemplo, com que antenas polarizadas linearmente sejam mais aplicadas onde a orientação dos itens taggeados é sempre a mesma, como em uma linha de produção automatizada. As características de montagem da antena em um leitor variam de acordo com as necessidades da aplicação. Em certos casos, como em leitores *handheld*, a antena é montada no próprio leitor. Em outros casos, algumas antenas podem ser postas em locais distantes do leitor e posicionadas estrategicamente, de forma a melhorar a qualidade e o alcance dos sinais de rádio. Por exemplo, no rastreamento de um pallet o leitor pode ser conectado junto a uma rede de antenas tal que forme uma zona de detecção como um portal, conforme figura 3.15, para aumentar a eficiência de leitura e assegurar uma boa performance em locais de carregamento.

Figura 3.15 – Portal de antenas [3]

Os leitores também podem ser divididos em 2 categorias:

- ***Handhelds*:** Um leitor *Handheld*, como o mostrado na figura 3.16, é um leitor móvel (portátil), que pode ser operado como se fosse um computador de mão. Esse tipo de leitor, normalmente, possui antena interna. Contudo, esses leitores são, geralmente, mais caros. Recentes avanços na tecnologia dos leitores estão contribuindo para a redução do seu custo e, também, resultando em leitores *Handheld* cada vez melhores.

Figura 3.16 – Leitor *Handheld*, de RFID [5]

- ***Stationary*:** Um leitor *Stationary*, como o mostrado na figura 3.17, é um leitor fixo. Esses leitores são instalados em portas, portais ou outros locais. A estrutura na qual o leitor é instalada não precisa ser estática. Por exemplo, alguns leitores *Stationary* são instalados em empilhadeiras. Da mesma forma, podem ser instalados leitores no interior de caminhões de entrega. Os leitores *Stationary* geralmente necessitam de antenas externas para uma boa leitura dos tags - um leitor pode prover até quatro conexões para encaixe de antenas externas. O custo de um leitor fixo é, normalmente, muito menor do que o custo de um leitor portátil, por isso, eles são o tipo mais comum utilizado atualmente.

Figura 3.17 – Leitor *Stationary*, de RFID [5]

Também podem ser destacados outros dois tipos de leitores:

- ***Agile*:** Um leitor *Agile*, como o da figura 3.18, pode operar em diferentes freqüências ou pode utilizar diferentes protocolos de comunicação tag-leitor-tag. Atualmente a maioria dos leitores desse tipo é *Stationary*.

Figura 3.18 – Leitor *Agile*, de RFID [6]

- ***RFID Printer*:** Um leitor *RFID Printer*, mostrado na figura 3.19, é um equipamento que pode imprimir um código de barras e criar (ou seja, escrever dados) um tag em uma *smart label*, tudo em apenas uma operação. Uma *smart label*, mostrada na figura 3.20, consiste de uma etiqueta com código de barras que possui um tag RFID. Vários tipos de informação, tais como os endereços do remetente e do destinatário, informações do produto e quaisquer outras informações podem ser impressas na etiqueta também. Um *RFID Printer* lê a *smart label* que ele acabara de escrever, para validar a operação de escrita. Se essa validação falha, a impressora descarta a *smart label* que ele imprimira. Esse equipamento procura resolver a necessidade de separadamente criar um tag RFID onde códigos de barra já são utilizados, o que reduz custos. Um negócio que está utilizando códigos de barras para suas operações pode utilizar as *RFID Printers* como um primeiro passo na adoção da tecnologia de RFID [1]. A informação do código de barras provê uma identificação legível por um ser humano, para o objeto que contém o tag. Também, os sistemas e operações existentes permitem utilizar os mesmos dados contidos no código de barras, com poucas, ou nenhuma, alterações.

Figura 3.19 – RFID *Printer* [7]

Figura 3.20 – *Smart Label* [1]

3.2.4 RFID System Software

O *RFID System Software*, ou software do sistema de RFID, consiste de um conjunto de funções necessárias para habilitar a interação básica entre tag e leitor. Na sua forma básica, a comunicação ocorre no nível de processamento de um sinal de rádio, o que requer hardware, firmware e um software para gerenciar os dados que são obtidos [3]. As funções normalmente constantes no software do sistema são:

- **Leitura/Escrita:** Esta é a função mais básica com um tag: o leitor se comunica com o tag para ler ou gravar dados; o tag acessa sua memória para ler os dados, conforme solicitado, e transmite de volta os dados ao leitor. O tag também pode ser suprido de dados pelo leitor (vindos do software de aplicação), gravando-os em sua memória, desde que o tag possua essa funcionalidade.

- **Anti-colisão:** Um software de anti-colisão é utilizado quando, em um dado momento, múltiplos tags estão presentes no campo de leitura de um único leitor, devendo ser identificados e monitorados ao mesmo tempo. Isso é comum na maioria das aplicações na cadeia de suprimentos. Por exemplo, em uma aplicação de gerenciamento de estoque, centenas, ou até milhares, de objetos podem estar dentro do campo de leitura de um único leitor. Um simples pallet de objetos com tags pode ter mais de 100 embalagens, cada um contendo dezenas de itens.

  O sistema de anti-colisão também requer cooperação entre os tags e os leitores, a fim de minimizar o risco de muitos tags responderem todos ao mesmo tempo. Em alguns casos, o algoritmo pode ser simples como cada tag espera uma quantidade aleatória de tempo antes de responder à solicitação do leitor.

- **Detecção/Correção de Erros:** Em um leitor podem ser empregados softwares sofisticados para detectar e corrigir erros de transmissão com os tags. Dessa forma, o software pode, também, incluir uma programação para detectar e descartar dados duplicados ou incompletos.

- **Segurança:** Codificação, Autorização e Autenticação são muito úteis quando há a necessidade da troca de dados entre o leitor e os tags ser segura. Ambos os tags e o leitor devem cooperar para executar o protocolo necessário para atingir o nível desejado de segurança dos dados. Por exemplo, para prevenir que um leitor não-autorizado capte dados de um tag, o tag e o leitor podem ter que executar um protocolo de autorização, através da troca de códigos secretos comuns. Depois de essa informação ter sido trocada e validada, o tag, então, transmite os dados ao leitor. Funções de segurançano tag requerem um CI sofisticado, o que pode impactar significativamente no custo do tag.

3.2.5 Middleware

Middleware é um termo que, quando aplicado à TI pode ser entendido como o que liga um ambiente computacional a outro. Ele é, sinteticamente, um software que integra sistemas, responsável pela integração das diferentes camadas de um ambiente de TI: comunicação, distribuição e controle das mensagens e processos relativos ao fluxo de trabalho. Também conhecido como *Application Infrastructure*, engloba produtos como servidores de aplicações, servidores de integração (EAI) e portais. Na implantação de um sistema de RFID, após a escolha dos tags e das antenas apropriadas para a aplicação, deve-se definir como os eventos gerados irão chegar aos sistemas legados. O *middleware* existe para resolver três problemas comuns a toda implantação de RFID:

- separar a aplicação da interface dos dispositivos;
- processar as observações capturadas pelos leitores de modo que as aplicações apenas processem eventos que sejam de interesse delas;
- prover um meio de gerenciar e obter as observações independente do leitor.

Um *middleware* deve prover, pelo menos, os três subsistemas abaixo:

- **Interface com o leitor:** interliga todos os leitores da rede, uma vez que cada leitor tem uma API específica, e uma rede pode ter mais de um tipo diferente de leitor. O *middleware* tem como função principal prover um meio único de controlar e obter informações dos leitores, ou seja, facilitar a integração dos leitores da rede;
- **Gerenciador de eventos:** em um cenário típico de um centro de distribuição, por exemplo, existirão dezenas de leitores, gerando de centenas a milhares de leituras para os aplicativos de controle. Uma aplicação de controle de centro de distribuição não está preparada para receber todos estes eventos e tratá-los instantaneamente. Para isso, uma aplicação deve filtrar estes eventos e enviar ao aplicativo apenas os relevantes ao processo, no contexto da aplicação. O sistema que tem esta lógica de filtragem dos dados relevantes é o *middleware*;
- **Interface com aplicação:** um dos benefícios do uso de *middleware* é o de prover uma interface padronizada para as aplicações. Uma interface orientada a serviço, também chamada de interface de aplicação, provê meios de se obter os eventos úteis para a aplicação, já processados. Seguindo os princípios da arquitetura orientada a serviços (SOA), esta interface deve seguir os padrões atuais de serviços web (*web services*). O *middleware* tem a capacidade de automatizar processos de um modo que não era possível antes, com as tecnologias de leitura de códigos de barra, que dependiam da intervenção humana. No entanto, esse nível de automação requer que os leitores sejam monitorados e gerenciados remotamente. Em alguns casos a solução é implantada em máquinas ou redes totalmente diferentes de onde a aplicação legada está, o que pode comprometer a infra-estrutura de rede (devido ao alto consumo de banda), caso não exista um *middleware* filtrando os eventos insignificantes [8].

Savant

Leitores RFID podem gerar milhares de eventos em um curto espaço de tempo. Existem estimativas que, com o rastreamento de itens ao longo da cadeia, a quantidade de dados trafegando na rede se multiplica por 100 e até por 1000. Um sistema de RFID deve usar uma arquitetura robusta para conseguir processar e filtrar toda esta quantidade de dados. Em suma ela deve apresentar as seguintes características:

- Ser uma arquitetura que suporte um grande volume de dados, para que tenha a capacidade de processar os eventos nos extremos da rede onde o dado está sendo gerado;

- Usar "concentradores" para processar o grande volume de dados gerado. Estes concentradores fazem a filtragem e agregação do fluxo sendo processado. O *Savant* é um sistema que funciona como se fosse o sistema nervoso central da rede EPCglobal;

- Criar uma infra-estrutura para distribuir os dados coletados de modo que a solução seja escalável e, mais tarde, fornecê-los aos sistemas legados.

Na figura 3.21 é mostrado um exemplo da arquitetura *Savant*. O padrão *Savant* define os módulos necessários para um projeto de RFID. O termo "*Savant*" significa um *middleware* distribuído que fique entre fontes de eventos e aplicações da empresa, com o intuito de filtrar dados. Seu foco inicial era de prover um padrão para o processamento de eventos, mas ele se concentrava mais em definir como os serviços deveriam ser implementados do que a interface entre eles. Sendo assim, esse padrão se tornou obsoleto e o padrão atual é a especificação ALE [8].

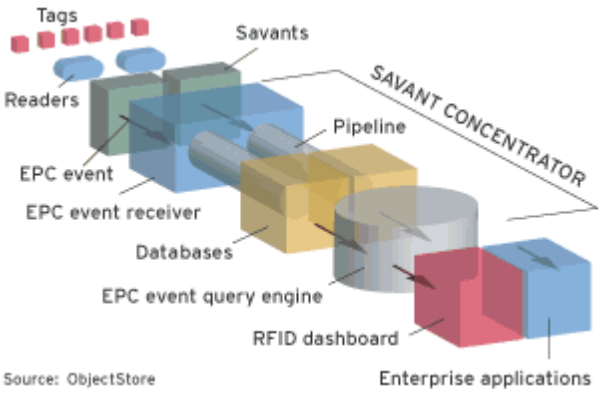

Figura 3.21 - Exemplo de arquitetura *Savant* [5]

ALE (*Application level events)*

A especificação ALE (Application Level Events) se refere a uma interface padrão desenvolvida pela EPCglobal para obter dados de uma grande variedade de leitores, independentemente de fabricante. O processamento das informações é feito em três etapas: receber os EPCs de uma ou mais fontes; filtrar, contar e agrupar os dados; e reportar tais eventos. Esse padrão descentraliza o processamento de dados, levando-o aos extremos da rede, diminuindo a distância para os eventos. Sendo assim, o sistema adquire uma flexibilidade que permite que o *middleware* seja instalado ou no próprio local onde os eventos são gerados, ou dentro do leitor (quando aplicável) ou, ainda, no data-center. Para que esse tipo de serviço esteja de acordo com a especificação ALE, ele precisa atender os seguintes requisitos:

- Padrão para gerenciamento de eventos: este padrão provê uma interface para receber, filtrar e agrupar eventos de qualquer leitor RFID. Aplicações compatíveis com esta interface não precisam ter um *driver17* para cada tipo de leitor, nem precisam usar interfaces proprietárias de cada fabricante;

- Flexibilidade: esta especificação é altamente extensível. Ainda que seu foco seja eventos EPC, extensões podem ser criadas para criar uma conexão com interfaces que não sejam de leitores RFID, como com bancos de dados que contenham configurações ou com CLPs e sistemas legados;

- Implementação livre: o padrão provê uma interface entre os clientes e o *middleware* que deixa a implementação a cargo de cada fornecedor. Deste modo, os fornecedores podem escolher a melhor plataforma, tecnologia e forma de instalação.

Por separar em diferentes camadas a captura, o processamento e a distribuição de eventos, este padrão permite que ocorram mudanças nessas camadas sem que haja interferência nos demais componentes do sistema, beneficiando fabricantes de leitores, provedores de soluções e usuários finais [8].

3.2.6 Software de aplicação

O software de aplicação recebe os dados enviados pelos tags, processados e organizados através do leitor e do *middleware*, e faz o tratamento de tais informações de acordo com a finalidade da aplicação. Tal software pode ser um já existente na empresa, e atualizado para comportar o gerenciamento do sistema de RFID, ou um novo. Como o software varia de acordo com a empresa e com a aplicação, não há um padrão a ser seguido.

3.3 Freqüências de operação

Uma consideração muito importante com relação ao RFID é a escolha da freqüência de operação. Sistemas RFID utilizam diversas bandas para comunicação, como mostra a figura 3.22.

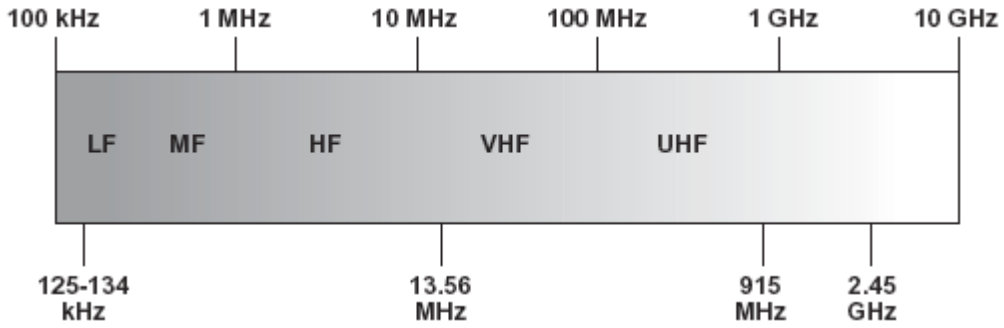

Figura 3.22 – Bandas de freqüência [2]

Basicamente são consideradas as seguintes faixas de freqüência para aplicações de RFID: LF, HF, UHF e freqüências de Microondas, consideradas como sendo as freqüências maiores do que 1GHz [1]. A escolha da freqüência de operação depende de várias variáveis, bem como afeta várias características do sistema a ser implantado, como segue:

- **Alcance de leitura:** Nas freqüências de operação mais baixas o alcance de leitura de tags passivos não passa de 50-60 cm (Tal alcance é extremamente restrito devido, principalmente, ao baixo ganho das antenas, visto que em baixas freqüências os comprimentos de onda são muito grandes, logo, muito maiores que as dimensões das antenas integradas nos tags. Como o ganho de uma antena é diretamente proporcional ao seu comprimento, que, por sua vez, é relacionado com o comprimento de onda, o ganho em baixas freqüências é muito baixo.) Em altas freqüências o alcance de leitura é muito maior, especialmente quando se utiliza tags ativos. No entanto, devido a possíveis danos que as altas freqüências possam causar à saúde humana, os órgãos reguladores impuseram limites de potência aos sistemas que utilizam UHF e Microondas, o que reduziu a distância de leitura, em sistemas RFID que utilizam essas freqüências, para algo em torno de 3-9 m, no caso de se usar tags passivos [2].

- **Utilização de tags ativos ou passivos**: Normalmente, tags passivos são usados nas faixas LF e HF, enquanto que os tags ativos são usados em UHF e em freqüências de Microondas. O motivo pelo qual se utiliza os tags dessa forma é histórico. Os primeiros sistemas RFID usavam as bandas HF e LF com tags passivos, devido ao alto custo da tecnologia na época. Porém hoje isso está sendo alterado. Os recentes avanços tornam possível usar tags ativos em bandas de alta freqüência, e essa tem sido a tendência do mercado de RFID [2].

- **Interferência de outros sistemas de rádio:** Sistemas de RFID são naturalmente propensos à interferência de outros sistemas de rádio. Particularmente, os sistemas RFID que operam na banda LF são muito vulneráveis, devido ao fato de que baixas freqüências não sofrem muitas perdas, ou atenuam muito pouco quando propagadas em curtas distâncias, se comparadas com altas freqüências. Ou seja, os sinais de rádio de outros sistemas de comunicação que estiverem operando aproximadamente na mesma freqüência LF criarão altos campos eletromagnéticos na antena do leitor RFID, ou seja, gera interferência. Já os sistemas que utilizam freqüências de Microondas estão muito menos susceptíveis a interferências externas, visto que as perdas nessas freqüências são muito maiores, e, geralmente, é necessário ter visada entre os irradiadores de microondas para que interfiram [1].

- **Líquidos e metais:** A performance de um sistema RFID é severamente afetada pela água ou por superfícies úmidas. Sinais HF são mais eficientes na penetração da água do que sinais UHF e do que os de Microondas, devido ao comprimento de onda de um sinal HF ser maior do que o de um sinal UHF ou de um de Microondas. Sinais em bandas de altas freqüências são mais absorvidos pelos líquidos do que os de baixas freqüências. Com isso, tags HF são uma melhor escolha para contêineres que contenham líquidos. Os metais têm como característica a reflexão de ondas eletromagnéticas, logo, sinais de rádio não podem penetrá-lo. Sendo assim, um metal pode não apenas obstruir uma comunicação, se postado entre o tag e o leitor, como também afetará a operação do sistema, visto que quando um metal é colocado próximo a uma antena, as características da antena são modificadas. É importante ressaltar que as bandas de freqüências mais altas são mais afetadas por metais do que as de freqüências mais baixas. Logo, quando há a necessidade de instalar tags em objetos feitos de metal, contêineres que portem líquidos ou materiais com alta permissividade dielétrica, algumas precauções especiais tem de serem tomadas, o que, invariavelmente, elevará o custo da solução [2].

- **Taxa de transmissão dos dados**: Quanto menor a freqüência de operação do sistema RFID, menor a taxa de transmissão. Sendo assim, sistemas que operam na banda LF têm taxas da ordem de Kbits/s, enquanto que nos sinais de freqüências de Microondas essa taxa pode atingir Mbits/s.

- **Antenas – Tamanhos e Tipos**: Como sinais de rádio de freqüências mais baixas possuem comprimentos de onda maiores, as antenas para sistemas que operam em LF e HF são maiores do que as que operam em sistemas de UHF e em freqüências de Microondas, mantendo-se o mesmo ganho de sinal, para efeito de comparação. Entretanto, essa diferença no tamanho das antenas conflita com o constante objetivo da indústria de produzir tags RFID cada vez menores e mais baratos. A fim de evitar elevar muito os custos dos tags, a maioria dos designers de sistemas ignoram o ganho das antenas, o que tem resultado em um baixo alcance de leitura para sistemas que utilizam as bandas LF e HF. Sendo assim, as antenas precisam ser maiores quando são usadas freqüências LF e HF, o que traz como resultado que tags LF e HF são tipicamente maiores do que tags para UHF e para freqüências de Microondas. Além do tamanho, a freqüência de operação do sistema também irá ditar o tipo de antena a ser utilizada. Sistemas LF e HF exigem antenas indutivas e por acoplamento indutivo, que, normalmente, são antenas em forma de loop. Enquanto que sistemas UHF e de

freqüências de Microondas exigem antenas por acoplamento capacitivo, que são do tipo dipolo [2][1].

- **Nulos de Antenas e problemas de orientação:** As antenas indutivas, tais como as utilizadas em LF e em HF, operam inundando a zona de leitura com sinais RF. Além disso, para os grandes comprimentos de onda dos sinais LF e HF, elas trabalham para inundar a zona de leitura com um sinal uniforme, que não tenha diferença de potência de um extremo a outro. Entretanto, as antenas dipolo, como as que são utilizadas nas freqüências UHF e nas de Microondas, operam emitindo sinais do transmissor até o receptor diretivamente. Isso, considerando-se o pequeno comprimento de onda dos sinais pertencentes à banda UHF e dos de freqüências de Microondas, dá oportunidade a pequenas ondulações na zona de leitura, o que não permite que a força do sinal, de um extremo a outro da zona de leitura, seja uniforme. Esse fato pode, inclusive, chegar a diminuir a potência do sinal, gerando pontos de nulidade de sinal, ou regiões de sombra. Os tags RFID que estiverem posicionados nessas regiões estarão efetivamente invisíveis para o leitor, o que pode, obviamente, causar problemas nos sistemas de UHF e de Microondas. Tais regiões de sombra também podem ocorrer com uma desintonização dos tags, que ocorre quando dois tags são colocados em uma distância muito pequena entre si, ou quando são colocados próximos a líquidos, metais e outros materiais com alta permissividade dielétrica. Os sistemas que utilizam UHF e freqüências de Microondas são mais sensíveis a diferenças na orientação das antenas, como mostra a figura 3.23. Antenas indutivas têm pouco ganho direcional, o que significa que a força dos campos em uma dada distância é a mesma acima, abaixo, na frente ou atrás da antena. Já antenas dipolo são mais diretivas, o que significa que em há diferenças na força dos campos em uma dada distância entre os pontos à frente do dipolo e sobre ele. Para tags que usam UHF ou freqüências de Microondas inundarem o leitor, a força do sinal pode não ser suficiente para estabelecer a comunicação. Todos esses problemas requerem que sistemas RFID que usam UHF ou freqüências de Microondas estejam programados com uma modulação mais complexa, chamada *frequency hopping*, para superar tais defeitos [2].

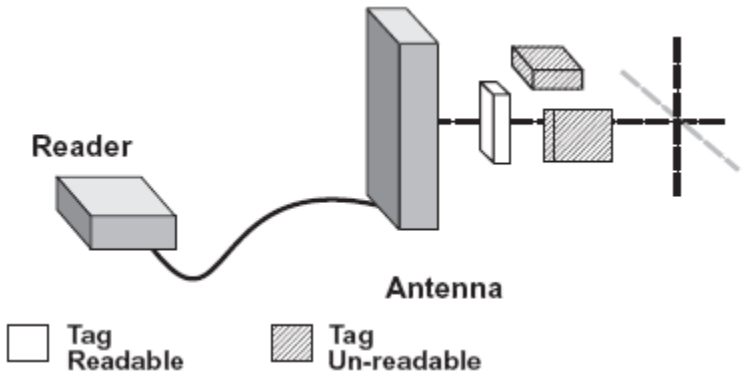

Figura 3.23 – Orientação das antenas [2]

- **Tamanho e preço dos tags:** Os sistemas de RFID atuais usam principalmente a banda LF, devido ao fato dos tags LF serem os mais fáceis de serem fabricados. Todavia, eles têm muitas desvantagens, como o grande tamanho, o que se traduz em um alto preço. Os tags HF são mais baratos de se produzir do que os LF, por isso sistemas RFID que usam a banda HF são, atualmente, os mais utilizados no mundo. A banda UHF representa o que há de mais evoluído em se tratando de RFID. Recentes avanços na tecnologia têm derrubado os preços dos tags UHF a ponto de poderem competir com os tags HF. Já os tags que operam em freqüências de microondas são semelhantes aos tags UHF, no que tange a possibilidade de serem menores e mais baratos.

3.3.1 Low Frequency (LF) – 125kHz & 134kHz

A faixa de freqüências chamada de Low Frequency compreende sinais entre 30kHz e 300kHz. Sistemas RFID normalmente utilizam freqüências entre 125kHz e 134kHz. Um sistema LF RFID típico opera ou em 125kHz ou em 134,2kHz. Sistemas nessa faixa de freqüências geralmente utilizam tags passivos (apesar de ser possível a utilização de tags ativos, devido à maturidade desse tipo de tag), têm baixa taxa de transferência de dados do tag para o leitor, devido à baixa freqüência, e são especialmente bons para quando o ambiente operacional contém metais, líquidos, sujeira, neve ou barro. Atualmente os sistemas LF RFID compreendem a maior parte das aplicações instaladas no mundo, até mesmo porque a faixa de freqüências LF é aceita no mundo todo.

3.3.2 High Frequency (HF) – 13,56MHz

A faixa de freqüências compreendida entre 3MHz e 30MHz é chamada de High Frequency. A freqüência típica utilizada em sistemas de RFID é 13,56MHz. Tais sistemas que utilizam essa freqüência, normalmente, usam tags passivos, tem uma baixa taxa de transferência entre o tag e o leitor e tem um bom desempenho diante de materiais como metais e líquidos. Sistemas HF RFID são amplamente utilizados, principalmente pela faixa de HF ser regulamentada no mundo todo. Suas aplicações englobam várias áreas, mas destaca-se a implantação em hospitais, pois a freqüência de 13,56MHz não interfere no funcionamento dos equipamentos médicos.

3.3.3 Ultra High Frequency (UHF) - 300MHz < f < 1GHz

A faixa de freqüências compreendida entre 300MHz e 1GHz é chamada de Ultra High Frequency, ou, simplesmente, UHF. Sistemas UHF RFID passivos normalmente operam nas freqüências 915MHz, nos Estados Unidos, e 868MHz, na Europa. Já os

sistemas ativos operam, geralmente, em 315MHz e 433MHz. Um sistema UHF RFID pode utilizar tanto tags ativos quanto passivos e tem uma alta taxa de transferência de dados entre o tag e o leitor, mas seu desempenho é fraco quando da proximidade com metais e líquidos, salvo quando se utiliza as freqüências baixas do UHF, como 315MHz e 433MHz. Os sistemas UHF RFID começaram a ser amplamente utilizados por causa do recente incentivo de empresas públicas e privadas, bem como do U.S. Department of Defense. Apesar disso, a banda UHF não é aceita mundialmente para aplicações de RFID [2][1].

3.3.4 Microwaves Frequency – 2,45GHz & 5,8GHz

As freqüências que estão acima de 1GHz são consideradas de microondas [1]. Os sistemas Microwave RFID operam normalmente ou em 2,45GHz ou em 5,8GHz, sendo que a primeira é a mais comum. Tais sistemas podem utilizar tags semi-ativos ou passivos, tendo uma alta taxa de transmissão de dados entre o tag e o leitor, apesar do desempenho diante de materiais como metais e líquidos ser muito fraco. Devido ao comprimento da antena ser inversamente proporcional à freqüência, a antena de um tag passivo operando em freqüências de Microondas tem o seu tamanho extremamente reduzido, o que resulta em um tag muito pequeno, visto que o microchip também tem um tamanho muito pequeno. A freqüência de 2,4GHz também é chamada de *Industry, Science, and Medical (ISM) Band* e é aceita no mundo todo [2].

A tabela 3.5.1 a seguir compara as diversas bandas de operação dos sistemas de RFID:

Tabela 3.5.1 – Bandas de freqüência dos sistemas RFID [2]

Freqüências	**125kHz**	**13,56MHz**	**860-960 MHz**	**>2,5GHz**
Alcance de leitura	<0,6m	<1m	<3-9m	Até 3m
Tipo de tag geralmente utilizado	Passivo	Passivo	Ativo ou Passivo	Ativo ou Passivo
Custo	Alto	Alto-médio	Baixo	Baixo
Aplicações típicas	Controle de acesso, monitoramento animal	Smart Cards	Rastreamento de pallets	Coleta eletrônica de pedágio
Taxa de transmissão de dados	Baixa ----------			Alta
Performance próximo a metais e líquidos	Melhor ----------			Pior

Tamanho do tag passivo	Maior ---------- Menor

Existem restrições internacionais para definir quais as freqüências que podem ser utilizadas nos sistemas de RFID. Logo, algumas das freqüências citadas acima podem não serem válidas no mundo todo. A tabela 3.5.2 a seguir mostra algumas das restrições para as freqüências do RFID, bem como a máxima potência permitida.

Tabela 3.5.2 – Restrições para freqüências do RFID [1]

País / Região	LF	HF	UHF	Freqüências de Microondas
Estados Unidos	125-134kHz	13,56MHz, 10W ERP (Effective Radiated Power)	902-928MHz, 1W ERP ou 4W ERP	2,4-2,4835GHz, 4W ERP 5,725-5,850GHz, 4W ERP
Europa	125-134kHz	13,56MHz	865-865,5MHz, 0,1W ERP 865,6-867,6MHz, 0,2W ERP 867,6-868MHz, 0,5W ERP	2,45GHz
Japão	125-134kHz	13,56MHz	Não permitido. A banda de 950-956MHz está aberta para testes	2,45GHz
Singapura	125-134kHz	13,56MHz	923-925MHz, 2W ERP	2,45GHz
China	125-134kHz	13,56MHz	Não permitido. Futuras possibilidades: 840-843MHz e/ou 917-925MHz. A SAC(Standardization Administration of China) está empenhada em definir as normas para o RFID	2,446-2,454GHz 0,5W ERP

Já a tabela 3.5.3 mostra exemplos das propriedades de alguns materiais diante de ondas de RF. Materiais RF-lucent permitem que as ondas de RF passem por eles, já os RF-opaque e os RF-absorbent não, o que dificulta, mas não impossibilita, a aplicação do RFID em sistemas com objetos que possuam esses materiais.

Tabela 3.5.3 – Propriedades de materiais diante de ondas de RF [1]

Material	LF	HF	UHF	Freqüências de Microondas
Tecidos	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Madeira seca	RF-lucent	RF-lucent	RF-lucent	RF-absorbent
Grafite	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Líquidos (alguns tipos)	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Metais	RF-lucent	RF-lucent	RF-opaque	RF-opaque
Óleo de motor	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Produtos de papel	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Plásticos (alguns tipos)	RF-lucent	RF-lucent	RF-lucent	RF-lucent
Shampoo	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Água	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent
Madeira Úmida	RF-lucent	RF-lucent	RF-absorbent	RF-absorbent

CAPÍTULO 4

Padronização dos sistemas de RFID

O RFID é uma tecnologia de comunicação via rádio, portanto necessita de regulamentação em vários países. A regulamentação governamental no caso do RFID se faz necessária, por exemplo, para organizar o espectro eletromagnético, através da alocação e do licenciamento de segmentos do mesmo para cada tecnologia; para estabelecer as melhores práticas e os níveis de segurança para cada aplicação, protegendo a saúde das pessoas, como, por exemplo, estabelecendo o nível máximo de exposição de uma pessoa à radiação eletromagnética; bem como para definir o máximo permitido de interferência entre bandas de freqüência.

4.1 Órgãos e Normas aplicáveis

O mundo é organizado em três regiões regulatórias, conforme a figura 4.1:

- **Região 1**: Compreende a Europa
- **Região 2:** Compreende as Américas
- **Região 3:** Compreende a Ásia e a Austrália

Figura 4.1 – Regiões regulatórias, segundo o ITU

Como as maiores empresas que lidam com o RFID estão situadas nos Estados Unidos, na Europa e no Japão, os principais órgãos reguladores mundiais estão situados nesses lugares e têm grande influência no futuro da tecnologia de RFID. No Japão o Ministério do Gerenciamento Público, Assuntos Regionais, Correios e Telecomunicações (MPHPT) é quem regula o espectro de freqüências. Nos Estados Unidos o FCC (Federal Communications Commission) é quem executa essa tarefa. Já na Europa cada país tem seu próprio órgão regulador. Porém a maioria delas está unida

em duas organizações – a European Radiocommunications Commitee (ERO) e o European Telecommunications Standards Institute (ETSI)-, através das quais as responsabilidades são divididas, e ambas estão ligadas à Conferência Européia de Administração de Correios e Telecomunicações (CEPT) [2].

Os principais órgãos reguladores mundiais são citados na tabela 3.6.1 a seguir:

Tabela 3.6.1 – Órgãos reguladores

Organização	***Função***
International Telecommunication Union (ITU)	É uma organização internacional estabelecida para padronizar e regular mundialmente o rádio e as telecomunicações. Para o RFID ela divide o mundo em três regiões regulatórias.
European Telecommunications Standards Institute (ESTI), criado pela *European Conference of Postal and Telecommunications* (CEPT)	Regula o RFID na Europa
Federal Communications Commission (FCC)	Regula o RFID nos Estados Unidos
Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT)	Regula o RFID no Japão
Office of the Telecommunications Authority (OFTA)	Regula o RFID em Hong Kong
Standardization Administration of China (SAC)	Regula o RFID na China
EPCglobal	Desenvolve padrões para a rede EPCGlobal
International Organization for Standardization (ISO)	Desenvolve padrões para o RFID e para algumas outras aplicações
Agência Nacional de Telecomunicações (ANATEL)	Regulamenta o uso das freqüências, bem como certifica e homologa todos os produtos que podem ser utilizados no Brasil

Muitos dos sistemas RFID são projetados para utilizarem as bandas ISM (Industrial-Scientific-Medical). Inicialmente criadas para o uso não-comercial industrial, científico e médico, elas vêm sendo utilizadas em várias aplicações comerciais, como em WLANs, Bluetooth e nos próprios sistemas de RFID. Sendo assim, quem usa essas bandas de freqüências pula as etapas licenciatórias, que seriam obrigados a passar se utilizassem outra banda, visto que as ISM não são reguladas [2].

Entretanto, como mencionado anteriormente no trabalho, a maioria dos sistemas RFID utiliza as bandas LF, HF, UHF e as freqüências de Microondas. A alocação no espectro dessas bandas não é a mesma no mundo todo. Entre Estados Unidos, Japão, Europa e China existem várias diferenças com relação a esta alocação.

- A banda LF (125kHz – 134kHz) está disponível para uso nos EUA, na Europa e no Japão. O RFID compartilha essa banda com aplicações de navegação da aeronáutica e da marinha.

- A banda HF (13,56MHz) também está disponível para uso nos EUA, na Europa e no Japão, com níveis muito semelhantes de potência.

- Já para a banda UHF há várias diferenças na regulação nos EUA, na Europa e no Japão. No momento o foco das atenções está nessa banda, visto que as principais aplicações em RFID que têm surgido utilizam freqüências nessa faixa.

- As freqüências de Microondas estão disponíveis em muitos lugares, porém com muitas divergências com relação às regulamentações. Por exemplo, o limite de potência transmitida, em vários lugares, é de 4W, entretanto, no Japão é de apenas 1W [2].

Padrões ISO

O ISO é uma organização padronizadora internacional, composta por representantes de organizações padronizadoras nacionais. Fundada em 1947, a ISO define padrões industriais e comerciais no mundo todo. A ISO desenvolveu padrões para o RFID nas seguintes áreas:

- Padrões de identificação relacionados à codificação do *ID Number* ou outras informações contidas nos tags

- Protocolos de interface aérea que definem as regras de comunicação entre tags e leitores

- Protocolos de dados para o *middleware*

- Padrões para testes, tendências e segurança [4]

Alguns dos padrões desenvolvidos pela ISO para aplicações RFID estão na tabela 3.6.2 a seguir:

Tabela 3.6.2 – Padrões ISO para RFID

Padrão ISO	***Descrição***
ISO/IEC 15961	Troca de informações em um sistema RFID para gerenciamento de itens (Protocolo de dados para interface de aplicação)
ISO/IEC 15962	Regras de codificação dos dados e de funções para memória lógica, para gerenciamento de itens
ISO/IEC 15963	Identificação única para tags RFID
ISO/IEC 18000-*i*	Parâmetros para interface de comunicação aérea em diferentes freqüências de operação
ISO/IEC 18047-*i*	Métodos de teste de equipamentos RFID para diferentes freqüências de operação
ISO/IEC 19762-3	Vocabulário para técnicas de Identificação Automática e Captura de Dados (AIDC)
ISO/IEC 24730-1	Application Program Interface (API) para sistemas de RTLS (Real-Time Locating Systems)

*O valor da variável **i** depende da freqüência de operação do sistema.*

Os protocolos de interface aérea definem as regras para comunicação entre leitores e tags. Isto inclui regras sobre:

- Codificação dos dados, modulação e demodulação
- Comandos de comunicação para executar operações no tag, como leitura, escrita, modificação dos dados, bloqueio das informações, bem como para destruir o tag.
- Algoritmos anti-colisão

A ISO também desenvolveu padrões para as aplicações do RFID, como:

- **Rastreamento Animal (Utilizando a banda LF):** A ISO desenvolveu dois padrões para esse fim: o ISO 11784 e o ISO 11785. O ISO 11784 define a estrutura do código pra tags utilizados em animais. Os animais podem ser identificados pelo código do

país e um único ID nacional. O ISO 11785 define os parâmetros técnicos para a comunicação entre tag e leitores

- **Cartões de identificação e dispositivos relacionados (Utilizando a banda HF):** Foram desenvolvidos três padrões para tal fim: o ISO 10536, o ISO 14443 e o ISO 15693. Esses são os padrões ISO mais utilizados atualmente, entretanto, são aplicáveis apenas a sistemas HF RFID.

  O ISO 10536 define os parâmetros para *contactless smart cards*, com alcance de leitura de 7-15cm, utilizando 13,56MHz. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca das dimensões e da localização das áreas de acoplamento; a parte 3, acerca dos sinais eletrônicos e dos procedimentos de *reset* do cartão; e a parte 4, acerca da resposta ao *reset* e dos protocolos de transmissão.

  O ISO 14443 é aplicado a *proximity smart cards*. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca da potência e da interface dos sinais; a parte 3, acerca da inicialização e do sistema anti-colisão; e a parte 4, acerca dos protocolos de transmissão.

  O ISO 15693 é aplicado a *vicinity smart cards*. Esse padrão está dividido em quatro partes. A parte 1 versa acerca das características físicas do cartão; a parte 2, acerca da inicialização e da interface aérea; a parte 3, acerca dos protocolos; e a parte 4, acerca dos comandos e de funções de segurança.

- **RFID AIDC (Automatic Identification and Data Capture) e Tecnologias de Gerenciamento de Itens:** Para essas aplicações foram desenvolvidos os padrões ISO 15961, o ISO 15962, o ISO 15963, o ISO 18000 e o ISO 18001.

  O ISO 15961 define padrões para a interface de aplicação e para os protocolos de dados. O ISO 15962 define especificações para regras de codificação, funções de memória e protocolos de dados. O ISO 15963 define um sistema de numeração único para os tags. O ISO 18000 está dividido em sete partes, conforme a tabela 3.6.3. O ISO 18001 define padrões para a tecnologia de endereçamento de informações.

Tabela 3.6.3 – Divisão da norma ISO 18000 [9]

Parte 1	Parâmetros genéricos para interface de comunicação aérea, para todas as freqüências aceitas mundialmente
Parte 2	Parâmetros para interface de comunicação aérea em 125kHz
Parte 3	Parâmetros para interface de comunicação aérea em 13,56MHz

Parte 4	Parâmetros para interface de comunicação aérea em 2,45GHz
Parte 5	Parâmetros para interface de comunicação aérea em 5,8GHz
Parte 6	Parâmetros para interface de comunicação aérea em 860-930MHz
Parte 7	Parâmetros para interface de comunicação aérea em 433MHz

A ISO determina padrões para várias outras áreas. Mas a tecnologia RFID possui um órgão padronizador específico: a EPCglobal. A EPCglobal Inc. é uma joint-venture entre a GS1 (formalmente conhecida como EAN International) e a GS1 US (formalmente conhecido como Uniform Code Council Inc.). A organização EPCglobal foi criada para conseguir a adoção e a padronização da tecnologia EPC no mundo inteiro, de uma forma ética e responsável. A EPCglobal desenvolveu um padrão, aprovado em dezembro de 2004, que pode revolucionar a tecnologia RFID: o EPCglobal Gen 2 (popularmente chamado de Gen 2). Esse padrão é, provavelmente, a forma de avançar no sentido de obter uma padronização dos tags RFID, que é um dos principais problemas atualmente [4].

4.2 EPCglobal Network

O Auto-ID Center, situado no Massachusetts Institute of Technology (MIT), trabalhando em conjunto com líderes da indústria e instituições acadêmicas de várias partes do mundo, desenvolveu um sistema para trazer os benefícios do RFID para a cadeia mundial de suprimentos. Esse sistema compreende o Electronic Product Code (EPC), tecnologia RFID e o software de suporte baseado nos padrões EPCglobal. Esse sistema é conhecido como *EPCglobal Network*. A *EPCglobal Network* é composta, basicamente, por quatro componentes: um objeto com uma etiqueta EPC, um computador rodando Savant, um servidor ONS (Object Name Service) e um servidor PML (Product Markup Language). O computador *Savant* e os servidores ONS e PML são conectados à internet e situados bem distantes uns dos outros. A figura 4.2 ilustra o funcionamento da *EPCglobal Network*.

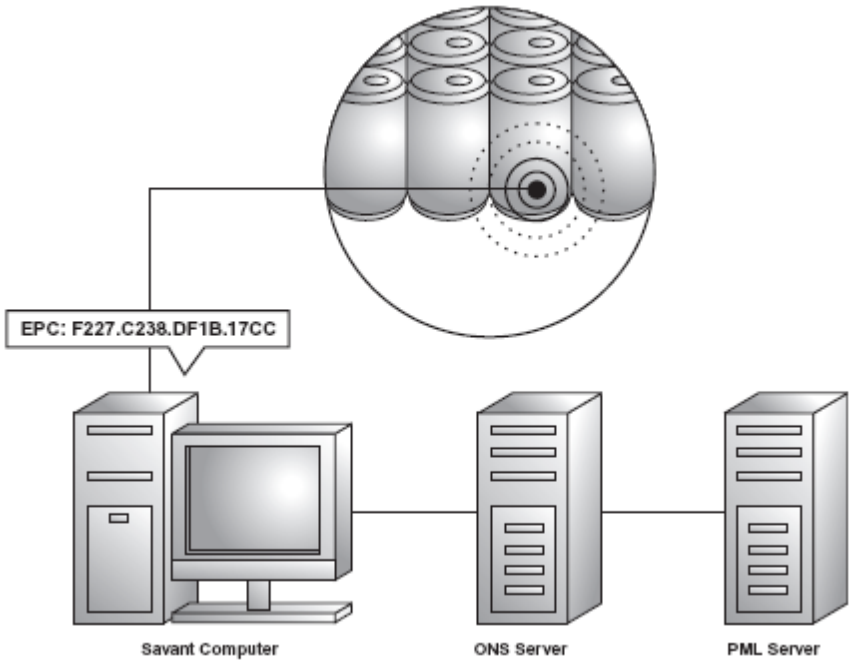

Figura 4.2 – Funcionamento da *EPCglobal Network* [2]

Em um objeto, como uma lata de refrigerante, é colocada uma etiqueta EPC. Essa etiqueta grava um número, um identificador único, que indica qual o fabricante da lata de refrigerante, bem como um número de série para cada lata em particular. O computador *Savant*, que é, necessariamente, uma rede de leitores e um cliente rodando uma aplicação ou um software, lê a etiqueta EPC na embalagem. Esse processo pode ocorrer em qualquer local da cadeia de suprimentos. Vários computadores *Savant* e leitores podem ser instalados na fábrica, em centros de distribuição, em mercearias ou em grandes redes de varejo. Vamos assumir que esse computador *Savant* esteja instalado em um varejista. Uma vez que ele tenha lido a etiqueta EPC da lata, ele fornece o número dela para o servidor ONS, que atua como o inverso de uma lista telefônica. Ele pega o número EPC e fornece o nome e o endereço da empresa que fabricou a lata de refrigerante, enviando, então, esses dados de volta ao computador *Savant*. O computador *Savant* pode usar esses dados para contatar diretamente o servidor PML da empresa. Se todas as empresas tiverem um site e um servidor web na *EPCglobal Network*, todas elas terão um site PML e um servidor PML. Supondo que o fabricante da lata de refrigerante seja a empresa Soda. O computador *Savant* no varejista irá contatar o servidor PML da Soda, com o número de série único da lata de refrigerante. O servidor PML da Soda, por sua vez, deve conter todos os tipos de informação acerca daquela lata em particular, como a data e o local de fabricação, se o produto foi ou não passado por um *recall*, por quais lugares ele passou ao longo da cadeia de distribuição, etc. O computador *Savant* deve consultar essas informações para estar certo de que a lata de refrigerante está apropriada para venda. Além disso, se ela for a última lata de Soda na prateleira, o computador *Savant* deve solicitar mais produtos. Tudo isso pode ser feito com pouca ou sem qualquer intervenção humana. Esse é, basicamente, o funcionamento da *EPCglobal Network* [2].

A *EPCglobal* está desenvolvendo padrões e especificações para os seguintes componentes da *EPCglobal Network*:

- Especificações dos dados de um tag EPC
- Interface de comunicação para sistema HF e UHF
- Protocolos de leitura
- Savant
- ONS (Object Name Service)
- PML (Physical Markup Language)

4.3 EPC (Electronic Product Code)

4.3.1 Descrição

EPC é uma família de esquemas de códigos para tags. Ele foi projetado para sanar as necessidades de várias indústrias, enquanto, ao mesmo tempo, garante singularidade para todos os tags compatíveis com o EPC, chamados *EPC tags*.

4.3.2 Características

Os esquemas dos códigos do EPC tipicamente contêm um número serial único, chamado de *EPC number*, que pode ser utilizado para identificar um objeto. O *EPC number* é estruturado em quatro partes, conforme a figura 4.3.

A primeira parte é o cabeçalho, composta por 8 bits. O cabeçalho serve para que se identifique o comprimento, o tipo, a estrutura, a versão e a geração do EPC. No caso da lata de refrigerante, citada anteriormente, estaria, por exemplo, a versão do EPC.

A segunda parte é o *EPC Manager*, composta por 28 bits. Ela serve para que se identifique o "manager", que, normalmente, é o fabricante do produto. Novamente fazendo a analogia com a lata de refrigerante, o *EPC Manager* seria "Soda".

A terceira parte é o Object Class, composto por 24 bits. Ela serve para identificar precisamente o tipo de produto. Continuando a analogia com o caso da lata, o Object Class seria, por exemplo, Soda Diet, 350ml, U.S. version.

A quarta e última parte do *EPC Number* identifica o número de série do produto. No caso, seria o número de série da lata de Soda na qual o tag está colocado.

Existem duas versões de tags: uma versão que possui uma memória de 64 bits e outra, que possui uma memória de 96 bits. Tags com maior capacidade de memória podem até serem utilizados, mas 96 bits já tem se mostrado suficiente para as atuais necessidades mundiais. Um tag de 96 bits, como o mostrado na figura 4.3, com 28 bits para o *Manager Number*, 24 bits para o *Object Class* e 36 bits para o *Serial Number*, podem identificar 268 milhões de empresas diferentes, cada uma delas tendo mais de 16 milhões de produtos diversos e 68 milhões de números de série para cada tipo de produto. Esse números são mais do que suficientes para cobrir todos os fabricantes mundiais, durante muitos anos. Os tags de 64 bits foram desenvolvidos para preencher uma necessidade da indústria de produtos mais baratos, visto que tais tags possuem um custo de produção muito mais barato do que os tags de 96 bits, e para colaborar com a manutenção do custo inicial da implantação baixo [2].

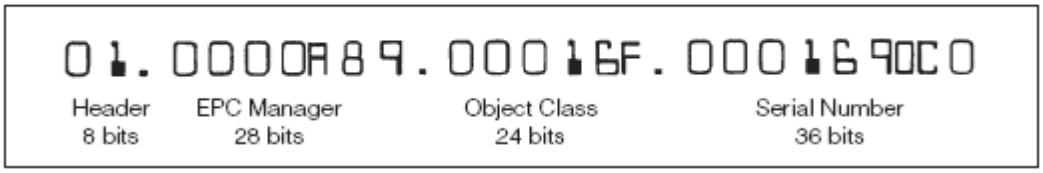

Figura 4.3 - EPC (*Electronic Product Code*) Tipo 1 [2]

4.3.3 Classificação

Além das versões em 64 bits e em 96 bits, os *EPC tags* são divididos também em classes, de acordo com a sua funcionalidade, ou se possui ou não, alimentação própria. A figura 4.4 ilustra as classes dos *EPC tags*.

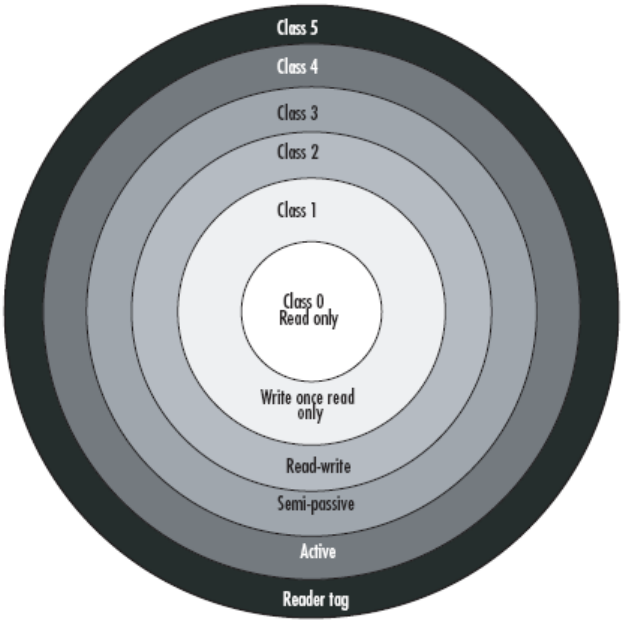

Figura 4.4 – Classes dos *EPC tags* [4]

As principais características de cada classe estão mostradas na tabela 3.6.4.

Tabela 3.6.4 - Características das classes do EPC

Classe do tag	***Tipo***	***Memória***	***Comunicação***	***Propriedades***
Classe 0	Passivo	Read-Only	Não inicia comunicação	*EPC Number* é programado durante o processo de fabricação
Classe 0+	Passivo	Write-Once-Read-Many	Não inicia comunicação	Programado uma única vez, pelo usuário final, utilizando o mesmo protocolo da Classe 0

Classe 1	Passivo	Write-Once-Read-Many	Não inicia comunicação	*EPC Number* é programado pelo usuário final
Classe 2	Passivo	Write-Once-Read-Many	Não inicia comunicação	Codificação
Classe 3	Semi-Passivo	Re-Writable	Não inicia comunicação	Capacidades dos Classe 2 mais extras, como sensores integrados
Classe 4	Ativo	Re-Writable	Pode iniciar comunicação; alimenta sua própria comunicação; é possível uma comunicação tag-to-tag	Capacidades dos Classe 3 mais extras
Classe 5	Ativo	Re-Writable	Pode iniciar comunicação; alimenta sua própria comunicação; é possível uma comunicação tag-to-tag	Capacidades dos Classe 4 mais extras

4.3.4 Futuro do EPC

Deve-se notar que os tags EPC não comportam muito mais dados do que símbolos de códigos de barra UPC. Alguns argumentam que o EPC não tira total vantagem dos benefícios oferecidos pela tecnologia de RFID. A EPCglobal argumenta que esse projeto serve para que se tenha um tag EPC de baixo custo. Agora existe a segunda geração das etiquetas EPC, conhecida como Generation 2, ou simplesmente Gen 2, considerando-se que a anterior era a EPC Gen 1. A estrutura de classes dos tags, a princípio, permanecerá no Gen 2, entretanto as funcionalidades dos mesmos serão aumentadas. Esse remanejamento é motivado, em parte, pelo Wal-Mart, DoD (US Department of Defense) e outros grandes *players* do mercado, para que hajam estruturas de dados mais flexíveis e seções de memória regraváveis, ao contrário dos números de produtos estáticos existentes na Gen 1. O padrão Gen 2 foi publicado e adotado pela ISO e suas implantações pertencem em sua maioria à banda UHF. A tabela 3.6.5 compara algumas características dos padrões EPC Gen1 e EPC Gen2.

Tabela 3.6.5 – Comparação entre EPC Gen1 e EPC Gen2

Característica	*Generation 1*	*Generation 2*
Freqüência de operação	860-930MHz	860-960MHz
Capacidade de memória	64 ou 96 bits	96-256 bits
Outras características	-	Leitura mais veloz e confiável do que no Gen1

4.4 Importância da padronização para o desenvolvimento da tecnologia

A padronização de produtos é muito importante para o desenvolvimento de uma tecnologia. Através dela, todos os vendedores seguirão o mesmo padrão para fabricar equipamentos, o que traz uma padronização técnica, que permite a interoperabilidade dos equipamentos. Isso beneficia os consumidores e ajuda os vendedores a desenvolver uma competição mais sadia. Outro importante ponto a ser tocado é que devido aos órgãos padronizadores não estarem seguindo os interesses de determinada empresa, a padronização, geralmente, define uma plataforma mais eficiente para que as indústrias do mercado possam operar e avançar [4].

A criação de padrões também leva aos consumidores uma maior confiabilidade em uma determinada tecnologia, bem como, geralmente, reduz os custos da mesma e facilita a implementação.

4.5 Vantagens e Desvantagens

Regulamentações e padronizações dos sistemas de RFID têm influenciado diretamente no mercado, em várias áreas, incluindo em operações comerciais e na infra-estrutura de TI. Essa influência traz consigo as vantagens e as desvantagens, apesar das primeiras serem, normalmente, muito maiores do que as desvantagens.

Uma das principais vantagens das regulamentações e das padronizações do RFID é que, por exemplo, as regulamentações estabelecem limites com relação à radiação eletromagnética emitida, fazendo, assim, com que diminua o risco de problemas causados pelo excesso de radiação, visto que os limites tem de ser atendidos. As regulamentações também estruturam o mercado para que haja uma competição sadia,

já que evitam a concorrência desleal, onde as empresas colocam vantagens em seus produtos que acarretam, por exemplo, em danos aos usuários (como é o caso de uma exposição à altas taxas de radiação eletromagnética). Assim, as regulamentações fazem com que as empresas produzam produtos diferenciados através de preços mais vantajosos, ou melhores características, ou, ainda, a prestação de serviços aos consumidores. Também pode se observar do ponto de vista de que as regulamentações possibilitam avanços na tecnologia, devido, principalmente, à maior facilidade à entrada de novas empresas no segmento, promovendo, da mesma forma, o empreendedorismo, que pode leva ao desenvolvimento de novidades no setor direta, ou indiretamente. As padronizações do RFID são muito vantajosas, pois, considerando-se que todos os dispositivos serão produzidos seguindo os mesmos padrões, eles se tornarão interoperáveis entre si, o que trará benefícios aos consumidores e, também, aos vendedores. Outra vantagem é que eles tendem a reduzir o custo das aplicações e facilitar a implementação, bem como tendem a desenvolver nos consumidores uma maior confiança na tecnologia.

Uma das desvantagens das regulamentações e das padronizações do RFID está relacionada com a diminuição do alcance de leitura dos tags, devido à imposição de limites de potência emitida. Essa desvantagem afeta principalmente as aplicações com tags passivos, tendo em vista que esses necessitam da energia provinda do leitor para energizar seu circuito. Logo, se a potência emitida pelo leitor é limitada em um valor mais baixo, o alcance da leitura de tal tag será diminuída. As regulamentações também influenciam negativamente no que diz respeito às freqüências de operação, já que, devido à diferença entre as regiões do planeta, um determinado equipamento RFID que funciona em uma dada região, pode não funcionar em outra.

CAPÍTULO 5

Comparação com outra tecnologia de identificação: BarCode (Código de Barras)

Um código de barras é um esquema no qual símbolos impressos representam informações. Tais símbolos geralmente são compostos de barras verticais, espaços, retângulos e pontos. Um método que codifica caracteres alfanuméricos usando esses símbolos é chamado de simbologia. Duas simbologias podem usar os mesmos ou diferentes símbolos para codificar um mesmo caractere. Em torno de 270 simbologias diferentes foram inventadas para suportar requisitos específicos e, aproximadamente, 50 são amplamente utilizadas hoje. As simbologias são classificadas em: linear, bi-dimensional e tri-dimensional.

A simbologia linear consiste em linhas verticais, com diferentes larguras e com espaços em branco separando duas linhas adjacentes. O número máximo de caracteres que pode ser codificado com uma simbologia linear é 50.

A simbologia bi-dimensional tem a maior capacidade de armazenamento de dados. O número máximo de caracteres que podem ser codificados com a simbologia de código de barras bi-dimensional é 3750.

Uma simbologia tri-dimensional é um código de barras em alto-relevo impresso em uma superfície. Um código de barras tridimensional não depende, assim, do contraste entre as linhas do código de barras e seus espaços para que a leitura seja efetuada. Este tipo de código de barras pode ser sujeito a condições adversas do ambiente, enquanto um papel com um código de barras impresso, em situações ambientais semelhantes, pode ser facilmente destruído.

Leitores

O princípio de funcionamento de um leitor de código de barras, também chamados *scanner*, é através de um feixe de luz, conforme a figura 5.1. A direção do escaneamento é irrelevante, entretanto, durante a leitura, o feixe de luz não pode se mover para fora da região onde está o código de barras. Logo, geralmente, quanto maior o comprimento do código de barras, menor tem de ser a distância do leitor para que o escaneamento seja efetuado corretamente. Durante o processo de leitura o *scanner* mede a intensidade da luz refletida pelas regiões pretas e brancas, no caso de barras verticais. As barras pretas absorvem a luz, enquanto que as brancas, ou os espaços, refletem a luz. Um dispositivo eletrônico chamado fotodiodo, ou fotocélula, traduz esse padrão luminoso em uma corrente elétrica, ou em um sinal analógico. Circuitos elétricos, então, decodificam essa corrente em dados digitais (caracteres ASCII), dados esses que foram originalmente codificados pelo código de barras.

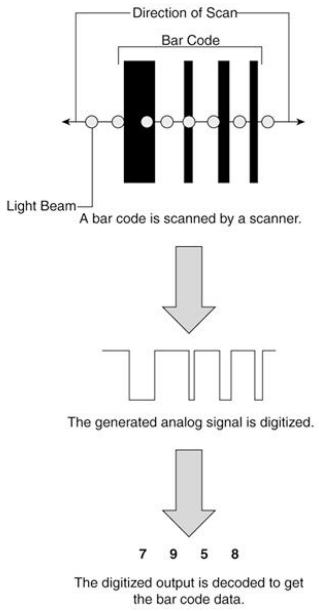

Figura 5.1 – Funcionamento de um leitor de código de barras [1]

Alguns dos tipos de leitores são as canetas, os à *laser*, os CCD (Charged Coupled Device) e as câmeras.

O leitor tipo caneta, mostrado na figura 5.2, é o mais barato e o mais leve, devido à não-existência de partes móveis (o usuário efetua a leitura manualmente). Por sua pequena área de leitura, o código de barras necessita estar em contato com o leitor durante todo o processo de escaneamento. Outra desvantagem desse tipo de leitor é mostrada quando um código de barras é colocado em um objeto rugoso. Devido à necessidade do total contato entre o leitor e o código, se a superfície não é suficientemente plana o leitor pode não capturar os dados corretamente [1].

Figura 5.2 – Leitor de código de barras, tipo caneta [1]

O leitor à *laser*, mostrado na figura 5.3, é o mais utilizado. Um *laser* localizado dentro do leitor automaticamente escaneia o código de barras. Uma das vantagens desse tipo de leitor é a sua capacidade de ler um código de barras mesmo se ele não estiver em

uma superfície lisa. Ele consegue isso porque é possível focar seu feixe de luz em um ponto muito pequeno. Com isso, geralmente, apenas um escaneamento é necessário para ler um código de barras. Portanto, esse tipo de leitor pode ler códigos de barra a uma alta taxa, mesmo que o código esteja com uma má qualidade. Esse leitor é freqüentemente utilizado em indústrias, onde um objeto que possua um código de barras se move a uma velocidade constante. A distância máxima de leitura para um leitor à *laser* é em torno de 9m [1].

Figura 5.3 – Leitor de código de barras, à *laser* [1]

O leitor CCD, mostrado na figura 5.4, pode ler um código de barras sem ter contato com o produto, mas a uma distância próxima. Seu princípio de funcionamento é baseado em uma matriz de centenas de pequenos sensores de luz que está localizada na frente do leitor. Quando a imagem do código de barras é projetada nestes sensores, eles geram um padrão de voltagem. Esse padrão é idêntico ao padrão gerado pelo leitor à *laser*. Alguns desses sistemas utilizam fontes adicionais de luz, como um flash, para aumentar a distância focal. A máxima distância de leitura para esse tipo de leitor, e essa é sua principal desvantagem, é algo em torno de 15 cm, devido ao seu limitado campo de visão. O número de sensores luminosos no leitor é que determina o contraste mínimo necessário para que a leitura seja efetuada [1].

Figura 5.4 – Leitor de código de barras, CCD [1]

Os leitores do tipo câmera, como o mostrado na figura 5.5, são os resultados dos últimos avanços na tecnologia do código de barras. Uma pequena câmera dentro do leitor captura a imagem do código de barras. Essa imagem é, então, processada usando

tecnologia de processamento de imagens digital para determinar o conteúdo do código de barras. Uma desvantagem desse tipo de leitor é que ele é muito sensível quanto à qualidade do código de barras. Ou seja, um contraste insuficiente entre os símbolos brancos e pretos ou um espaço vazio podem comprometer a leitura. O leitor tipo câmera vêm se tornando cada vez mais barato, menor e mais veloz. Com isso, um grande número de usuários está substituindo seus *scanners* à laser pelos do tipo câmera [1].

Figura 5.5 – Leitor de código de barras, tipo câmera [1]

Simbologias de BarCode Lineares

- ***UPC (Uniform Product Code)***

O UPC , *Uniform Product Code*, é uma simbologia de código de barras dirigido pelo UCC, *Uniform Code Council*. Os dois maiores tipos de UPC são o UPC-A e o UPC-E.

O UPC-A consiste de 12 dígitos, dos quais o último é utilizado com um dígito de checagem; o primeiro representa o tipo do produto; os próximos cinco dígitos, o código do fabricante; e os cinco dígitos subseqüentes identificam o produto atual. Essa simbologia é a que é amplamente utilizada nas redes de varejo.

O UPC-E, mostrado na figura 5.6, consiste de sete dígitos, dos quais um é usado como dígito de checagem. Essa simbologia também é chamada de UPC com zeros suprimidos, porque ele pode comprimir um código UPC-A em um código de seis dígitos, suprimindo os zeros para o código do fabricante e controlando os zeros do produto atual. O sétimo dígito é usado como um dígito de checagem para os primeiros seis. Sendo assim, o UPC-E sempre pode ser convertido de volta a um UPC-A. Essa simbologia é utilizada em pequenos varejistas.

Tanto o UPC-A, quanto o UPC-E podem ser acrescidos de um código de dois ou cinco dígitos, conforme as figuras 5.7 e 5.8. Normalmente as publicações ou os periódicos contém esse acréscimo.

Figura 5.6 – Exemplo de código de barras UPC-E [1]

Figura 5.7 – Exemplo de código de barras UPC-A +2 [1]

Figura 5.8 – Exemplo de código de barras UPC-E +5 [1]

- ***EAN (European Article Numbering)***

O EAN, *European Article Numbering*, é a versão européia do UPC. Os dois principais tipos do EAN são o EAN-13, mostrado na figura 5.9, e o EAN-8, mostrado na figura 5.10.

Figura 5.9 – Exemplo de código de barras EAN-13 [1]

Figura 5.10 – Exemplo de código de barras EAN-8 [1]

O EAN-13 é a simbologia européia equivalente ao UPC-A. Comparado ao UPC-A, um símbolo EAN-13 contém um dígito adicional, que, juntamente com o vigésimo dígito, representa o código do país. Essa simbologia é muito utilizada nas publicações, para representar os números ISBN dos livros. Um código ISBN é um código de barras EAN-13 com os três primeiros dígitos sendo 978 e os demais nove dígitos representando os primeiros nove dígitos do número ISBN [1].

O EAN-8 consiste de oito dígitos, dos quais os dois primeiros são utilizados para o código do país. Os próximos cinco dígitos são usados para dados e o último, como dígito de checagem.

Da mesma forma que no UPC, o código EAN também pode ser acrescido de mais dois ou cinco dígitos, tanto no EAN-13, como no EAN-8. Quem utiliza esse acréscimo são, assim como no UPC, os periódicos e as publicações. Nos códigos ISBN, esses números suplementares começam com 5, sendo que os quatro dígitos restantes são utilizados para codificar o preço do livro.

Também há outras simbologias, como a simbologia linear *Code 128*, que utiliza letras e números, mostrado na figura 5.11, e as bi-dimensionais PDF417, que consiste de pequenos códigos de barra sobrepostos podendo representar até 2525 caracteres,

mostrado na figura 5.12, *Aztec Code*, que é formado por vários blocos e pode representar até 3750 caracteres, como mostrado na figura 5.13, e *DataMatrix*, que pode codificar até 3116 caracteres, mostrado na figura 5.14.

Figura 5.11 – Exemplo de código de barras *Code 128* [1]

Figura 5.12 – Exemplo de código de barras *PDF417* [1]

Figura 5.13 – Exemplo de código de barras *Aztec Code* [1]

Figura 5.14 – Exemplo de código de barras *DataMatrix* [1]

Cada uma das soluções, tanto RFID, quanto BarCode, tem seus prós e contras. As vantagens que o BarCode tem sobre os sistemas de RFID são:

- **Baixo custo:** O custo de implementação de uma solução de BarCode é, geralmente, muito menor do que o de uma solução equivalente utilizando RFID

- **Precisão:** Em alguns casos, a precisão da leitura em uma solução de BarCode é a mesma, se não maior, do que em uma equivalente de RFID. Os sistemas de código de barras possuem precisões de leitura em torno de 95%, enquanto que no RFID chega-se a 80%

- **Independe do material:** Um sistema de código de barras pode ser utilizado com sucesso em qualquer tipo de material, ao contrário do RFID, que tem problemas com a leitura em materiais metálicos ou em embalagens que contenham líquidos

- **Maturidade:** A tecnologia de BarCode existe há mais de 30 anos, sendo, provavelmente, a tecnologia mais amplamente empregada no mundo. Durante esse tempo, mais de 50 padrões foram desenvolvidos, dentre esses, alguns que tem aceitação mundial

Já as vantagens do RFID com relação ao BarCode são:

- **Dinamismo:** Os dados de um tag RFID podem ser reescritos em torno de 10.000 vezes (assumindo um tag RW). Já os dados em um código de barras são inalteráveis; cada vez que se fizer necessário alterar algum dado, um novo código de barras precisará ser gerado

- **Linha de visada:** Normalmente um leitor RFID não precisa de uma linha de visada para ler os dados contidos em um tag. Já os leitores de código de barras sempre precisam de uma linha de visada para efetuar a leitura corretamente

- **Alcance de leitura:** Um tag RFID pode ter uma distância de leitura muito maior do que a de um BarCode. Dependendo de alguns fatores, esse alcalce vai de alguns centímetros a centenas de metros

- **Memória:** Um tag RFID pode armazenar muito mais informações do que um código de barras

- **Múltiplas leituras:** Um leitor de RFID pode ler um número muito grande de tags de uma só vez. Um leitor de código de barras, entretanto, lê um código por vez

- **Durabilidade:** Um tag RFID, geralmente, é robusto, resistindo à condições adversas do ambiente. Já o código de barras é facilmente danificado, por exemplo, por sujeira

- **Duplicidade:** Um tag RFID é muito mais difícil de ser duplicado, quando comparado a códigos de barras

Também existem as desvantagens que são comuns aos dois sistemas. Duas das principais são:

- **Presença de obstáculos:** Conforme dito anteriormente, um leitor de código de barras precisa de uma linha de visada para efetuar a leitura corretamente. Portanto, se houver qualquer tipo de obstáculo entre o leitor e o código de barras, a leitura não é feita. No caso do RFID, dependendo da freqüência utilizada e alguns outros fatores, como a potência transmitida, um leitor pode não estar apto a ler um tag, caso haja, entre o leitor e o tag, materiais *RF-opaque*, como o metal, ou *RF-absorbent*, como a água

- **Presença de umidade:** Para os leitores de código de barras, a presença de partículas de água no ambiente podem provocar a distorção da luz necessária para efetuar a leitura, através da refração. Para o caso dos leitores de RFID operando em UHF ou em freqüências de Microondas, as partículas de água podem absover a energia RF, resultando em energia insuficiente para atingir os tags para que a transferência de dados seja efetuada

CAPÍTULO 6

RFID – Aplicações onde seu uso significa vantagem competitiva

6.1 Transporte Urbano

O transporte urbano é um dos setores onde existe grande aplicabilidade dos sistemas de RFID, particularmente de *contactless smart cards*. Muitas empresas de transporte ainda operam com altos custos operacionais. Devido à redução dos recursos financeiros, há a necessidade de adotar soluções que reduzam tais custos. O uso dos *contactless smart cards* como sistema de passe eletrônico, também chamado de bilhetagem eletrônica, contribui muito para essa situação, além de contribuir com o conforto e a agilidade do sistema de transporte.

Esse tipo de aplicação se baseia, sinteticamente, na substituição dos bilhetes de papel por um *contactless smart card* e na instalação de um leitor no ônibus, metrô ou trem. Esse *smart card* porta informações do usuário, como informações pessoais, e armazena os créditos que são convertidos em passagens. Um problema crítico nos sistemas de bilhetagem eletrônica é o tempo tomado para aquisição dos créditos ou para a verificação do cartão, principalmente quando se trata da bilhetagem em ônibus e trens, onde a checagem do cartão e a passagem só podem ser efetuadas dentro do veículo. Apesar disso, as soluções utilizando RFID, como as com *contactless smart card* levam ampla vantagem quando comparadas a outros sistemas. A tabela 4.1 mostra os tempos de processamento, aproximados, para diferentes tecnologias.

Tabela 4.1 - Tempos de processamento para diferentes tecnologias [10]

Tecnologia	***Tempo de processamento (s)***
RFID (*Contactless Smart Card*)	1,7
Verificação visual pelo cobrador	2
Smart Cards com contato	3,5
Dinheiro	>6

O funcionamento do sistema de transporte urbano é descrito pela figura 6.1, a seguir:

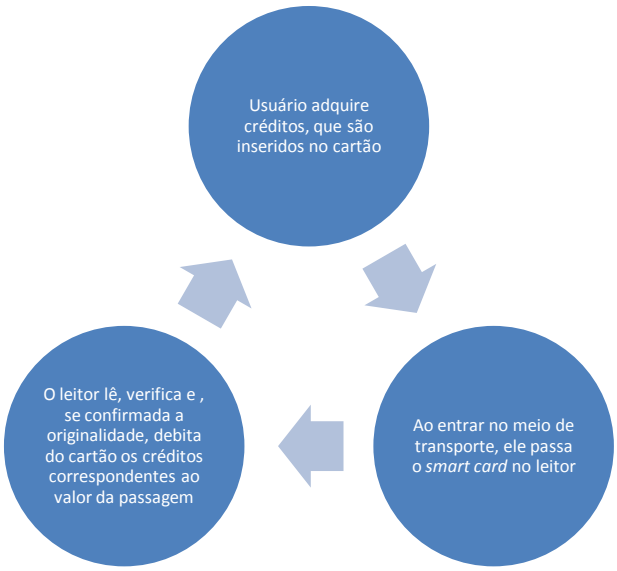

Figura 6.1 – Funcionamento do sistema de transporte urbano

Alguns pontos importantes a se destacar nesta solução são a segurança da informação contida no cartão, que está criptografada através de algoritmos como o 3DES, AES e RSA, a portabilidade do cartão, visto que seu tamanho é semelhante ao de um cartão de crédito, a dificuldade de se falsificar um *smart card* e a resistência tanto do leitor, quanto do cartão, já que este último é projetado para uma vida útil de mais de 10 anos, resistindo à umidade, ao frio, à areia e à sujeira.

Sendo assim, há poucas desvantagens ao se implantar um sistema de bilhetagem eletrônica. O principal é o custo da solução, que é elevado quando comparado com o tradicional sistema de bilhetes. Porém, esse custo é rapidamente recuperado quando da instalação do sistema, pois haverá uma significativa redução dos custos operacionais.

São muitas as vantagens da bilhetagem eletrônica através de *smart cards*:

- **Para os passageiros:** Não há mais a necessidade de portar dinheiro; os *smart cards* podem ser recarregados com grandes quantias; os cartões continuam válidos quando da mudança das passagens; o passageiro não precisa saber a tarifa exata, nem portar diversos tipos de bilhete para utilizar transportes com tarifas diferentes, pois o sistema deduz do cartão a quantia correta.

- **Para os motoristas:** Quando da cobrança direta ao motorista, o sistema eletrônico evita o desvio da atenção do mesmo, para efetuar a venda da passagem; não há mais o porte de dinheiro no interior do veículo, evitando a ação de ladrões; não há mais a necessidade de efetuar o cálculo do balanço diário: o sistema faz isso automaticamente.

- **Para as empresas de transporte:** Redução dos custos de operação e manutenção de equipamentos de venda de bilhetes, como os existentes no exterior; maior facilidade para alterar o valor das tarifas, pois não precisa imprimir novos bilhetes; redução da dos roubos nos veículos, visto que não haverá mais o porte de dinheiro no interior dos mesmos; e a eliminação da falsificação dos bilhetes.

- **Para o governo:** Redução da necessidade de subsídios para o setor, devido à redução de custos.

Sistemas de tarifas

Normalmente o sistema de transporte de uma cidade é dividido em várias zonas e baseado em diferentes meios de transporte, como ônibus, trens, metrôs, etc. Isso dificulta muito para os passageiros, visto que precisam portar diferentes bilhetes, cada um custando um determinado valor e para um determinado itinerário ou meio de transporte. Os sistemas de bilhetagem eletrônica facilitam nesse ponto também, pois podem ser criadas diferentes formas de cobrança da tarifa, sendo que o usuário precisa portar apenas o seu *contactless smart card*. Quatro das principais formas de cobrança são:

- **Sistema de Tarifas 1:** Pagamento é efetuado no início da viagem. Uma quantia fixa é deduzida do *contactless smart card*, independentemente da distância percorrida [10].

- **Sistema de Tarifas 2:** No começo da viagem, um *log* do momento do embarque é gravado no *contactless smart card*. Quando o usuário desembarca, a tarifa é automaticamente calculada e deduzida do cartão, de acordo com a distância viajada. Além disso, o cartão pode ser verificado a cada baldeação, para checar a existência de um *log* de embarque válido. Para coibir tentativas de manipulação, a inexistência de um *log* de saída pode ser penalizada pela dedução da tarifa máxima no começo da próxima viagem [10].

- **Sistema de Tarifas 3:** Esse modelo é melhor aplicado à redes interligadas, nas quais a mesma rota pode ser viajada utilizando-se diferentes sistemas de transporte, à diferentes tarifas. Toda vez que o passageiro muda de veículo, uma quantia pré-determinada é deduzida do cartão; tarifas promocionais para viagens de longa distância e pessoas com tarifas especiais podem ser automaticamente descontadas do cartão [10].

- **"*Best Price Calculation*":** Nesse sistema todas as viagens feitas são gravadas no cartão por um mês. Se um certo número de viagens for excedido, durante um dia ou um mês, então o cartão pode automaticamente utilizar uma tarifa bônus, durante um dia ou um mês. Isso dá ao consumidor máxima flexibilidade e as melhores tarifas possíveis. O cálculo do melhor preço aumenta o relacionamento com o consumidor e contribui muito para sua satisfação [10].

A figura 6.2 abaixo mostra um exemplo de utilização que envolve duas viagens de ônibus e uma de metrô, com a demonstração dos locais onde são efetuadas leituras/escritas nos cartões – pode-se verificar que o número de passagens a serem cobradas depende do tipo de sistema de tarifas utilizado.

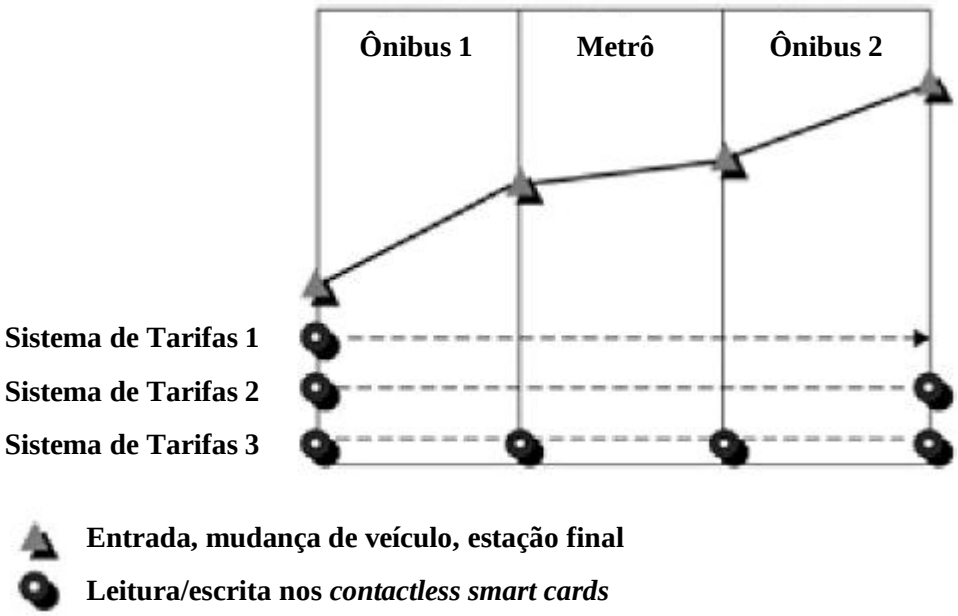

Figura 6.2 – Exemplo de utilização do sistema de transporte urbano [10]

Potencial de mercado

Estima-se que algo em torno de 50% do total de *contactless smart cards* vendidos no mundo são utilizados no setor do transporte público. As maiores áreas de utilização são, por exemplo, Seul, Hong Kong, Paris, Berlim e Londres [10]. No Brasil, São Paulo foi a cidade pioneira no sistema de bilhetagem eletrônica. A implantação do chamado "Bilhete Único" se deu em 2004. Hoje o sistema integra os serviços de ônibus, trens e metrôs que cortam a cidade e é a maior aplicação do gênero no Brasil, valendo-se de mais de 15.000 leitores e com mais de 10.700.000 *contactless smart cards* em circulação. Tal sistema tem integração temporal (2 horas), durante a qual o usuário pode utilizar quantas passagens forem necessárias, sendo que será debitada do seu cartão apenas uma. Em outros sistemas implantados no Brasil já há a facilidade da aquisição dos créditos pela internet, além dos postos credenciados.

6.2 Gerenciamento da Cadeia de Suprimentos

Um item pode ser rastreado na cadeia de suprimentos desde onde ele é produzido até onde ele é consumido ou reciclado, conforme mostra a figura 6.3. Considerando-se o processo de produção de refrigerantes, por exemplo, pode-se colocar um tag na embalagem plástica produzida, que contenha um número único de identificação. Essa embalagem pode, então, ser rastreada através da leitura dos dados do tag nos seguintes pontos da cadeia de suprimentos:

- Nas docas de saída do fabricante, onde a embalagem é carregada em um caminhão que deixará a fábrica
- Na chegada da embalagem nas docas de entrada do centro de distribuição
- Nas docas de saída do centro de distribuição, onde a embalagem é carregada em um caminhão que deixará o centro de distribuição
- Na chegada da embalagem no varejista
- Na saída da embalagem do varejista, quando comprada por um consumidor
- Na chegada da embalagem vazia ao centro de reciclagem

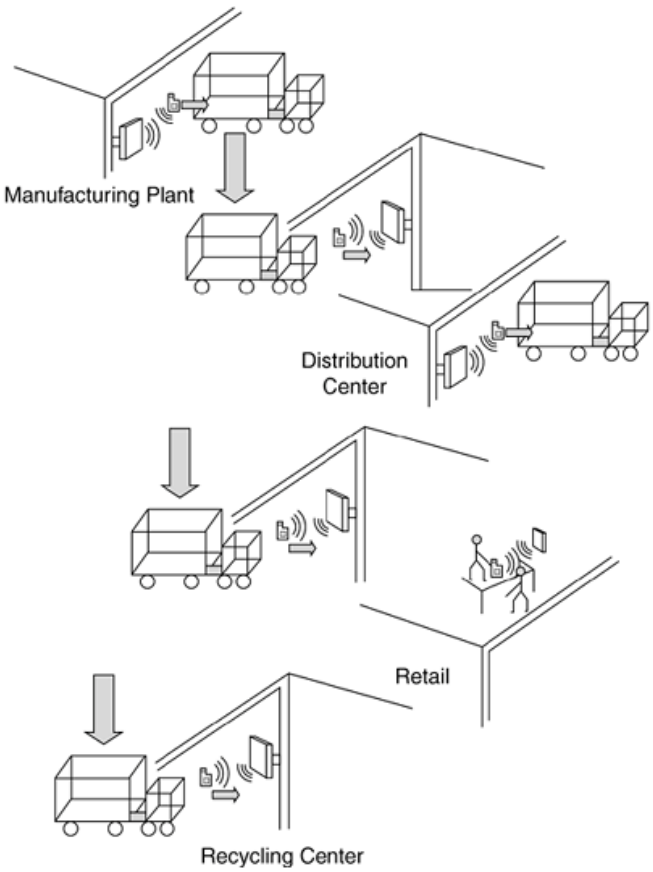

Figura 6.3 – Rastreamento de produtos na cadeia de suprimentos [1]

Os dados do tag também podem ser lidos em outros pontos da cadeia, como, por exemplo, quando essa embalagem for armazenada em uma determinada área do centro de distribuição, ou em um local específico no varejista. Também podem ser colocados leitores nas prateleiras do varejista, que identificarão a colocação ou a retirada do item nas mesmas. Um sistema secundário pode utilizar essa informação provida pelo leitor – que não pode tomar essa decisão sozinho, apenas repassa a lista de tags para o sistema- para determinar se essa prateleira precisa ser reposta com mais itens. A figura 6.4 mostra a lógica envolvida nesse processo. Também há a possibilidade do sistema receber a lista com os tags identificados na prateleira, olhar para um tipo específico de produto e verificar a quantidade do mesmo, a fim de determinar se a prateleira precisa ser completada.

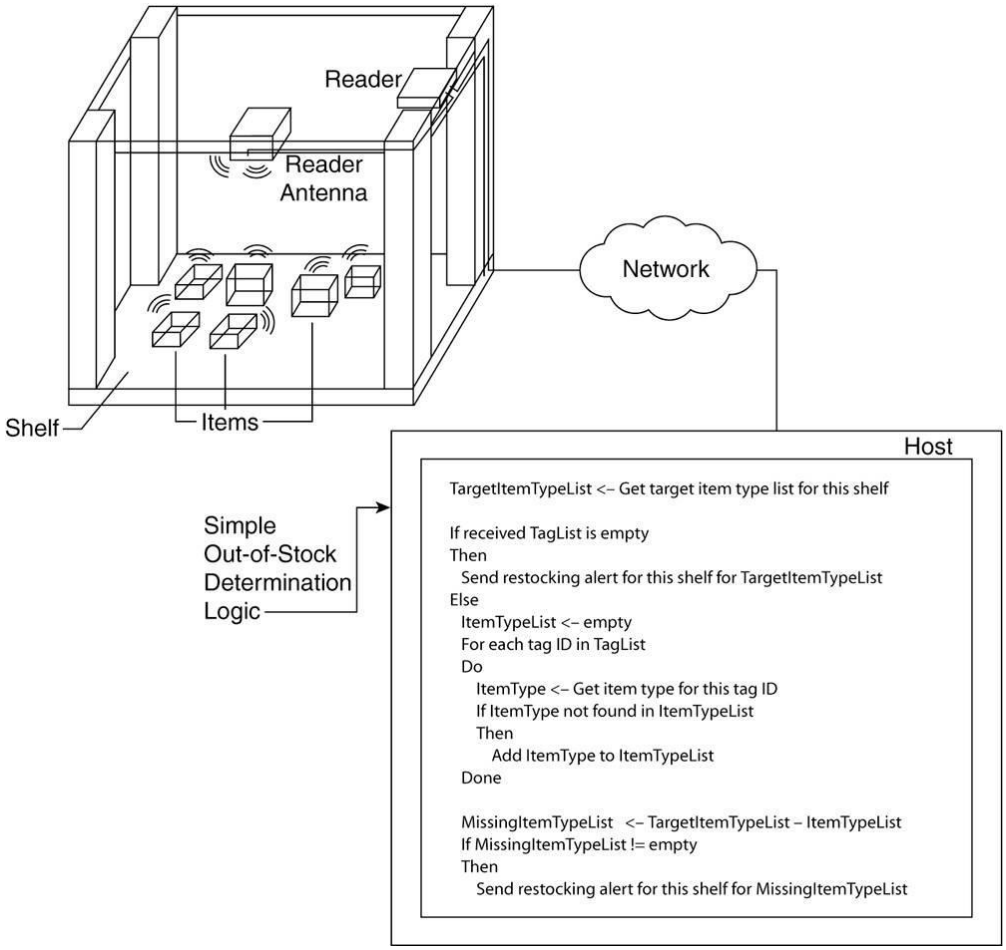

Figura 6.4 – Exemplo da lógica do controle da saída de produtos [1]

Sendo assim, a solução é totalmente personalizável, visto que a embalagem pode ser rastreada em todo seu trajeto, bem como o estoque pode ser completamente monitorado apenas com o acréscimo de leitores em determinados pontos.

As principais vantagens de se utilizar os sistemas de RFID nas aplicações de gerenciamento da cadeia de suprimentos são:

- **Melhor controle da produção:** Devido ao fato do item poder ser rastreado por toda a cadeia de suprimentos, e da informação obtida poder incluir a movimentação individual de cada item, problemas ocorridos durante o processo produtivo, bem como os locais onde ocorreram e as partes envolvidas podem ser muito mais facilmente identificados

- **Disponibilização do potencial de venda dos produtos ao varejista:** Visto que os compradores de um determinado item podem ser rastreados, vendedores podem utilizar esses dados para elaborar um plano de ação quando da existência de promoções especiais, por exemplo

- **Controle mais preciso do estoque:** Quem mais se beneficia desse benefício é o varejista. Com os dados mais precisos acerca do seu estoque, ele pode elaborar um plano de compras e de estoque baseado na rotatividade dos produtos, armazenando menos produtos que pouco vendem e mais, os que são mais vendidos, maximizando o potencial de vendas através da otimização do inventário do estoque

- **Melhor monitoramento dos produtos:** A possibilidade de saber precisamente onde se localizam determinados produtos e obter suas respectivas informações, disponibilizam aos empresários um melhor monitoramento do produto, podendo, assim, otimizar sua utilização, como, por exemplo, antever a aproximação do prazo de validade de determinado item, colocando-o a venda para evitar desperdício

- **Diminuição do estoque das redes de varejo:** Tendo em vista o controle das prateleiras que se pode obter com a implantação do sistema RFID, os dados da quantidade de itens presentes nestas pode ser utilizado para contactar diretamente o estoque, solicitando a reposição na prateleira e esse, por sua vez, através de um sistema secundário, ou quando adotada a *EPCglobal Network*, contactar o centro de distribuição solicitando o envio de mais produtos. Esse processo evita o armazenamento inútil de produtos, principalmente perecíveis, evitando desperdícios com itens com prazo de validade vencido.

O maior exemplo dessa aplicação é o caso Wal-Mart, a maior rede de varejo do mundo. Em junho de 2003 ele exigiu de seus 100 maiores fornecedores a implementação de sistemas de RFID, com EPC incluso no tag, no nível de pallets e grandes embalagens até 1 de janeiro de 2005 caso quisessem continuar fornecendo a ele. A recomendação foi seguida e, posteriormente, expandida de forma que mais 200 fornecedores implantassem sistemas de RFID até o final de 2006.

6.3 Segurança

Os sistemas RFID têm sido utilizados com sucesso em soluções de controle de acesso. Normalmente são utilizados tags para controlar o acesso ou monitorar o trajeto de objetos e *smart cards* para realizar essa função com pessoas. Esse tipo de aplicação se baseia no princípio de um tag que contém dados de identificação e que é portado pelo objeto ou pela pessoa para obter acesso a áreas controladas. Essa utilização do RFID está em um estágio bem avançado quando comparado com outros tipos de aplicações. O maior exemplo dessa maturidade é a existênca de padronização para ela (ISO 15693).

Um exemplo desse uso é a colocação de um tag no vidro de um veículo, com dados que permitam ao carro acessar um determinado local da garagem. Esse sistema depende da permissão de acesso estar associada àquele tag, permitindo ou não a entrada. Geralmente são utilizados tags passivos de 13,56MHz para essa aplicação. Tags ativos ou semi-passivos são utilizados apenas quando a distância para leitura é muito grande.

Sistema de segurança patrimonial e controle de acesso perimetral

Esta aplicação do RFID é utilizada para controlar o acesso a áreas específicas de um prédio, fábrica ou qualquer outro tipo de construção. Um exemplo disso é a porta de entrada de uma sala de alta segurança de uma grande empresa, como uma sala que contém um cofre, por exemplo. O acesso a ela, se não for controlado, pode resultar em grandes prejuízos para a corporação.

Os sistemas de segurança patrimonial e de controle de acesso normalmente utilizam *smart cards*, ou, ainda, tags ativos no formato de cartões. A informação de permissão ou recusa para entrada em salas é armazenada no tag, sendo uma das principais vantagens da utilização de RFID nesse tipo de aplicação: a portabilidade da informação. Dessa forma, todos os dados constam no cartão, não necessitando consultar o servidor central quando da passagem do cartão por um leitor, reduzindo, assim, o tráfego da rede. Os leitores possuem armazenadas informações sobre quais dados o cartão deve conter para liberar ou recusar o acesso. Sendo assim, estando a rede operante ou inoperante, ao verificar os dados contidos no cartão, o próprio leitor que autoriza ou não o acesso. Outro ponto de vista dessa vantagem diz respeito à possibilidade do sistema operar quando estiver com problemas na conexão de rede. O modo como são tratados os acessos quando essa condição de dificuldades na rede é atingida depende do tipo de sistema: Online ou Offline. As características principais desses sistemas são:

- **Sistemas Online:** Eles são mais utilizados onde a autorização de acesso de um grande número de pessoas tem de ser consultado em apenas alguns locais de acesso. Este é o caso, por exemplo, das entradas principais de edifícios comerciais ou de escritórios. Nesse tipo de sistema todos os terminais são conectados a um servidor central, por meio de uma rede. O sistema se mantém online através do constante envio de mensagens de controle, por parte dos leitores, mantendo a conexão TCP/IP sempre ativa. Essa é uma vantagem e uma desvantagem desse tipo de sistema, visto

que tal constante envio de mensagens de controle (o intervalo de tempo entre uma e outra é da ordem de milissegundos) pode sobrecarregar a rede.

- **Sistemas Offline:** São muito utilizados nas situações onde há um número de locais a serem controlados muito grande. Ao contrário dos sistemas online, ele se baseia na operação offline e, de tempos em tempos, envia os dados coletados ao servidor central. Caso a rede esteja inoperante no momento, ele armazena os dados até que ela volte a operar. Essa função evita o problema do sobrecarregamento da rede, apesar de não eliminá-lo, visto que, dependendo do software adotado, assim que a rede voltar a ficar online, todos os leitores podem enviar seus dados de uma só vez, gerando um congestionamento no sistema.

Sendo assim, há muitas vantagens com a aplicação dessa solução. Algumas delas são:

- **Flexibilidade no controle da segurança:** As permissões associadas a um certo ID, para um determinado acesso, podem ser garantidas ou revogadas dinamicamente, baseado no sistema de controle de acesso central. Da mesma forma, um ID é primeiramente enviado (via um leitor conectado à rede) para o sistema de segurança central. Esse sistema, então, usa uma variedade de fatores, como o número de tempo de acesso para essa facilidade, através desse ID e, então, decide se a permissão deve ser aceita. Além disso, pode ser integrado a esse sistema outros tipos de aplicação de RFID, como controle de patrimônio (através da colocação de um tag em objetos, como laptops, impressoras, etc.), ou ainda, através da utilização dos tags ativos, monitorar a movimentação das pessoas dentro do edifício. Por exemplo, se o sistema de controle de acesso determina que uma pessoa não tem a permissão necessária, ele pode enviar um alerta ao sistema de monitoramento para executar uma ação, como começar a gravação de um vídeo para monitorá-la, ou alertar a segurança para observar tal pessoa, etc.

- **Economia:** Hoje em dia os valores dos tags caíram muito. Principalmente dos *smart cards*, que são os mais utilizados nos sistemas de controle de acesso

- **Maturidade:** Esse tipo de aplicação já está há muito tempo sendo utilizada, logo, pode-se dizer que é uma tecnologia dominada. Há muito ainda para evoluir, mas o que existe atualmente é dominado. O simples fato de ser uma solução baseada em uma padronização ISO, a ISO 15693, é um exemplo dessa maturidade.

Muitos são os *cases* desse tipo de aplicação, inclusive no Brasil, como é o caso da CSN(Companhia Siderúrgica Nacional), Gerdau, COSIPA (Companhia Siderúrgica Paulista), Siemens, etc.

6.4 Monitoramento animal

Hoje, o uso do RFID está se tornando comum para monitoramento animal. Um tag colocado em um animal pode ser utilizado para saber sua origem, monitorar sua

saúde (monitorar peso, idade, controlar data de vacinação, saber quais as vacinas o animal já tomou), sua movimentação (movimentação no pasto, tempo de ordenha, quantidade de leite produzido, etc), etc. Esse tipo de aplicação também pode ser utilizado para monitorar as características da vida de animais silvestres, como migração, reprodução, etc. O padrão ISO 11784/11785 é o padrão internacional que norteia as aplicações de identificação animal por rádio-freqüência. Os sistemas de monitoramento animal são baseados na freqüência 134,2kHz e em tags passivos, visto que uma vez aplicados, não necessitam de manutenção.

Tags utilizados

A figura 6.5 ilustra os tipos de tags que podem ser aplicados no monitoramento animal, a 6.6 a secção transversal de três dos tipos e a figura 6.7, os locais onde eles são aplicados. Os tags subcutâneos são os que apresentam menor índice de infecção e/ou rejeição pelo organismo dos animais.

A figura 6.8 ilustra um leitor utilizado na identificação animal.

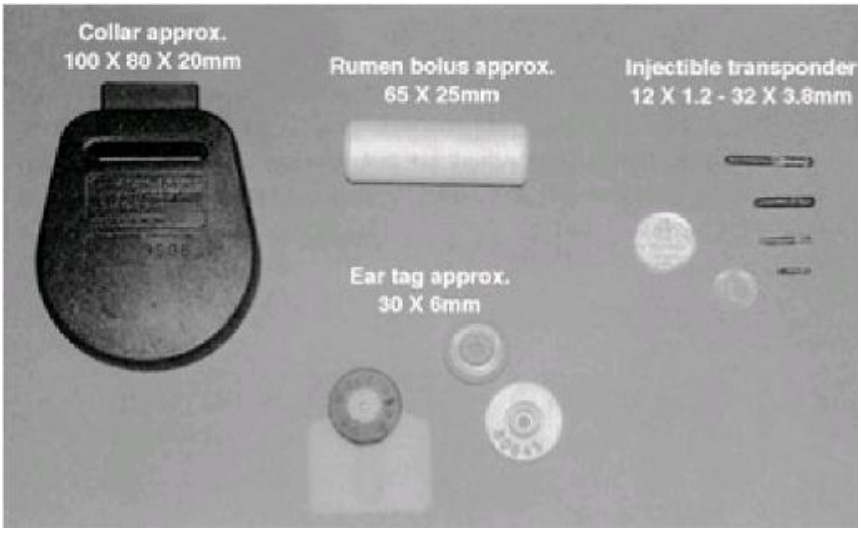

Figura 6.5 – Tags utilizados no monitoramento animal [10]

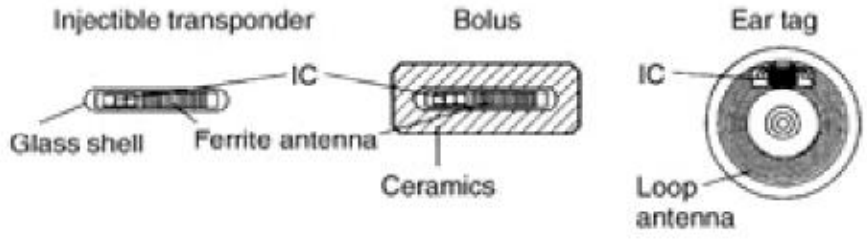

Figura 6.6 – Secção transversal dos tags utilizados no monitoramento animal [10]

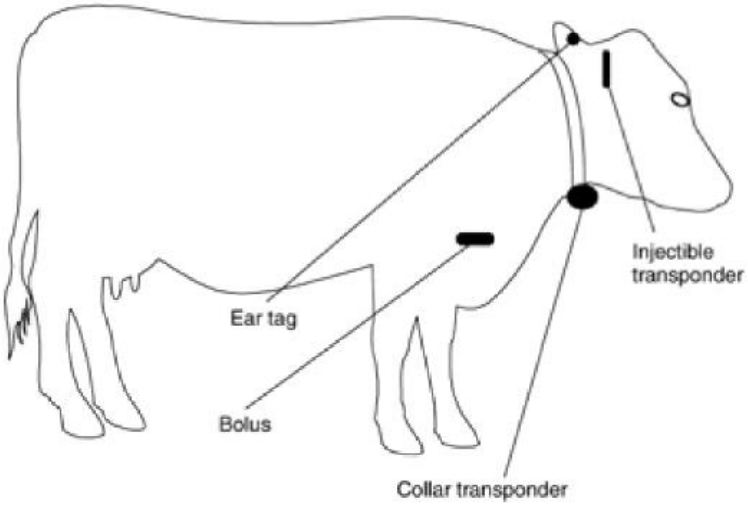

Figura 6.7 – Locais de aplicação dos tags para monitoramento animal [10]

Figura 6.8 – Leitor utilizado na identificação animal [11]

No Brasil está em implantação o SISBOV – Sistema Brasileiro de Rastreabilidade da Cadeia Produtiva de Bovinos e Bubalinos, que tem como objetivo o controle e o rastreamento do processo produtivo, no âmbito das propriedades rurais de bovinos e bubalinos. Foi criado pelo Ministério da Agricultura, Pecuária e Abastecimento (MAPA) visando estabelecer normas para a produção de carne bovina e/ou bubalina com garantia de origem e qualidade. O sistema é de adesão voluntária para os produtores rurais, mas obrigatória no caso de comercialização da carne bovina e/ou bubalina em mercados que exijam o rastreamento.

De acordo com as novas regras, todos os bovinos e bubalinos dos estabelecimentos rurais aprovados no SISBOV serão obrigatoriamente identificados

individualmente e cadastrados na Base Nacional de Dados, com o registro de todos os insumos utilizados na propriedade durante o processo produtivo.

A partir de 2009, só será permitido o ingresso de bovinos e bubalinos nos estabelecimentos rurais aprovados no SISBOV se oriundos de outros estabelecimentos na mesma condição [12].

6.5 Automação de Bibliotecas

O sistema de automação de bibliotecas baseado na tecnologia de RFID funciona basicamente da seguinte forma: Todos os itens do acervo são catalogados e neles são colocados tags. Leitores são postos nas prateleiras, em computadores destinados a efetuar o empréstimo do livro e em urnas para sua respectiva devolução. O princípio do sistema é: o usuário consulta o livro em um dos computadores ligados ao sistema, que, por sua vez, se comunica com a base do software de gerenciamento dos livros. Esse software faz uma busca no recinto localizando a exata prateleira na qual está o livro desejado. A retirada do livro da prateleira é registrada no sistema como uma saída. Caso o usuário deseje solicitar o empréstimo, ele se dirige a um dos terminais, passa seu *smart card* e o livro pela leitora, efetuando, assim, o registro do empréstimo. Automaticamente é alterado no sistema o status do livro, para "emprestado" e a inseridos os dados do usuário, a data de devolução, etc. Estando o livro com esse status, quando o usuário passa no portal instalado na saída da biblioteca, o sistema não alarma para um possível furto; porém, quando o status não for esse, o sistema exibe um alerta de roubo. Quando o usuário devolve o livro em uma urna, ela automaticamente modifica o status do livro para "disponível" e gera uma pendência no sistema, alertando que tal livro deve ser recolocado na prateleira, informando o local exato em que ele deve estar. Assim que ele é colocado de volta no seu lugar de origem, a pendência é eliminada.

Usualmente são utilizados tags passivos, flexíveis, finos e de 13,56MHz, conforme mostrado na figura 6.9, principalmente devido ao tamanho reduzido e ao baixo custo, podendo serem aplicados diretamente ao material da biblioteca, ou serem convertidos em *smart labels* (tags impressos em impressoras especiais).

Figura 6.9 – Tags utilizados na automação de bibliotecas [13]

As principais vantagens da aplicação de RFID na automação de bibliotecas são:

- **Organização:** Sempre será possível saber onde estão e a quais prateleiras os livros pertencem, evitando perdas e desorganização do acervo

- **Facilidade de localização:** Sempre se saberá onde está o livro, inclusive quando estiver em outra prateleira

- **Maior segurança contra roubo:** Se o usuário não efetuar a solicitação de empréstimo e tentar sair da biblioteca com o livro, o sistema alarmará

A biblioteca do Vaticano, que contém um acervo de 40 milhões de livros e manuscritos, começou a implantação do RFID em 2003. O RFID foi escolhido devido ao seu baixo custo e devido ao fato de que não danifica as obras, que inclui manuscritos antigos e a mais antiga e completa versão conhecida da Bíblia [14].

6.6 Sistema de pagamento de pedágio

Empresas administradoras de pedágios de vários países utilizam RFID para permitir aos motoristas pagarem o pedágio eletronicamente nas cabines, ou seja, sem parar o veículo. O sistema de pedagiamento eletrônico pode funcionar de duas maneiras: pré-paga ou débito automático em conta corrente. No sistema pré-pago o consumidor abre uma conta na administradora responsável pela coleta do pedágio, com uma determinada quantia de dinheiro. Então o consumidor recebe um tag, que geralmente é instalado no pára-brisa do veículo, contendo um *ID number* que, no software, faz referência às informações do veículo e do proprietário. Quando o usuário passa pela cabine de pedágio habilitada com um leitor, este lê o *ID number* do tag, acessa a conta cadastrada neste e a quantia referente à tarifa é subtraída automaticamente, liberando a passagem do veículo. O tag pode mostrar o status da conta por meio de indicadores luminosos. Por exemplo, uma luz verde pode significar pagamento efetuado e uma luz amarela pode significar que o saldo de créditos da conta está baixo. Tais créditos podem ser adquiridos por meio de cartão de crédito comum, pela internet ou por telefone.

A diferença do sistema pré-pago para o sistema de débito automático é que, ao invés do consumidor criar uma conta com o administrador e colocar créditos nessa conta, ele cadastra no software do sistema sua conta bancária padrão. Quando faz a passagem pela cabine de pedágio, é efetuada a marcação da passagem no software. Ao final do mês é elaborada uma fatura que tem seu valor debitado automaticamente da conta cadastrada.

O modo de funcionamento do sistema de cobrança eletrônica de pedágio é mostrado na figura 6.10.

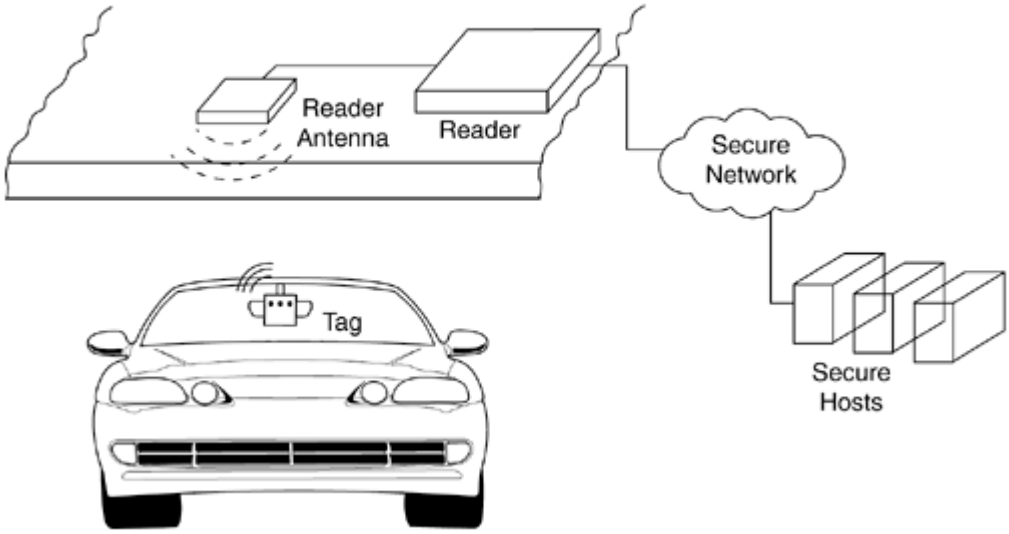

Figura 6.10 – Sistema de cobrança eletrônica de pedágio [1]

As principais vantagens desse tipo de aplicação são:

- **Rapidez, agilidade e conveniência:** Tudo que o consumidor tem que fazer é se dirigir à cabine de pedágio; o resto é automático: não há a necessidade de parar, nem de portar a quantia de dinheiro correta para o pagamento, ou esperar em filas de atendimentos

- **Não há a necessidade de portar dinheiro:** O tag elimina a necessidade de portar dinheiro para efetuar o pagamento da tarifa do pedágio

- **Segurança:** O tag é relacionado com o veículo. Portanto, se o tag de um dado carro for utilizado em outro o sistema, dependendo do software utilizado, pode ser recusada a passagem do mesmo. Também há um fator de segurança se o tag for roubado, pois basta que o usuário comunique o roubo junto à administradora do pedágio para que o tag seja retirado da base de dados, ficando inutilizado

- **Redução de custos:** Como o sistema é totalmente eletrônico, há uma significativa redução dos custos operacionais, como, por exemplo, com quadro de funcionários, visto que não há mais a necessidade de atendentes nas cabines

Um desafio para esse tipo de aplicação de RFID a aceitação por todas as administradoras de pedágio, para que efetivamente os benefícios possam ser aproveitados em várias rodovias, não limitando o uso a algumas delas.

Normalmente são empregados tags semi-passivos, que, além de conter o *ID number*, também podem conter circuitos eletrônicos que permitem a exibição, por exemplo, do nível de bateria, do status da conta, etc.

Alguns dos maiores cases de sistemas de pagamento eletrônico de pedágio são o SunPass, na Flórida, e o E-Z Pass, em New Jersey. No Brasil o projeto pioneiro foi um sistema baseado no débito automático, em São Paulo, chamado Sem Parar. Hoje ele se chama Via Fácil e abrange quatro estados (São Paulo, Rio de Janeiro, Paraná e Rio Grande do Sul), além de permitir, da mesma forma que nas cabines de pedágio, o pagamento eletrônico do estacionamento do Aeroporto de Congonhas – SP, da Universidade FAAP - SP e vários outros conveniados, incluindo estacionamentos de shoppings centers.

Uma aplicação também relacionada a automóveis, que no Brasil se chamará SINIAV – Sistema Nacional de Identificação Automática de Veículos, é a identificação eletrônica de veículos. O sistema SINIAV consiste no acoplamento de um tag no pára-brisa de cada veículo, que conterá um número de série (único para cada placa), o número do chassi, o número do Renavam e a placa do veículo. Desse modo, o objetivo é que seja possível evitar furtos e roubos, bem como obter um controle mais efetivo do tráfego urbano. A previsão é que até 2011 todo o sistema esteja plenamente operacional em todos os estados do Brasil, incluindo o Distrito Federal.

CAPÍTULO 7

Análise da aplicação RFID 13,56MHz - *Smart Cards*

O *smart card* pode ser resumido como sendo um cartão plástico que contém um circuito integrado embutido, que possui componentes para transmitir, armazenar e processar dados. Os dados podem ser transmitidos utilizando-se ou contatos na superfície do cartão (*contact smart cards*) ou campos eletromagnéticos, sem qualquer contato (*contactless smart cards*). *Smart cards* oferecem algumas vantagens quando comparados com cartões magnéticos (como os utilizados por bancos):

- **Memória:** O *smart card* possui uma capacidade de armazenamento de dados muito maior do que a de cartões magnéticos

- **Segurança:** Os dados armazenados no cartão são protegidos contra acesso não-autorizado

- **Vida útil:** Durabilidade muito maior dos *smart cards*, com relação aos cartões magnéticos, que, normalmente, têm vida útil de dois anos

7.1 Padrões

O pré-requisito para a penetração mundial dos *smart cards*, como seu uso, na Alemanha como cartão telefônico, cartão de plano de saúde e cartão bancário, tem sido a criação de padrões nacionais e internacionais.

Tendo em vista que o *smart card* é o único componente do sistema que o usuário porta, é extremamente importante que se tenha o reconhecimento e a aceitabilidade no sistema todo, o que pode ser facilmente obtido através do estabelecimento de padrões.

Padrões internacionais para os *smart cards* são desenvolvidos sobre a supervisão da ISO (*International Organization for Standardization*) / IEC (*International Electrotechnical Comission*) e do CEN (*Comiteé Europeén de Normalisation*). A figura 7.1 representa a estrutura dos grupos de trabalho da ISO e da IEC, e os padrões pelos quais eles são responsáveis.

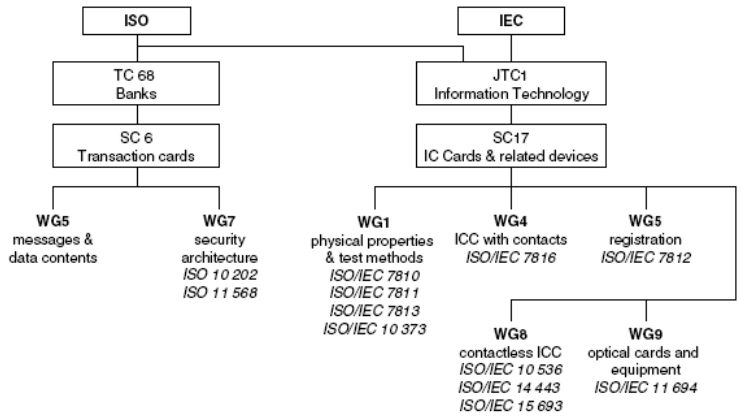

Figura 7.1 – Estrurura dos grupos de trabalho (WG) ISO/IEC e os padrões pelos quais são responsáveis [11]

Como pode ser visto, há dois comitês técnicos que desenvolvem padronizações para cartões. O primeiro é o ISO 68/SC6, que é responsável pela padronização dos cartões utilizados nas transações financeiras. O segundo é o ISO/IEC JTC1/SC17, que é responsável por *Smart Cards*.

As principais normas ISO para os *Smart Cards* são:

- **ISO/IEC 7816:** É a família de padrões ISO mais importante para *Smart Cards* microprocessados. É dividido em 15 partes. As quatro primeiras partes são
    - **Parte 1 –** Define as características físicas de um cartão com contato
    - **Parte 2 –** Define os tamanhos e posições dos contatos do *Smart Card*, bem como suas possíveis organizações no cartão. Também descreve o método a ser utilizado para medir as posições dos contatos no *Smart Card*
    - **Parte 3 –** O padrão ISO mais importante para os parâmetros elétricos de um *Smart Card* microprocessado. Ele especifica tanto as características elétricas, como tensão de alimentação, quanto define os protocolos de sinais e de transmissão.
    - **Parte 4 –** O padrão ISO mais importante para definições no nível de aplicação. Ele define a organização e a estrutura dos arquivos, a arquitetura de segurança, códigos de retorno, dentre outros parâmetros. Basicamente, esse padrão se refere ao formato dos comandos de acesso ao cartão com contato
- **ISO/IEC 10536:** Esse padrão descreve as características físicas, dimensões e localizações das áreas de acoplamento de *Contactless Smart Cards*. Também especifica os sinais elétricos dos componentes indutivos e capacitivos utilizados para acoplar o cartão ao terminal e a transmissão de dados a nível físico, bem como os protocolos utilizados nessa transmissão
- **ISO/IEC 14443:** Esse padrão define, através de características físicas, de potência dos sinais, dos algoritmos de inicialização e anti-colisão, dos protocolos de transmissão, dentre outros, os *Proximity Cards*, que são *Contactless Smart Cards* que podem ser utilizados em situações onde o terminal está a uma distância menor que algumas dezenas de centímetros
- **ISO/IEC 15693:** Esse padrão regulamenta os *Vicinity Cards*, que são *Contactless Smart Cards* que podem ser utilizados em situações onde o terminal está a uma distância menor que 1m.

7.2 Classificação

A classificação dos *smart cards*, conforme mostrado na figura 7.2, se norteia, basicamente, pelas seguintes características:

- **Método de transmissão dos dados:** Os dados contidos nos *smart cards* podem ser transmitidos utilizando-se tanto os contatos na superfície do cartão (*smart cards* com contato), como campos eletromagnéticos (*contactless smart cards*).

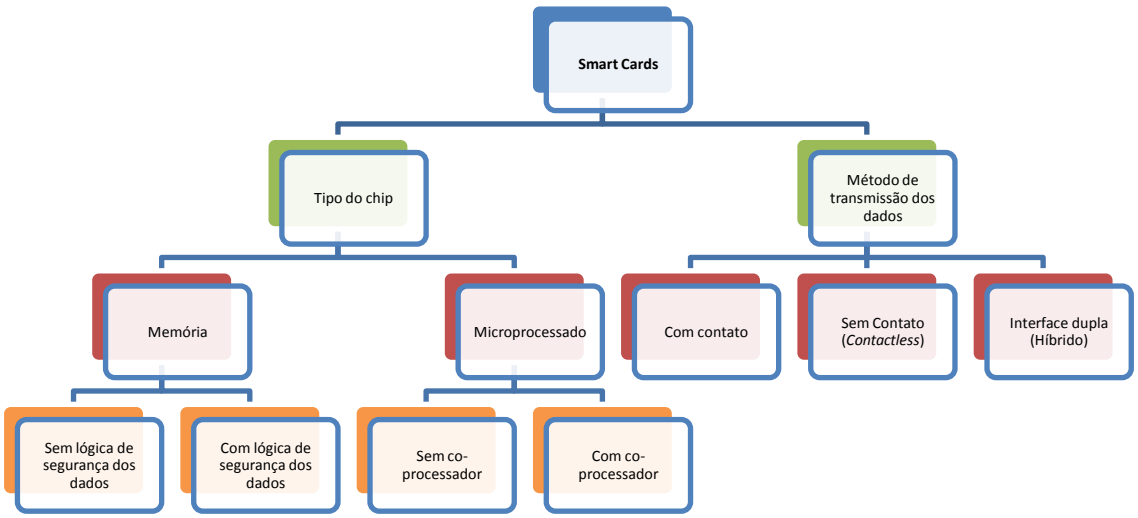

Figura 7.2 – Classificação dos *Smart Cards*

- **Tipo do chip:** O *smart card* pode ser microprocessado (com ou sem um co-processador) ou apenas de memória (com ou sem lógica de segurança dos dados)

7.2.1 Memory Smart Cards

No *Memory Smart Card* os dados necessários para a aplicação estão armazenados na memória, que, normalmente, é do tipo EEPROM. O acesso à memória é controlado pela lógica de segurança, que, no caso mais simples, consiste de proteção contra gravação ou apagamento da memória, ou de parte dela. Entretanto, há os tipos de *Memory Smart Cards* que possuem uma lógica de segurança bem mais complexa, fazendo as vezes de uma criptografia, garantindo mais segurança na transmissão dos dados. A figura 7.3 mostra a arquitetura básica de um *Memory Smart Card* com lógica de segurança.

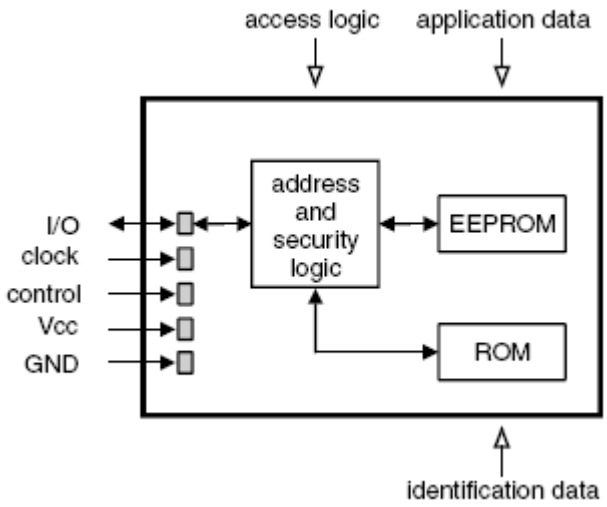

Figura 7.3 – Arquitetura básica de um *Memory Smart Card* com lógica de segurança [11]

7.2.2 Microprocessed Smart Cards

A principal característica desse tipo de cartão, como o próprio nome sugere, é a presença de um microprocessador, sendo que este é acompanhado de ROM, RAM e EEPROM, como mostrado na figura 7.4.

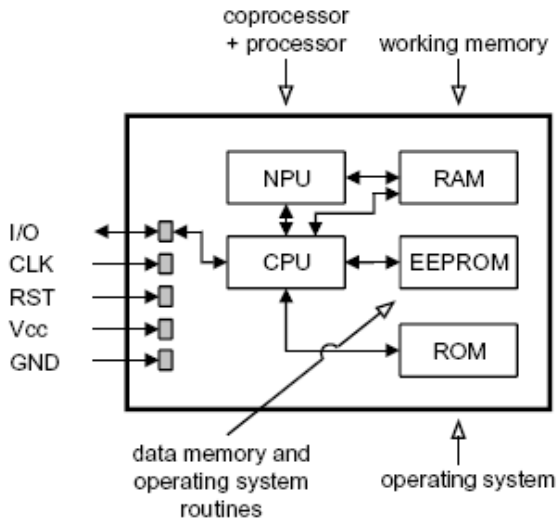

Figura 7.4 – Arquitetura básica de um *Microprocessed Smart Card* com co-processador [11]

A ROM contém o sistema operacional do chip, que é gravado nele quando da sua fabricação. Sendo assim, todos os cartões produzidos na mesma linha de produção possuem o mesmo conteúdo de ROM, e este não pode ser alterado durante a vida do cartão.

Na EEPROM dados e programas podem ser escritos e lidos, sob o controle do sistema operacional.

A RAM é a memória de trabalho do processador, de uso exclusivo deste. Esta memória é volátil, logo, todos os dados nela armazenados são perdidos assim que o chip é desalimentado.

O *Microprocessed Smart Card* tem uma vantagem muito importante no que diz respeito à segurança dos dados, com relação ao *Memory Smart Card*: na lógica de entrada, em um cartão de memória há a necessidade do recebimento de um sinal de controle do leitor, enquanto que no cartão microprocessado toda a lógica de segurança é executada pelo microprocessador nele contido.

Também há a possibilidade da incorporação, na estrutura do *Microprocessed Smart Card*, de um co-processador (NPU – *Numerical Processor Unit*), para realização de operações relacionadas à segurança e criptografia.

7.2.3 *Smart Cards* com contato

Os *smart cards* com contato, como o próprio nome sugere, necessitam estar em contato com a antena do leitor para que o processo de leitura seja efetuado corretamente. Tais contatos que, normalmente, são seis ou oito contatos dourados, que podem ser vistos em qualquer *smart card*, fornecem energia, sinais de *clock* e de *reset*, bem como uma interface serial bi-direcional. O cartão e o leitor seguem um protocolo para acordarem uma voltagem e uma *clock speed*, sendo que esta pode determinar a velocidade interna de processamento, bem como a taxa de transferência dos dados entre o cartão e o leitor. Muitos cartões trabalham com 5V de tensão de alimentação e 9.600 bps de taxa de transmissão; entretanto, cartões embutidos em sistemas, como em telefones celulares, trabalham com tensões menores e taxas de transmissão maiores. Um *smart card* com contato, como o mostrado na figura 7.5, e de acordo com as normas ISO aplicáveis, possui os seguintes componentes:

- Microprocessador de 8 bits
- Memórias ROM e RAM
- Memória de armazenamento não-volátil, como a EEPROM
- Sistema operacional interno

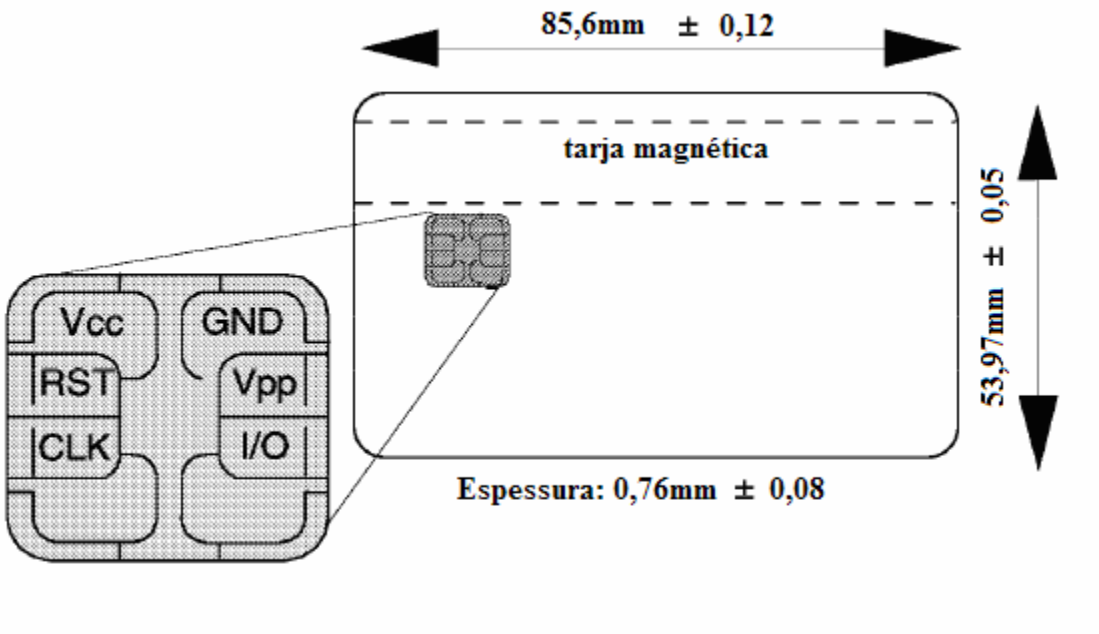

Figura 7.5 –Características físicas de um *Smart Card* com contato, com tarja magnética – opcional [10]

Embora os *smart cards* com contato, devido a sua maior simplicidade de construção, sejam muito mais baratos do que os *contactless smart cards*, é importante frisar um problema muito comum em sistemas eletromecânicos: falhas de contato. Essas falhas podem ser causadas por fatores como sujeira, desgaste do contato metálico, vibração do leitor, etc. Outro problema com os *smart cards* com contato é a danificação do cartão por descargas de energia estática.

7.2.4 Contactless Smart Cards

Os *Contactless Smart Cards* não necessitam de qualquer conexão física entre o cartão e o leitor para transferência de energia e dados, em uma curta distância, pois utilizam ondas de RF tanto para alimentar o cartão, como para comunicação entre o cartão e o leitor. O cartão tem incorporado uma antena (algumas voltas de fios embutidas no cartão e postas próximas às bordas do mesmo) no lugar do contato metálico na superfície do cartão. Sendo assim, eles não precisam ser inseridos no leitor, apenas aproximados a uma distância que pode chegar a 1m, o que evita muitos dos defeitos ocorridos com os *smart cards* com contato. Outra importante vantagem com relação aos *smart cards* com contato é a liberdade com relação à orientação de apresentação do cartão no leitor. Enquanto que no caso dos com contato há uma orientação específica de apresentação para que possa haver a leitura, daí a necessidade de serem inseridos no leitor, nos *contactless* não importa como o cartão é apresentado ao leitor. Isso representa uma grande vantagem em aplicações que não têm uma orientação específica de apresentação do cartão, como em sistemas de controle de acesso, onde uma porta ou catraca podem ser autorizadas para acesso por meio de um

cartão que esteja no bolso de uma pessoa, por exemplo. Outra aplicação onde o *contactless* é muito utilizado é no transporte público, no qual há uma necessidade de um grande número de pessoas serem identificadas em um curto espaço de tempo. Sendo assim, nessa aplicação sua vantagem principal é que ele evita a necessidade do usuário ter de inserir o cartão em um leitor, o que iria requerer muito tempo, além de reduzir o risco de vandalismo como a colocação de gomas de mascar ou colas no local de inserção do cartão.

Uma das desvantagens dos *contactless* para os cartões com contato é o preço. Devido à maior complexidade, seu custo é maior do que o de um cartão com contato, que é simples na sua arquitetura.

Os *Contactless Smart Cards* também são divididos em 4 categorias:

- ***Close-Coupling Cards*:** São cartões que precisam ser inseridos ou encostados nas superfícies próximas à antena do leitor, para que o processo de leitura seja efetuado corretamente. Esse tipo de cartão possui uma vantagem com relação aos cartões com contato: devido a não necessidade, em um cartão *contactless*, de qualquer percurso físico e condutor entre a superfície do cartão e o CI do mesmo, ele é muito mais tolerante a danos causados por descargas eletrostáticas. As especificações dimensionais dos cartões *close-coupling* são as mesmas dos cartões com contato.

- ***Remote-Coupling Cards*:** São *smart cards* que podem transmitir dados por distâncias que vão de alguns centímetros a um metro do leitor. São divididos em 2 grupos:

    - ***Proximity Smart Cards*:** São cartões *contactless* que operam a curtas distâncias - aproximadamente 10 cm. A quantidade de energia que é transmitida a essa distância é suficiente para alimentar o microprocessador do cartão. São conhecidos como *Mifare*® os cartões que operam na freqüência típica de 13,56MHz, mas existem também os que utilizam freqüências variando entre 125kHz e 135kHz. São muito utilizados em sistemas de transporte público e de segurança.

    - ***Vicinity Smart Cards*:** São cartões semelhantes aos *Proximity*, porém com um alcance de até 70cm. Apesar da larga vantagem do alcance de leitura, com relação aos demais tipos de *smart cards*, o custo da estrutura(cartões e leitores) de uma solução com *vicinity smart cards* inviabiliza muitas de suas aplicações. Ele possui três modos de funcionamento: leitura (com alcance de cerca de 70cm), autenticação (com alcance de cerca de 50cm) e gravação (com alcance de cerca de 35cm). Também utilizam a energia transmitida pelo leitor, a essa distância, para alimentar o microprocessador do cartão. Operam na freqüência de 13,56MHz. Sua principal aplicação é em sistemas de controle de acesso.

7.2.5 Dual-Interface Smart Card

Dual-Interface Smart Cards são cartões híbridos que, ao mesmo tempo, possuem duas interfaces, como *Contact Smart Card* e *Contactless Smart Card*, ou tarja magnética e *Contact Smart Card*, ou tarja magnética e *Contactless Smart Card*, ou, ainda, tarja magnética, *Contact Smart Card* e *Contactless Smart Card* – chamados de cartões de interface tripla, como o mostrado na figura 7.6. Para algumas aplicações é interessante ter ambas as interfaces, com contato e sem contato. Por exemplo, as instituições bancárias, inclusive no Brasil, estão substituindo seus cartões magnéticos por cartões híbridos, com tarja magnética e *Contact Smart Card*, conforme o da figura 7.7, para que haja uma transição mais suave dos cartões magnéticos para os *smart cards*, tendo em vista o custo que a substituição de todos os leitores de uma única vez geraria.

Figura 7.6 – *Dual-Interface Smart Card (Smart Card* com e sem contato)

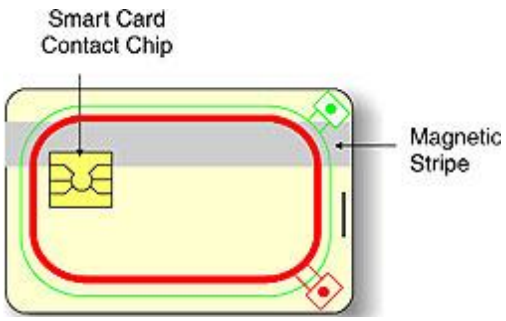

Figura 7.7 – *Dual-Interface Smart Card* (Cartão magnético e *Smart Card* com contato)

7.2.6 Comparação entre os *Smart Cards*

As principais características dos tipos de *smart cards*, exceto dos *Dual-Interface*, visto que estes são uma mescla dos demais tipos existentes, estão descritas na tabela 7.1 a seguir:

Tabela 7.1 - Principais características dos tipos de *smart cards*

	Contact	***Close-Coupling***	***Proximity***	***Vicinity***
Alcance de leitura	Contato	~2mm	~10cm	~70cm
Freqüência de Operação	3,57MHz	4,91MHz	13,56MHz ou 125-135kHz	13,56MHz
Exemplo de Aplicação	*Banking*	*Vending Machines*	Controle de Acesso	Passaporte
Velocidade de Leitura	Baixa	Média	Alta	Alta
Custo	Baixo ---------- Alto			

7.3 Aplicações

Algumas das aplicações dos *smart cards* são:

- **Cartões de débito:** Hoje, inclusive no Brasil, são muito utilizados os *smart cards* com contato como cartões de débito, como o da figura 7.8, principalmente devido à segurança dos dados e à dificuldade de interceptação dos mesmos e de clonagem.

Figura 7.8 – Exemplo de *smart card* utilizado como cartão de débito

- **Dinheiro eletrônico:** A utilização dos *smart cards* como dinheiro eletrônico vem sendo amplamente estendida. São soluções como o cartão de crédito pré-pago mostrado na figura 7.9, em que o usuário insere créditos e pode utilizar o mesmo cartão para compras, alimentação, etc. Empresas adquirem esta solução para, por exemplo, que os funcionários efetuem compras em *vending machines* dentro dos próprios prédios, sem a necessidade de portar dinheiro

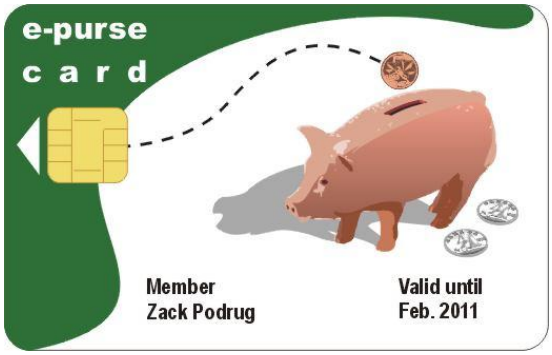

Figura 7.9 – Exemplo de *smart card* utilizado como dinheiro eletrônico

- **Cartões de fidelidade:** O cartão, por exemplo, de crédito, sempre que utilizado, acumulará pontos, que ficarão gravados no próprio chip, evitando o porte de vários cartões de fidelidade, de diversas empresas

- **Transporte urbano:** O uso do smart card no transporte urbano é, hoje, uma das maiores aplicações do mesmo. Através da inserção de créditos no cartão para uso posterior, o usuário evita o porte de dinheiro para utilizar o sistema de transporte. Também se evita, assim, o porte de dinheiro dentro dos veículos de transporte, reduzindo o risco de assaltos. Outras funcionalidades podem ser agregadas aos sistemas, como bônus por utilização ou tarifas reduzidas em determinados horários.

Na figura 7.10 é mostrado o sistema implantado no transporte urbano de São Paulo, o Bilhete Único

Figura 7.10 – Exemplo de *smart card* aplicado no transporte urbano [15]

- **Controle de acesso:** Essa é outra grande aplicação do *smart card*, principalmente devido à enorme segurança agregada à solução. O usuário porta um cartão no qual são gravadas desde suas informações pessoais, como nome, foto e identidade, até as permissões para acesso a certos locais. Através da colocação de leitores nos locais de acesso, como portas, conforme a figura 7.11, e catracas, pode ser implementado o controle de acesso a um edifício, bem como a determinadas áreas deste, como também a estacionamentos

Figura 7.11 – Ilustração do acesso através de uma porta, com o uso de um Smart Card

- **TV por assinatura:** O cartão pode ser utilizado como um cartão de crédito pré-pago para efetuar a compra de filmes, shows e demais eventos *pay-per-view*. Outra forma de utilização, inclusive já posta em prática no Brasil, é a gravação dos pacotes contratados pelo assinante em um smart card; este é inserido no aparelho

decodificador da TV por assinatura, que, automaticamente, libera os canais autorizados e bloqueia os não contratados. Um exemplo é o da figura 7.12:

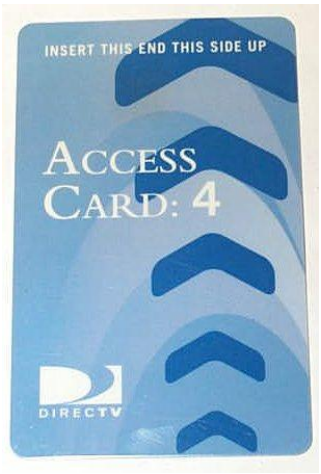

Figura 7.12 – Exemplo de smart card utilizado como cartão de acesso a TV por assinatura

- **Saúde:** Informações como doenças, últimas visitas médicas, últimos medicamentos receitados, atual condição de saúde, informações sobre o plano de saúde, entre outras, podem ser gravadas no cartão, como o mostrado na figura 7.13, e utilizadas em visitas ao médico, que poderá, assim, consultar todas essas informações. Isso facilita o prognóstico médico, bem como agiliza o processo de liberação de consultas pelos planos de saúde, ou ajuda na hora de adquirir um medicamento, visto que o mesmo cartão que contém a receita dos medicamentos indicados pelo médico pode ser lido em uma farmácia

Figura 7.13 – Exemplo de *smart card* utilizado como cartão-saúde

CAPÍTULO 8

Estudo de caso – Presidência da República Federativa do Brasil

A proposta do estudo de caso do sistema de controle de acesso da Presidência da República Federativa do Brasil surgiu devido à importância da demonstração de uma aplicação prática da tecnologia de RFID após o detalhamento mostrado durante este presente trabalho. Através de várias visitas às plantas, análise dos editais referentes ao projeto e entrevistas com os respectivos gestores competentes, como o Diretor da DITEL (Diretoria de Telecomunicações), vinculada ao Gabinete da Casa Civil da Presidência da República, Sr. Dilno Pereira Lopes, e o Gerente Executivo da empresa provedora da solução, Telemática Sistemas Inteligentes LTDA., o Sr. Ricardo Moragas Catón, foi desenvolvido esse estudo do sistema implantado nas dependências do Palácio do Planalto e seus anexos, Palácio da Alvorada, Palácio do Jaburu, Residência Oficial da Granja do Torto e Secretaria de Comunicação (Bloco A – Esplanada dos Ministérios).

Devido ao sigilo exigido pela Presidência da República, logicamente, por se tratar de um sistema de segurança, não foram permitidas fotos dos locais, bem como foi restringida a divulgação de informações consideradas confidenciais.

8.1 Objetivos

A Presidência da República Federativa do Brasil objetivou com a aquisição do sistema SIS controlar, monitorar e gerenciar todos os pontos de acesso das áreas alvo, inclusive possibilitando a recuperação de imagens gravadas relacionadas a eventos de acesso em pontos estratégicos com indicação de local, hora, usuário e número do evento. Para tanto, deveria ser implantado um sistema de controle de acesso que utilizasse tecnologia RFID, especificamente, para pessoas e veículos, *Smart Cards* ISO14443-A, para visitantes, tags ativos, com integração com um sistema de monitoramento por vídeo digital. É importante ressaltar que a solução deveria funcionar como uma plataforma única e totalmente integrada.

8.2 Situação anterior

Antes da implantação do sistema não existia qualquer tipo de controle de acesso, bem como monitoramento, de visitantes e/ou servidores. O controle de acesso de visitantes era realizado por meio de adesivos. Tais adesivos eram entregues mediante o cadastro dos dados pessoais e do local a ser visitado, em planilhas interligadas a uma base de dados. Essa base de dados possuía uma validade de três meses. Caso um visitante não voltasse dentro desse período, seu cadastro era automaticamente excluído. Além do pouco controle provido por essa solução, visto que não havia nenhuma restrição à entrada, freqüentemente tais adesivos se desprendiam da vestimenta dos visitantes. Sendo assim, não era raro encontrar visitantes vagando pelos corredores internos das instalações sem qualquer tipo de identificação.

Como não poderia ser diferente, servidores também tinham livre circulação dentro das instalações, porém podiam adentrar a locais de acesso ultra-restrito, por

exemplo, onde circulavam documentos secretos e confidenciais, tais como gabinetes e diretorias, pois não havia quaisquer barreiras à entrada.

Anteriormente, o acesso aos estacionamentos internos era praticamente livre. Por exemplo, uma pessoa que fosse se dirigir ao Senado poderia se identificar como visitante de algum departamento qualquer do Palácio do Planalto, apenas para deixar seu veículo. Também não eram raros eventos decorrentes de atos depredatórios nos veículos ali estacionados.

8.3 Descrição básica do projeto

A Presidência da República possuía, na época do edital, em seus cadastros o registro de aproximadamente 2.600 autoridades e servidores, 1.800 prestadores de serviço e terceirizados, tendo, ainda, uma média de 600 visitas/dia, bem como, o cadastro de 3.300 veículos, que utilizam seus estacionamentos. Quando da realização de eventos abertos ao público, era franqueada a entrada a centenas de visitantes, autoridades, fotógrafos e repórteres, e o sistema anterior era baseado somente na presença de seguranças postados em pontos estratégicos, visando impedir o acesso de pessoas não autorizadas às demais áreas do Palácio do Planalto, o mesmo ocorrendo com as demais instalações (Anexos e Palácios).

A implantação do sistema de controle de acesso através de *Smart Cards*, juntamente com o sistema de monitoramento por meio de circuito fechado de Televisão, permitiriam um controle efetivo, com redução dos riscos e diminuição da ocorrência de incidentes, advinda da aplicação de recursos de segurança on-line, com armazenamento de imagens e eventos.

O projeto, denominado de Projeto Sistema Integrado de Supervisão (SIS) do Complexo da Presidência da República, foi dividido em dois módulos no edital de compra: Módulo de Circuito Fechado de Televisão (MCFTV) e Módulo de Controle de Acesso (MCAS), sendo este último o foco desse estudo de caso; porém, não serão omitidas algumas das informações acerca do MCFTV, principalmente, e fundamentalmente, devido à integração entre esses módulos.

8.4 Pré-requisitos do sistema

A tecnologia básica que fora exigida pra o Módulo de Controle de Acesso (MCAS) era baseada na utilização de *Smart Cards* que, principalmente devido à segurança criptográfica dos dados embarcados no cartão, permitiria a inserção de dados biométricos (impressão digital) para validação positiva nos pontos de acesso considerados de alto risco, gerando um ganho em flexibilidade na operação, sem degradação de desempenho, e baixo custo de gerenciamento de dados biométricos; tags RFID ativos; dados biométricos (impressão digital); e em técnicas de identificação

biométrica facial em Vídeo Digital (reconhecimento facial), devendo restringir o acesso de pessoas e veículos a áreas não autorizadas.

O sistema de cartões de identificação deveria possuir as seguintes características:

- 10.000 cartões do tipo *Contactless Smart Card* (sem contato), de 1kB, conforme normas de padronização ISSO 14443-A. Foram escolhidos, principalmente, por apresentar maior agilidade nas operações de leitura/escrita, durabilidade, segurança, capacidade de multi-aplicação e maior flexibilidade para personalização.

- 70 leitores de *smart cards* para catracas, portas, etc., que fossem adequadas para uso interno ou externo (resistentes a intempéries), e que deveriam operar sem a necessidade de efetuar consultas à central de segurança para validar as informações lidas, pois os cartões conteriam todas as informações necessárias à validação do acesso

- Proteção criptografada dos dados embarcados no cartão

- Permitir a leitura e inserção de dados no cartão do usuário, no momento da aproximação do leitor

- Constar no cartão as áreas com acesso franqueado e dados biométricos (impressão digital) para a validação positiva nos pontos de acesso onde fosse necessário o controle

- Permitir a restrição dos acessos de pessoas e veículos a áreas não autorizadas, utilizando meios físicos de bloqueio, conforme a conveniência, tais como: catracas, portas com tempo de abertura monitorado e cancelas com automatizadas e informatizadas, ou até mesmo, sem efetuar restrição, porém, sinalizando a ocorrência da tentativa de acesso através de alarmes sonoros e visuais na central de segurança. Deveriam ser utilizados, para isso, leitores de s*mart cards*, suas respectivas antenas, e leitores biométricos, quando necessários, para garantir maior segurança no acesso a áreas reservadas

- Todas as solicitações de acesso, bem como as imagens da face e do documento de identificação dos usuários capturadas, deveriam ser gravadas e armazenadas em banco de dados específico para este fim e nos cartões – neste, exceto as imagens

- O software deveria possuir recursos de controle de tentativas de arrombamento, de tentativas de acesso indevido e do tempo de abertura de portas, gerando alarmes quando o tempo de abertura fosse acima do ajustado

- Permitir a verificação da data, hora e local dos acessos realizados pelo proprietário do *smart card*

- Interagir com o Módulo CFTV para a recuperação das imagens correspondentes a cada evento gerado e analisá-los dentro da mesma interface

- Permitir o registro, em base de dados para auditoria, da gravação de todos os eventos, tais como eventos de controle de acesso autorizados, não autorizados e eventos administrativos, como, por exemplo, a criação de um novo operador

- Permitir, de acordo com o nível de segurança, que determinados pontos de acesso, como salas com acesso restrito, operassem com dupla tecnologia de identificação ou validação positiva através do processo de leitura do *smart card* e biometria de impressão digital. A dupla tecnologia, quando se fizesse necessária, não deveria interferir em tempos de resposta do sistema, uma vez que os dados de validação biométrica fariam parte dos dados embarcados nos *smart cards*

- Implementação da função "Dedo do Pânico" nos 18 pontos de acesso sob controle de identificação biométrica. Tal função consiste no cadastramento de uma impressão digital para ser utilizado quando a pessoa estivesse agindo sob coação. Quando fosse utilizada essa impressão digital para acessar o local, seria emitido um alerta na central de segurança

- As estações de monitoramento, situadas nas entradas das instalações, deveriam exibir, quando solicitado pelo operador, a foto do usuário, pré-cadastrado no sistema para confirmação visual no momento da solicitação de acesso pela barreira física ou óptica. Nos pontos de controle considerados de alta segurança (salas com acesso restrito), deveria ser aplicada dupla tecnologia de identificação – *smart cards* e verificação de impressão digital (biometria) -, a fim de que fosse melhorada a eficiência do controle e que fosse agilizado o acesso, quando houvesse

Também estavam previstas as seguintes características no Módulo de Controle de Acesso do sistema a ser adquirido:

- Seria parte integrante da solução o monitoramento de eventos não autorizados, com a geração de alarmes em tela gráfica, através de mapas gráficos das instalações

- Deveria ser implementado nas áreas perimetrais um sistema de controle de intrusão baseado em barreira eletrônica (infravermelho, micro-ondas, etc.), integrado ao MCAS, permitindo, assim, um monitoramento efetivo das grandes áreas

- Sistema de Tags RFID ativos para que fosse possível o monitoramento da movimentação de pessoas e veículos, para controle de visitantes e veículos, fornecendo o controle das informações, em tempo real, sobre a localização do visitante dentro das instalações, tempo de trajeto, áreas acessadas, emitindo, ainda, um alerta, caso o visitante acesse alguma área que não lhe foi franqueado o acesso. Deveria possuir as seguintes características:

    - 103 Leitores RFID, para identificação de visitantes e veículos, com alcance suficiente para que fosse realizada a detecção sem diminuição nas velocidades do fluxo de veículos e pessoas existente, com suas respectivas antenas, posicionadas em locais estratégicos, ou seja, os leitores para identificação veicular deveriam ser instalados nos acessos aos estacionamentos (junto às cancelas), e os para identificação pessoal, nos pontos de acesso e corredores

- 10.000 tags RFID ativos RW (regraváveis) que seriam cadastrados e emitidos pelas Estações de Credenciamento utilizadas para cadastramento de usuários (visitantes, prestadores eventuais, veículos, etc.)

- Controle de visitantes com captura de imagem digital de documento, frente e verso, e face da pessoa, para que fosse possível, assim, a emissão do tag de visitante, determinando a rota de circulação autorizada e as respectivas zonas permitidas ao acesso, com tempo determinado pelo operador e controlado pelo sistema

- Entrada automática de veículos cadastrados, sempre que a leitura da placa do veículo (constante no MCFTV) e a identificação do tag forem positivadas pelo sistema - os dados do veículo deveriam ser previamente cadastrados no sistema

- Função *Anti-passback* implementada dentro do *smart card* do usuário. Tal função se traduz no impedimento de um mesmo cartão sair duas vezes de um local sem registrar uma entrada, ou vice-versa

- Validação e autorização independente de servidores e listas de acesso (consulta direta aos dados gravados no *smart card*), o que permitiria operação off-line e utilização da rede corporativa

- Software de gerenciamento, cadastramento de visitantes, integração com MCFTV, diferentes níveis de acesso, restrição de acesso a cartões extraviados ou cancelados e acesso imediato à janela no momento de ocorrência do evento

Também eram previstas as seguintes características acerca da integração entre o Módulo de Controle de Acesso (MCAS) e o Módulo de Circuito Fechado de Televisão (MCFTV):

- O MCAS deveria ser integralmente aderente ao MCFTV a fim de possibilitar automaticamente, no caso de alarme, a seleção de exibição da câmara referente à zona alarmada em estações de monitoramento, além de iniciar a gravação das imagens

- O MCAS deveria contemplar a instalação de salas com acesso restrito, devendo as mesmas possuir leitor de *smart card* para abertura externa e interna, leitor de dados biométricos (caso necessário), trava eletromagnética, dispositivo de fechamento automático de porta e sensor de porta aberta. Estas salas, além suportarem a inclusão do leitor de dados biométricos, possuiria, também, uma lista restrita de usuários franqueados

8.5 Solução implantada

Tendo em vista as características exigidas, a solução adotada pela Presidência da República Federativa do Brasil foi da empresa Telemática Sistemas Inteligentes LTDA..

8.5.1 Software de Aplicação

Tal sistema é uma plataforma, que contém vários subprogramas, dentre eles, o sistema de controle de acesso e coleta de ponto. O Suricato, que é o software de aplicação, integra várias tecnologias de identificação para acesso, dentre elas, *smart cards*, biometria digital e facial, sendo esta última apenas quando da integração com sistema de CFTV (Circuito Fechado de Televisão). Ele também armazena históricos de todas as informações de colaboradores, através de um registro de admissão até o seu desligamento.

O Suricato utiliza a tecnologia dos leitores CODIN, também da Telemática, para o controle de pessoas, objetos e veículos em áreas supervisionadas e restritas ao acesso comum. Na falta de comunicação (da rede de dados ou elétrica), os CODIN's alteram para o modo off-line, garantindo, assim a continuidade do acesso seguro das pessoas autorizadas. A segurança interna do sistema é garantida através de perfis de acesso e senhas, configuradas na instalação do produto. A interface do sistema, com seus respectivos menus, é mostrada na figura 8.1.

Figura 8.1 – Interface do Sistema Suricato

Estrutura

Neste menu, como mostrado na figura 8.2, existem os cadastros de dados obrigatórios para o sistema Suricato.

Cadastro de Empresa

Que é acompanhada do cadastro de suas filiais, centros de custos, organogramas e empresas terceirizadas.

Figura 8.2 – Menu Estrutura do Sistema Suricato

Cadastro de Planta

O cadastro da Planta define o nome de uma área que será referenciada para monitoração dentro de uma empresa e ao mesmo tempo, será dividida em segmentos denominados locais, onde serão instalados os dispositivos controladores.

Juntamente ao cadastro da Planta, faz-se necessário o cadastro de Portarias e Recepção, permitindo desta forma, a identificação do local que o visitante foi cadastrado.

Feriados

A tabela de Feriados será utilizada para controle de acessos e coleta de dados de ponto, com as restrições pertinentes a esses dias especiais.

Escala

O cadastro de Escala será definido para cada tipo de jornada de trabalho, sendo relacionada a cada colaborador para restrição do seu acesso e/ou coleta de seu ponto.

Situações Trabalhistas

Cadastra as diferentes situações dos colaboradores na empresa, bem como regras de acesso que serão geradas em cada situação. Exemplos de situações:

- Acidente de trabalho que impeça o acesso do colaborador por afastamento

- Férias, período em que o colaborador deverá estar com seu acesso bloqueado na empresa

Cargos

Cadastra os Cargos e Estruturas (em Níveis) da Empresa, criando uma hierarquia. Pode ser utilizado nas gerações de relatórios, consultas e filtros de distribuição de acessos e jornadas de trabalho. Filtro é uma funcionalidade do sistema que permite realizar uma seleção de, por exemplo, cargos para liberar, ou não, o acesso a um determinado local.

Nacionalidades

Cadastra as nacionalidades e as relaciona ao país.

Dispositivos

Todos os cadastros de dispositivos (equipamentos) como CODIN's, cancelas, catracas, câmeras e leitoras devem ser efetuados nesse menu, como mostrado na figura 8.3.

Cadastro de CODIN

Os dispositivos controladores (CODIN's) são incluídos no sistema nas seguintes etapas:

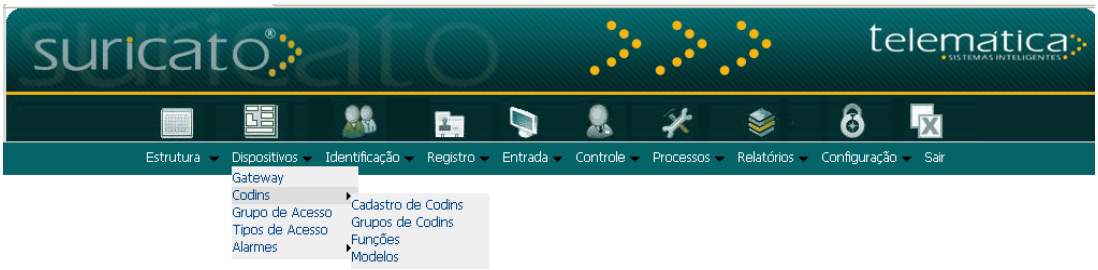

Figura 8.3 – Menu "Dispositivos" do Sistema Suricato

- Gateway
- Funções
- Cadastro

Grupo de Acesso

É necessário cadastrar o grupo de acesso no sistema para que seja informado através de quais dispositivos de controle (CODIN's, por exemplo) os colaboradores terão acesso.

Tipos de Acessos

O Tipo de Acesso é o estado da marcação do crachá que será exibido no display dos CODIN's ou catracas da Telemática, no momento da passagem do cartão de identificação do usuário.

São Tipos de Acesso, por exemplo, a mensagem exibida como "ACESSO PERMITIDO".

Alarmes e Reações

Devem ser informados no sistema todos os tipos de alarmes que serão gerenciados e qual o procedimento que deve ser realizado para cada tipo de alarme gerado. Como exemplo de procedimento, podemos citar a obrigatoriedade da realização de uma chamada para um determinado telefone.

Reações são processos automáticos gerados a partir de um alarme, ou seja, o Suricato deve, se assim configurado, enviar um e-mail assim que identificar um alarme, sem a intervenção do operador.

As seguintes funções podem ser executadas no menu de alarmes, como mostrado na figura 8.4:

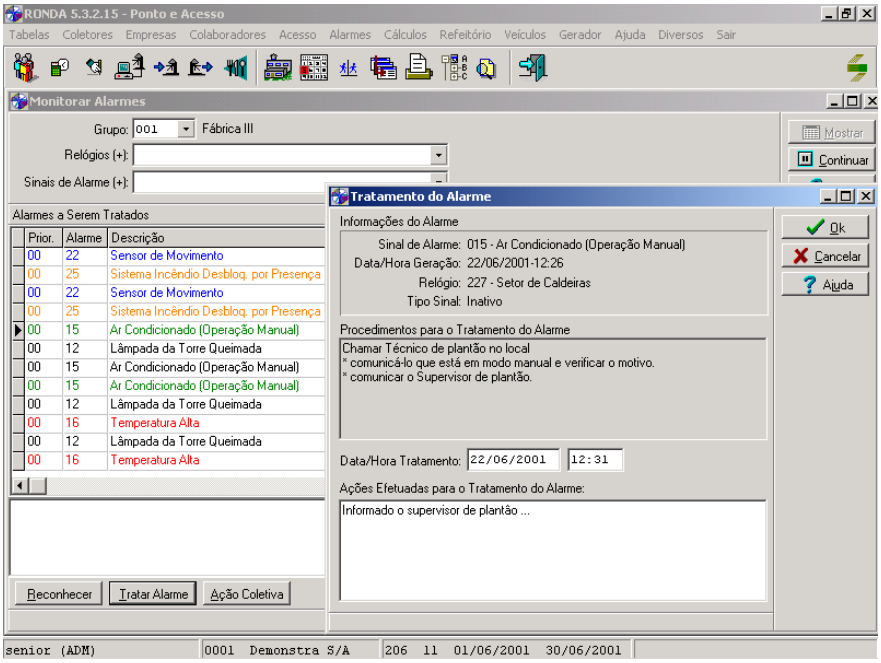

Figura 8.4 – Menu de alarmes do Sistema Suricato

- Recepção e monitoramento on-line de alarmes de intrusão, incêndio, emergência, violação e de falhas dos dispositivos de controle
- Controle do reconhecimento e do tratamento dos alarmes efetuados pelos operadores
- Visualização dos alarmes segundo a prioridade de tratamento
- Histórico de todos os alarmes recebidos e tratados
- Consultas e relatórios estatísticos do controle de alarmes

Identificação

No menu Identificação, como mostrado na figura 8.5, são registradas todas as pessoas que terão acesso às dependências da empresa.

Figura 8.5 – Menu "Identificação" do Sistema Suricato

O Suricato mantém um histórico sobre as alterações realizadas no cadastro de pessoas. Os históricos informam data e hora de alteração para cada uma das funções controladas:

- Filial
- Local
- Cargo
- Escala
- Afastamento
- Crachá
- Centro de Custo

- Contratos

Visitantes

Ainda neste menu, todos os visitantes são cadastrados previamente para uso pelo Módulo Entrada, normalmente instalado em Portarias e Recepções. Os dados de um visitante poderão ser alterados, bem como inseridos para futuros pré-agendamentos.

Pessoas Não Gratas

Pessoas cujos acessos devem ser bloqueados e alertados em eventual tentativa de acesso

Registro

Esse item de menu, como mostrado na figura 8.6, engloba as funcionalidades do registro de identificação:

Figura 8.6 – Menu “Registro” do Sistema Suricato

Crachá

Indispensável como passaporte de acesso, o crachá contém as informações para liberar ou bloquear o acesso de uma pessoa, créditos para refeitório, faixas horárias de acesso, jornada de trabalho, validade de acesso, entre outros.

A liberação de acesso é validada somente após a conferência dos seguintes itens:

- **Histórico de Afastamento do Colaborador –** verifica se o colaborar não está afastado

- **Grupo de Acesso –** verifica se o colaborador tem acesso ao local

- **Faixa Horária –** verifica se o colaborador está dentro da sua faixa de horário

- **Validade do Crachá –** verifica se o crachá não está com data expirada
- **Crédito de Acesso –** verifica se o local é restrito a crédito de acesso
- E outros crivos configurados no perfil de acesso individual.

Registro de Ocorrência

O Registro da ocorrência tem a mesma funcionalidade do "Livro de Ocorrência", ou seja, registra dados de eventos que ocorrem nas zonas de controle de uma empresa.

Perfil de Acesso

Essa função apresenta na tela, a partir do número da matrícula, todas as informações pertinentes a um registro de uma pessoa.

Cadastro de crachá

É utilizado como garantia para que uma pessoa não registre um crachá desconhecido no sistema, certificando que apenas crachás cadastrados no sistema podem ser atribuídos a uma pessoa, a um ativo ou a um objeto.

Cadastro de Crachá Mestre

Esse tipo de crachá é geralmente utilizado por uma pessoa, que tem acesso a todos locais da empresa. Quando o crachá mestre é cadastrado, ele é aceito em qualquer coletor dentro da empresa, não fazendo restrições de acesso.

Bloqueio e Desbloqueio de Pessoa e Crachá

Bloqueando uma pessoa, mesmo que ela receba outro crachá titular ou provisório, o sistema irá informar ao operador que essa pessoa está bloqueada.

Ao bloquear um crachá, o empregado usuário desse crachá perde o acesso às dependências da empresa, mas sua condição como titular não se altera, podendo entrar na empresa com outro crachá (provisório).

O desbloqueio ocorre de maneira rápida e sem necessidade de informação adicional.

Controle de Áreas Restritas

Concede a uma pessoa um acesso, por tempo determinado, complementando seu grupo de acesso.

Envio de Mensagens

Neste módulo é possível cadastrar uma mensagem de até 16 caracteres que deve ser exibida no display do CODIN para um crachá especifico, no momento de sua passagem pela leitora.

Controle de Acesso

Atribui créditos de acesso para colaboradores, individual ou coletivamente. Os créditos de acesso são utilizados, principalmente, para controle de cotas de refeitório.

Entrada

Recebendo um Visitante

O menu Entrada é utilizado para gerenciar a entrada de visitantes, conceder crachás provisórios e dar baixa de crachás para reutilização. Possui acesso direto através da interface do sistema Suricato, como mostrado na figura 8.7.

Figura 8.7 – Menu “Entrada” do Sistema Suricato

Provisórios

Permite o cadastro de crachás provisórios. Em uma eventual perda ou esquecimento do crachá titular do colaborador, é possível atribuir ao mesmo outro crachá, dito provisório, para o acesso as dependências da empresa. Ao atribuir um crachá provisório, o Suricato, assume automaticamente todo o perfil de acesso do crachá titular.

Materiais

Efetua o controle de entrada e saída de materiais na empresa. É realizado através das notas fiscais emitidas para os materiais em trânsito. São controladas as quantidades de material, a pessoa responsável e a origem - entrada ou saída.

Controle

Comandos

Gera e controla os comandos a serem enviados aos CODIN's, como bloquear ou desbloquear uma catraca e comandos de liberação de acesso em caso de situação de emergência.

Geração de Listas

Gera as listas, ou seja, arquivos que são enviadas aos CODIN's para restringir ou liberar o acesso de determinados colaboradores quando o sistema operar, eventualmente, em modo offline, ou seja, sem comunicação com o servidor de banco de dados. Possui acesso através do menu Controle do sistema Suricato, como mostrado na figura 8.8.

Figura 8.8 – Menu "Controle" do Sistema Suricato

Monitorar

Monitorar com Grid

Permite o acompanhamento em tempo real dos acessos - válidos ou inválidos - de pessoas em uma determinada localidade da empresa. São exibidos os dados cadastrais da pessoa, bem como sua fotografia.

Monitorar Alarmes

Permite o acompanhamento em tempo real de todos os alarmes gerenciados e configurados pelo sistema.

Os Alarmes podem ser reconhecidos e tratados de acordo com os procedimentos exibidos em tela e previamente configurados.

Monitorar com Plantas

Monitora online, através de ambiente gráfico, com plantas baixas das instalações, como mostrado na figura 8.9. Visualiza toda área controlada e mantém integração com os alarmes, sensores e acessos configurados no sistema.

Todos os eventos são apresentados dinamicamente na interface. É possível reconhecer e tratar o alarme.

No aspecto funcional, o Controle com Plantas permite *zoom* das áreas na navegação e alteração de planta de maneira rápida e amigável, tudo com controle na tela.

Integrada ao sistema CFTV, mostra imagens ao vivo dos locais onde há câmera ou reproduz o momento exato de um evento (alarme).

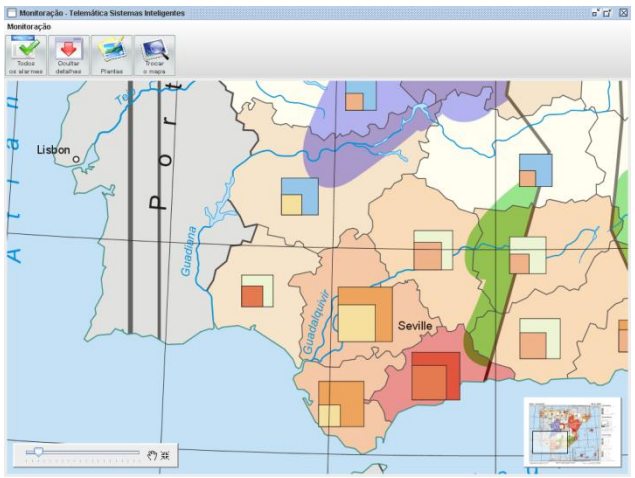

Figura 8.9 – Monitoramento com Plantas, do Sistema Suricato

Processos

Processos Automáticos

Executa processos agendados de forma automática, sem nenhuma interação com usuário, através de um servidor de aplicações. Utiliza-se da estrutura WEB para execução dos processos, o mesmo utilizado para o ambiente dos aplicativos do sistema Suricato, como mostrado na figura 8.10.

Toda a parte do agendamento e cadastramento das tarefas é feita no sistema. O cadastro dos processos automáticos está disponível em vários itens de menu e em "Processos Automáticos". Existem vários sub-menus, um para cada tipo de processo que pode ser cadastrado.

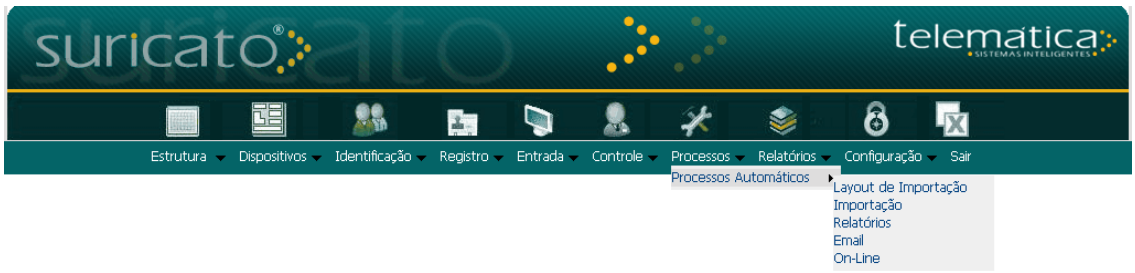

Figura 8.10 – Menu “Processos” do Sistema Suricato

Importação

Esse processo realizará automaticamente a importação do arquivo texto informado no campo "Arquivo de Entrada", utilizando o padrão inserido no campo “*Layout* de Importação”. O *layout* deve ter sido criado previamente. Este arquivo do tipo texto seria, por exemplo, o cadastro de um funcionário.

Relatórios

Essa função gera o relatório selecionado, com agenda de data e hora ou intervalo de tempo pré-definidos.

O formato de arquivo gerado é PDF e o destinatário poderá recebê-lo por e-mail, numa conta definida na configuração.

E-mail

Configurar e-mails para serem enviados automaticamente, com dados como mensagem (texto), remetente, destinatários e assunto.

On-Line

São realizadas neste item as configurações de comandos que devam ser enviados aos CODIN's de acordo com este agendamento. Por exemplo, a geração e a carga - download - nos CODIN's da lista (arquivo) de liberação de acessos.

Configuração

Através deste menu são definidas as configurações do sistema, como mostrado na figura 8.11.

Figura 8.11 – Menu "Configuração" do Sistema Suricato

Configuração de E-mail

Neste módulo, configura-se o servidor de e-mail utilizado na empresa.

Usuários / Grupo de Usuários (Login / Logout)

Para acessar (LOGIN) o sistema, é necessário atribuir autorização de acesso às pessoas responsáveis pela utilização do Suricato.

Aplicativos

Esta função especifica as permissões de usuários, ou seja, todas as aplicações de cadastros, incluindo as funções de inclusão, alteração, exclusão e consulta devem ser descritas em Aplicativos.

Crachás e Definições Gerais de Crachá

Devem ser registradas as configurações do crachá e suas funcionalidades como pré-cadastro e provisórios e também configurações de utilização do crachá no sistema, ou seja, todas as validações e consistências que serão associadas ao seu uso.

Controle de Frota

Permite as seguintes funcionalidades, como mostrado na figura 8.12:

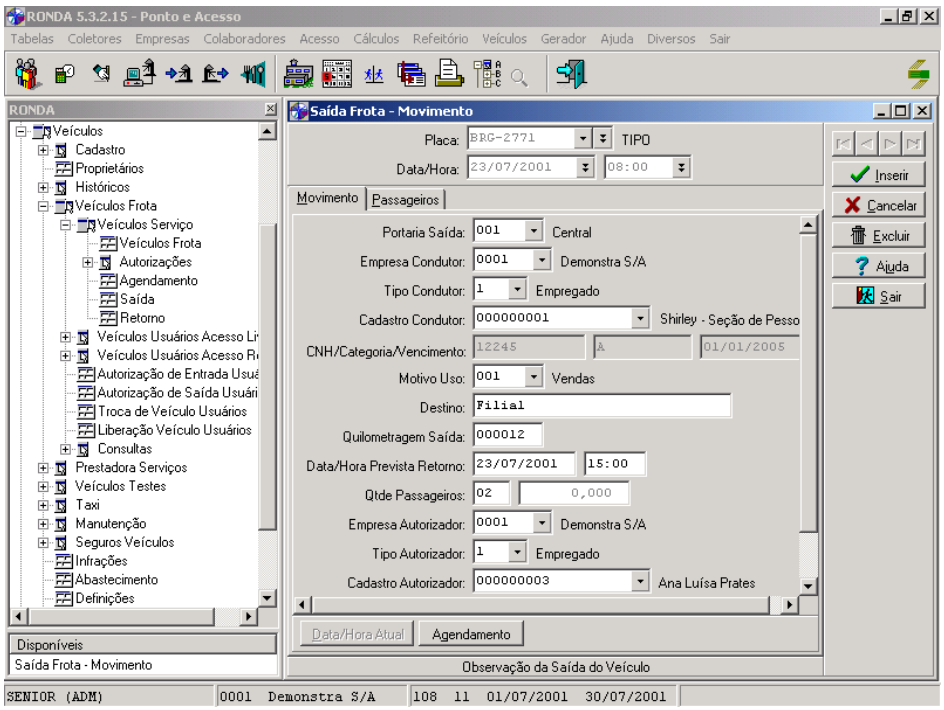

Figura 8.12 – Menu de controle de frota, do Sistema Suricato

- Controle da movimentação de saída e de retorno dos veículos da frota e dos veículos dos colaboradores usados a serviço da empresa
- Controle da entrada e da saída de veículos de particulares, de prestadores de serviço e dos veículos de carga e descarga
- Controle da movimentação dos veículos de teste das empresas montadoras
- Agendamento do uso dos veículos da frota
- Controle dos veículos da frota: manutenções preventivas e corretivas, abastecimentos e consumo de combustível, quilometragem percorrida, seguro
- Controle dos condutores dos veículos da frota: veículos autorizados, categoria habilitação, vencimento habilitação (CNH), infrações de trânsito, pontos na carteira
- Agendamento de táxis e conveniados
- Controle de ocorrências de trânsito, tais como sinistros e reclamações

- Consulta do proprietário do veículo estacionado
- Consulta da situação do veículo: disponível, em uso, sem retorno, em manutenção, agendado, imobilizado para conserto
- Relatórios estatísticos para o acompanhamento da movimentação e da utilização dos veículos

Relatórios e Consultas

Os Relatórios emitidos pelo Suricato estão disponíveis impressão e visualização em tela. Consultas também são visualizadas em tela.

Os relatórios são gerados em formato padrão PDF para impressão ou leitura em tela.

As consultas disponíveis no sistema, através de solicitação direta no menu do sistema Suricato, como mostrado na figura 8.13, são:

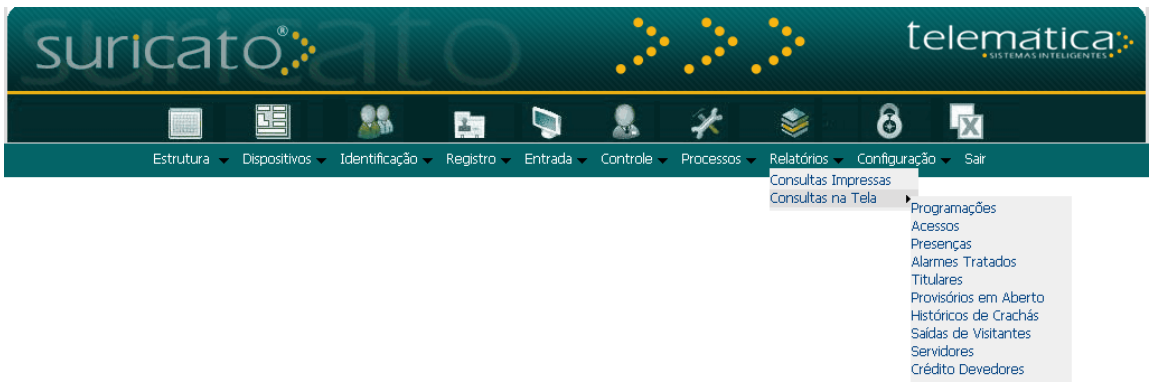

Figura 8.13 – Menu “Relatórios” do Sistema Suricato

- Programações
- Acessos
- Presenças
- Alarmes Tratados
- Titulares
- Provisórios em Aberto
- Histórico de Crachás

- Saídas de Visitantes
- Colaborador
- Controle de Devedores de Créditos de Refeitório

8.5.2 Leitores

Os leitores utilizados na solução são os CODIN's MD 400, com leitura de biometria digital, os CODIN's MD 410, para cancelas e portas, as catracas PD 300 e GT 300, com leitores integrados, e os leitores *smart card* de mesa.

CODIN MD 400

São leitores de cartões de proximidade, de código de barras, de *Contactless Smart Cards* e de biometria digital, como o mostrado na figura 8.14.

Figura 8.14 – Leitor CODIN MD 400, integrante do Sistema Suricato

Suas principais características são:

- Possui memória de armazenamento do log de operações e/ou transações
- Armazena todas as regras de acesso voltadas ao seu respectivo ponto de controle e as cruza com as regras estabelecidas para cada usuário, permitindo ou não um determinado acesso
- Capacidades de registro de log de operações e Backup para falta de energia e/ou comunicação off-line
- A coleta de informações pode ser realizada de modo on-line ou off-line, de acordo com a melhor arquitetura definida pelo cliente para sua aplicação

- Resistente a situações críticas de trabalho, ou seja, locais de temperaturas oscilantes, umidades extremas, ambientes sujeitos a condensação

- Operação: Pode trabalhar on-line, off-line, Stand-alone ou Cliente x Servidor realizando leitura e escrita em cartões smart card

- Possibilita instalar sensores para informar ao sistema quando uma porta ou fechadura se encontram abertas, ou pode ser instalado um sensor no próprio gabinete do equipamento para detectar a abertura do mesmo

CODIN MD 410

São leitores sem leitura de biometria digital, como o da figura 8.15, utilizados em cancelas e portas, como unidade remota dos MD 400, sendo controlados por estes.

Figura 8.15 – Leitor CODIN MD 410, integrante do Sistema Suricato

PD 300

São catracas de controle de acesso, como a da figura 8.16, com leitores magnéticos, de código de barras, de cartões de proximidade, smart card e de biometria digital integrados. Elas funcionam como bloqueios de acesso físico. Podem operar no modo online ou offline, de acordo com o sistema no qual estão inseridas. No modo online toda a validação de acesso é feita em uma base de dados, bem como os registros contendo as informações do acesso em tempo real. Já no modo offline toda a validação de acesso é feita na memória do próprio coletor de dados, bem como os registros contendo as informações do acesso que serão coletadas posteriormente.

Figura 8.16 – Catraca PD 300, integrante do Sistema Suricato

GT 300

São catracas, como a da figura 8.17, destinadas ao uso de pessoas portadoras de deficiência, que contém leitores magnéticos, de código de barras, de cartões de proximidade e de *smart cards*.

Figura 8.17 – Catraca GT 300, integrante do Sistema Suricato

Leitores *Smart Card* de mesa

Os leitores de *Contactless Smart Cards*, como o da figura 8.18, foram desenvolvidos para efetuar o cadastro de visitantes de acesso. São instalados na porta Serial ou USB do PC, e funcionam integrados com o Sistema de Controle de Acesso. Têm um alcance de leitura de, aproximadamente, 50mm.

Figura 8.18 – Leitores *Smart Card* de mesa, integrante do Sistema Suricato

8.5.3 Tags

Foram utilizados na solução implantada *Contactless Smart Cards Mifare*® que operam na freqüência de 13,56MHz e tags ativos, que operam na freqüência de 433MHz, conforme as figuras 8.19 e 8.20. Os tags ativos possuem as seguintes dimensões: 86mm x 54mm x 5mm e pesam 15g. As características de ambos os tags, tanto dos *Contactless Smart Cards* como dos tags ativos, foram detalhadas em capítulo específico deste presente trabalho.

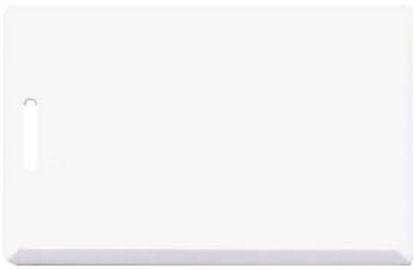

Figura 8.19 – Contactless Smart Card Mifare®, 13,56MHz

Figura 8.20 – Tag ativo, 433MHz

8.6 Futuras ampliações

Há previsão da implementação de outras funcionalidades ao sistema. Uma delas é o controle e monitoramento de ativos (patrimônio), estimados em cerca de 20.000 itens, através da colocação de tags nestes. Outra é a efetiva instalação de tags ativos nos veículos, de forma a permitir o controle e o monitoramento da frota, tendo em vista que essa função foi prevista no projeto, mas ainda não foi implementada.

Estando o sistema completamente instalado, através dos dois módulos (MCAS e MCFTV) e do controle de ativos, outras possíveis ampliações são baseadas na utilização das informações constantes na Base de Dados, a fim de implementar funcionalidades decorrentes de sistemas periféricos de comunicação, energia, climatização, iluminação, etc.. Um exemplo é um colaborador que entra no edifício, o sistema de controle de acesso registra sua entrada e as luzes da sua sala são acesas, o ramal telefônico é ligado, o ar condicionado é acionado, o computador é inicializado, etc.; o inverso ocorrendo quando da saída deste do prédio, otimizando, assim, a utilização de energia e demais recursos, permitindo a redução dos custos operacionais.

Outra funcionalidade muito importante a ser implementada no sistema é a certificação digital. Essa função de segurança é feita através da utilização de tags com dois processadores: um para realizar as operações da certificação digital, como autorização das transações utilizando criptografias mais complexas, e outro para as demais operações da comunicação com o leitor. Essa função permite, dessa forma, que a comunicação tag-leitor, e vice-versa, seja dotada de uma seguridade muito maior, garantindo que os dados, mesmo sendo interceptados, não sejam captados e/ou alterados.

CAPÍTULO 9

Desafios para o sucesso do RFID

A tecnologia de RFID está crescendo muito rapidamente. As iniciativas do *Wal-Mart* e do *DoD*, as quedas crescentes dos custos de implementação da tecnologia, o desenvolvimento de um padrão para o RFID e o alto retorno dos investimentos no setor são fatores que contribuem para essa evolução. Outra iniciativa que deve produzir um efeito de redução de custos ainda maior é a lei *US Health*, que exige que até 2010 todos os medicamentos que necessitam de receita nos Estados Unidos deverão conter um tag, posto pelo fabricante do produto, a fim de conter o enorme crescimento da falsificação de remédios.

Apesar de tudo isso, há vários desafios a serem transpostos pela tecnologia de RFID para que se torne uma unanimidade entre os provedores de solução. Tais desafios se devem, principalmente, às práticas do mercado e ao fato de ser uma tecnologia nova.

Alguns dos desafios são:

- **Precisão:** A cada vez maior necessidade de confiabilidade e precisão das informações obtidas pelos sistemas de coleta de dados exige um constante aprimoramento dos mesmos. Este é um dos principais desafios para os fabricantes de leitores e tags, que precisam ser continuamente atualizados visando assegurar a precisão absoluta nos processos em que são aplicados tais componentes.

- **Integração das empresas:** Tendo em visa a não existência de uma padronização das informações e de normas comuns para o RFID, muitas empresas do setor encontram dificuldades na adaptação de seus sistemas às novas exigências tecnológicas.

- **Tags para cada tipo de material:** O desempenho de um sistema de RFID depende do tipo de objeto que está sendo monitorado, bem como do ambiente onde o sistema está implantado. Dessa forma, objetos que contenham materiais como metais ou líquidos, que absorvem a energia RF emitida por um leitor comum, comprometem a aplicabilidade da solução de RFID. Para que haja tal implantação, se faz necessária a utilização de tags especiais para cada tipo de material. Isso representa um grande problema para a afirmação da tecnologia, visto que uma empresa que possui diversos tipos de produtos, e que deseje instalar um sistema de RFID, precisará adquirir e lidar com diversos tipos de tags, o que torna a solução muito complexa e, na maioria das vezes, cara.

- **Inexistência de um padrão mundial:** Os sistemas de RFID, normalmente, operam em regiões sem licença, do espectro de freqüências. Ou seja, o leitor de RFID deve seguir alguns princípios operacionais para que opere sem a necessidade de uma licença de transmissão de rádio especial, emitida pelos órgãos competentes. O governo de cada país é responsável pela definição das partes do espectro que não necessitam de licença para operação, e, destes, quais são liberadas para o RFID. As divergências entre os governos e as definições já existentes, juntamente com o demorado processo de padronização, levam a solução dessa questão ao longo prazo.

- **Custo:** Este é a principal barreira da evolução da tecnologia de RFID, representando, assim, o maior desafio para a indústria do setor. O alto custo de uma solução de RFID, principalmente quando comparado a outros sistemas, como o Barcode,

muitas vezes inviabiliza a implantação da mesma. Ou limita a aplicação do RFID no monitoramento e/ou rastreamento de produtos de alto valor, ou de conjuntos de produtos, como pallets e fardos

CAPÍTULO 10

Conclusões

O objetivo deste trabalho foi realizar uma análise sistêmica da tecnologia de identificação por radiofreqüência, ou RFID, com pouca ênfase aos aspectos técnicos e mais voltada para o funcionamento geral desta, bem como à caracterização de tudo o que compõe o sistema. Tal meta foi atingida com êxito, tendo em vista que foram detalhados, ao longo deste, cada componente, seus diversos tipos e suas respectivas funções dentro do sistema, sempre buscando um enfoque diferente dos trabalhos anteriores, relacionados a esse assunto, realizados na UnB.

O estudo de caso foi muito importante para elucidar a aplicabilidade do RFID, dando ênfase a um dos principais componentes do sistema, que é o software de aplicação, que gerencia todas as informações obtidas nos processos de leitura. Também foi muito importante efetuar esse estudo por se tratar de um caso de grande importância e por ter sido executado por uma empresa nacional, que venceu uma concorrência contra várias multinacionais, o que demonstra que o Brasil está no mesmo nível tecnológico do mundo, com relação ao RFID.

Tendo em vista as informações obtidas, passíveis de liberação pelos responsáveis, e a data da contratação da solução, conclui-se que a iniciativa da Presidência da República Federativa do Brasil à época foi bastante ousada, aderindo a uma tecnologia que ainda era muito pouco utilizada no país. Tal iniciativa, principalmente por se tratar de um órgão de tamanha importância como a Presidência da República, é fundamental para incentivar outros órgãos e empresas a também adotarem o RFID, contribuindo para a difusão da tecnologia no Brasil.

Efetuando-se uma análise de todos os benefícios trazidos com a implantação do sistema SIS, como o controle de quem acessa áreas que exigem alta segurança e o monitoramento dos visitantes, que algumas vezes eram encontrados vagando pelo interior das instalações, e traçando-se um paralelo entre as situações anterior e posterior à instalação do SIS, verifica-se que o sistema atendeu a todas as necessidades expostas pela contratante.

O RFID, apesar de ser uma tecnologia antiga, tendo em vista a data do seu surgimento, é muito nova se for observado o desenvolvimento pelo que vem passando nos últimos quinze anos, comparado ao que passou pelos mais de trinta anteriores. Como toda tecnologia que há pouco vem sendo descoberta, sofre com a descrença de muitos, o que se traduz no maior obstáculo que o RFID tem de transpor para se tornar uma tecnologia completamente difundida globalmente, como se tornou o código de barras, que hoje está consolidado. Porém, como visto, o RFID não é um concorrente direto do código de barras, portanto não o substituirá totalmente, principalmente devido ao custo da solução de um com relação ao outro. Mesmo assim, o estágio de maturação obtido pelo BarCode é uma meta a ser alcançada pelo RFID, para torná-lo uma unanimidade no mundo todo. Dessa forma, a previsão é de que nos próximos anos a tecnologia de RFID evolua muito, ainda mais considerando a adoção do padrão *ECPglobal Network*, que trará uma total integração do sistema, significando uma grande vantagem principalmente para a cadeia de suprimentos, na qual poderá haver um controle total dos produtos.

Imagina-se que muito em breve se consiga produzir um tag que custe menos de U$0,005, vencendo outra das principais barreiras da evolução do RFID, que é o preço.

Isso faria com que aumentasse ainda mais a difusão da tecnologia, podendo chegar, assim, aos pequenos estabelecimentos, que ainda vêem na implantação desta algo inviável economicamente. Um exemplo do descréscimo de valor proveniente da afirmação da tecnologia no mundo é o dos Smart Cards, visto que um cartão custava mais de 40 dólares no seu lançamento e hoje custa menos de 1 dólar.

Sendo assim, nos próximos anos o RFID estará cada vez mais integrado às vidas das pessoas, da mesma forma que a televisão, os computadores e os telefones celulares já estão.

Portanto, tendo em vista o crescimento exponencial das necessidades de utilização do RFID em uma economia cada vez mais globalizada, iniciativas da UnB em pesquisa e desenvolvimento relacionadas a essa tecnologia seriam extremamente importantes e, porque não dizer, quase que vitais na preparação de seu corpo discente, colocando-o em acordo com as tecnologias mais avançadas de identificação por radiofreqüência que, ao que tudo indica, chegaram para ficar.

Como sugestão, talvez a UnB talvez pudesse iniciar o processo de conhecimento interno do RFID proporcionando um “case” através da implantação do controle dos volumes da Biblioteca Central (BCE).

Referências Bibliográficas

1. LAHIRI, Sandip. ***RFID Sourcebook***, IBM Press, 2006.

2. HUNT, V. Daniel. PUGLIA, Albert. PUGLIA, Mike. ***RFID – A Guide to Radio Frequency Identification,*** John Wiley & Sons Inc., 2007.

3. MANISH, Bhuptani. SHAHRAM, Moradpour. ***RFID Field Guide: Deploying Radio Frequency Identification Systems,*** Prentice Hall PTR, 2005.

4. SANGHERA, Paul. ***RFID+ Study Guide and Practice Exam,*** Syngress Publishing,Inc., 2007.

5. Motorola Inc., http://www.motorola.com. Acesso em 7 de maio de 2008.

6. Sensormatic Electronics Corporation, http://www.sensormatic.com. Acesso em 7 de maio de 2008.

7. ZIH Corporation, http://www.zebra.com. Acesso em 7 de maio de 2008.

8. GLOVER, Bill. BHATT, Himansu. ***RFID essencials***, O'Reilly, 2006.

9. AUTO-ID Labs of MIT – Massachusetts Institute of Technology. *http://autoidlabs.mit.edu*. Acesso em 27 de outubro de 2007.

10. FINKENZELLER, Klaus. ***RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification,*** 2ª ed. John Wiley & Sons Inc., 2003.

11. RANKL,Wolfgang. EFFING, Wolfgang. ***Smart Card Handbook***, 3ª ed. John Wiley & Sons Inc., 2003.

12. Ministério da Agricultura, Pecuária e Abastecimento, http://www.agricultura.gov.br. Acesso em 8 de maio de 2008.

13. Integrated Technology Group, http://integratedtek.com. Acesso em 23 de março de 2008.

14. International Communication Union, http://www.itu.int. Acesso em 8 de maio de 2008.

15. Prefeitura Municipal de São Paulo, http://www.prefeitura.sp.gov.br. Acesso em 9 de maio de 2008.