César Filipe Duarte Cardoso

# Controlo de Acessos

César Filipe Duarte Cardoso

# Controlo de Acessos

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestrado em Engenharia Mecânica, realizada sob orientação científica de Prof. Doutor José Paulo Oliveira Santos, Professor Auxiliar do Departamento de Engenharia Mecânica da Universidade de Aveiro.

**O júri / The jury**

| | |
|---|---|
| Presidente / President | **Prof. Doutor António Gil D'Orey de Andrade Campos**<br>Professora Auxiliar da Universidade de Aveiro |
| Vogais / Committee | **Prof. Doutor José Paulo Oliveira Santos**<br>Professor Auxiliar da Universidade de Aveiro (orientador) |
| | **Prof. Doutor André Ventura da Cruz Marnoto Zúquete**<br>Professor Auxiliar da Universidade de Aveiro |

**Agradecimentos / Acknowledgements**

Em primeiro lugar agradecer aos meus pais e irmão, pelo seu apoio incondicional ao longo de todo o meu percursos académico. Ao Professor Doutor José Paulo Oliveira Santos, meu orientador, pela disponibilidade e colaboração. Aos meus amigos pelo apoio prestado a todos os níveis, e finalmente, um especial obrigado, aos colegas e amigos do laboratório, pela capacidade de ouvir, ajudar e motivar.

**Palavras-chave** sistemas de controlo de acessos; autenticação; identificação; NFC; sistema integrado; XBee; Android; Base de Dados; microcontrolador; dispositivo móvel

**Resumo** A presente dissertação propõem o desenvolvimento de um sistema de controlo de acessos físicos alternativo, tal como, no processo validar a implementação da tecnologia *Near Field Communication* como meio de identificação/autenticação nesta área. Os esforços para o desenvolvimento deste sistema foram orientados no sentido de demonstrar e propor uma solução baseada num protótipo funcional, de sistema de controlo de acessos físico dotado de tecnologia inovadora, para implementação em habitações comuns, que quer pelo baixo volume de soluções disponíveis no mercado, necessidade, ou preço, apresentam uma fraca aderência (baseado possivelmente, na desconfiança em termos de fiabilidade e/ou segurança). Analisando o panorama atual, onde o mercado, sob a forma de serviços, flui e apresenta um nível de convergência para um único dispositivo, constata-se a possibilidade de contribuir sob esta forma, no contexto de controlo de acessos. Este é um dos aspetos que sustentou a proposta de implementação nesta dissertação. O presente trabalho consistiu, numa primeira fase, na investigação do tema, desde a sua génese mais conceptual, às topologias e arquiteturas, principais tecnologias de comunicação de suporte, entre outros variadíssimos pontos relacionados. Este processo permitiu entender o contexto dos sistemas de controlo de acessos a nível cientifico/tecnológico, mas também, numa perspetiva de definição de objetivos da dissertação, entender o contexto deste tema na sociedade e mercado, determinando o escopo da solução proposta/implementação como um contributo técnico-científico, e desta forma, tentar induzir a experimentação da tecnologia *Near Field Communication* (NFC) em controlo de acessos físicos. Desta forma, entenda-se os objetivos traçados, como o primeiro passo, que pretende induzir o desenvolvimento de soluções em controlo de acessos ,baseados em NFC, para que num futuro este duo surja, sob a forma de produto robusto, flexível, e fiável.

**Keywords** access control systems; authentication; identification; NFC; integrated system; XBee; Android; Database; microcontroller; mobile device

**Abstract** This thesis proposes the development of an alternative physical access control system, as in the process, validate the NFC technology through the implementation of it as a tool of identification/authentication in this area. The efforts to develop this system were instructed to demonstrate and propose an approach based on a working prototype of physical access control system, equipped with innovative technology, and for deployment in public housing. This was motivated due to the poor adherence (based possibly on distrust in terms of reliability and/or safety), price, and need. Hence, the low volume of "*breakthrough*" solutions available in the market is a fact. Analyzing the current situation, where the market in the form of services ,flows and provides a level of convergence to a single device , in the context of access control systems, it appears to be the possibility to contribute in this way. This is one of the aspects that supported the proposal for implementation in this document. Initially, this work consisted in theme research, in a conceptual way at the most, addressing it's focus to the topologies and architectures, key support technologies of communication, among other numerous different points related. This process allowed to understand the context of access control systems in scientific/technological level, but also, in a perspective of defining objectives of the thesis, understand the context of this issue in society and market, determining the scope of the proposal solution/implementation as a technical and scientific input, and thus try to induce trial experiments of the NFC technology in access control systems. Therefore, understand the established objectives, as the first step, meant to induce the development of access control solutions, based on NFC, so that in the future this duo can emerge as a form of a robust,flexible ,and reliable product.

# Conteúdo

# Lista de Tabelas

# Lista de Figuras

# Unidades, Símbolos e Acrónimos

**ABAC** *Attribute-based access control*

**ACL's** *Access Control List's*

**API** *Application Programming Interface*

**APDU** *Application Protocol Data Unit*

**ARP** *Address Resolution Protocol*

**ASCII** *American Standard Code*

**AT** *Hayes Command Set*

**AWG** *American Wire Gauge*

**BD** Base de Dados

**BH** *Broadcast Hops*

**bps** *bits per second*

**CAT5** *Category 5 cable*

**CAT6** *Category 6 cable*

**CCA** *Clear Channel Assesment*

**CD** *Collision Detection*

**CID** *Cluster Identifier*

**CLH** *Cluster Head*

**CLK** *Clock Signal*

**cm** *centímetros*

**COM** *Communication Port/Serial Port Interface*

**CN** *Exit Command Mode*

**CPU** *Central Processing Unit*

**CRC** *Cycling Redundancy Check*

**CSMA** *Carrier-Sense Multiple Access*

**CTS** *Clear to Send*

**D6** *DIO6 Configuration*

**D7** *DIO7 Configuration*

**DAC** *Discretionary Access Control*

**DC** *Direct Current*

**DCL** *Data Control Language*

**DDL** *Data Definition Language*

**DEP** *Data Exchange Protocol*

**DH** *Destination Address High*

**DL** *Destination Address Low*

**DML** *Data Manipulation Language*

**DQL** *Data Query Language*

**DSSS** *Direct Sequence Spread Spectrum*

**DTL** *Data Transaction Language*

**DVD** *Digital Versatile Disc*

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

**EIA** *Electronics Industry Association*

**E.U.A** Estado Unidos da América

**FCS** *Frame check sequence*

**FFD** *Full Function Device*

**Gbit/s** *Gigabits*/segundo

**GHz** *gigahertz*

**GND** *Ground (reference voltage)*

**GSM** *Global System for Mobile Communications*

**HF** *High Frequency*

**HVAC** *heating, ventilation, and air conditioning*

**I2C** *Inter-Integrated Circuit*

**ICMP** *Internet Control Message Protocol*

**ICSP** *In Circuit Serial Programming*

**ID** *Identity*

**IDE** *Integrated Development Environment*

**IEC** *International Electrotechnical Commission*

**IEEE** *Institute of Electrical and Electronics Engineers*

**I/O** *Input/Output*

**IP** *Internet Protocol*

**ISO** *International Organization for Standardization*

**JIS** *Japonese Industrial Standard*

**JPEG** *Joint Photographic Expert Group*

**kB** *Kilobyte*

**kbit/s** *Kilobits*/segundo

**kHz** *quilohertz*

**LAN** *Local Area Network*

**LF** *Low Frequency*

**LLC** *Logic Link Control*

**LLCP** *Logical Link Control Protocol*

**LRC** *Longitudinal Redundancy Check*

**MACM** *Mandatory Access Control model*

**MAC** *Medium Access and Control*

**Mbit/s** *Megabits*/segundo

**MHz** *megahertz*

**MIME** *Multipurpose Internet Mail Extensions*

**MNO** *Mobile Network Operator*

**MY** *Unique Source Address*

**NB** *Serial Parity*

**NCI** *NFC Controller Interface*

**ND** *Node Discover*

**NDEF** *NFC Data Exchange Format*

**NFC** *Near Field Communication*

**NI** *Node Identifier*

**NIR** *Near Infrared*

**NRT** *NFC Record Type*

**NWK** *Network Layer Overview*

**OBEX** *OBject EXchange*

**OEM** *Original Equipment Manufacturer*

**OSI** *Open Systems Interconnection*

**OTP** *One-Time Password*

**P2P** *Peer to Peer*

**PAN** *Personal area network*

**PAP** *Physical Access Point*

**PC** *Personal computer*

**PCB** *Printed Circuit Board*

**PDA** *Personal digital assistant*

**PDCA** *Plan-Do-Check-Act*

**PDU** *Protocol Data Unit*

**PICC** *proximity integrated circuit card*

**PIN** *Personal Identification Number*

**PHY** *Physical Layer*

**PWM** *Pulse-Width Modulation*

**RAM** *Random Access Memory*

**RARP** *Reverse Address Resolution Protocol*

**RBAC** *Role-Based Access Control*

**RE** *Restore Defaults*

**RF** Radiofrequência

**RFID** *Radio-Frequency Identification*

**RFD** *Reduced Function Device*

**RFU** *Reserved for Future Use (Read-Only register)*

**ROM** *Read Only Memory*

**RS** *Recommended Standard*

**RST** *Reset signal (used to reset the chip communications)*

**RTD** *NFC Record Type Definition*

**RTS** *Request To Send*

**RTU** *Remote Terminal Unit*

**RX** *Receive Line*

**SAM** *Security Access Module*

**SE** *Secure Element*

**SD** *Secure Digital*

**SFD** *Start-of-frame delimiter*

**SFR** *Special Function Register*

**SIM** *Subscriber Identity Module*

**SMS** *Short Message Service*

**SNEP** *Simple NDEF Exchange Protocol*

**SO** Sistema Operativo

**SPI** *Serial Peripheral Interface*

**SQL** *Structured Query Language*

**SSP** *Security Support Provider*

**TCP** *Transmission Control Protocol*

**TIA** *Telecommunications Industry Association*

**TX** *Transmission Line*

**UART** *Universal Asynchronous Receiver/Transmitter*

**UDP** *User Datagram Protocol*

**UHF** *Ultra High Frequency*

**UICC** *Universal Integrated Circuit Card*

**URI** *Uniform Resource Identifier*

**URL** *Uniform Resource Locator*

**USB** *Universal Serial Bus*

**V** *Volt*

**VB** *Visual Basic*

**Vcc** *Power Supply*

**Vpp** *voltage peak to peak*

**WAN** *Wide Area Network*

**WAV** *WAVEform audio format*

**WDT** *Watchdog Timer*

**WIFI** *Short Message Service*

**WR** *Write*

**XML** *eXtensible Markup Language*

# Capítulo 1

# Introdução

## 1.1 Enquadramento

Nos dias de hoje a segurança é um dos aspetos fundamentais e mais relevantes na vida das pessoas e instituições, quer na proteção dos seus bens, informações, e espaços.

Para colmatar este problema, desde os primórdios se recorre à utilização de fechaduras manuais para simplesmente proibir o acesso de pessoas alheias a um dado espaço ou objeto(edifícios, cofres, veículos, etc.), salvaguardar zonas que mesmo acedidas com intenção não ilícita podem ter consequências nefastas ao nível de equipamentos e sistemas, e mais recentemente, sistemas com um nível de funcionalidades mais avançadas, apoiadas pelos mais diversos sistemas de monitorização e controlo, que se destinam, a além de não permitir o acesso de pessoas sem permissão, apresentar funções de controlo de fluxo de indivíduos (por exemplo, em espaços de eventos com limite de entrada e controlo de acesso automático); monitorizar os acessos em tempo real; criar sistemas internos que auditam o comportamento de utilizadores autenticados; entre outros.

Verificando-se, a dada altura, um avanço tecnológico de tão grande dimensão, constatou-se com base no nível de integração das tecnologias, no desenvolvimento de soluções para implementações de segurança, a necessidade, de denominar esta grande área, de sistemas de controlo de acessos. Com o aparecimento de complexos sistemas de informação, e sistemas computacionais com grandes necessidades de segurança, esta área de interesse dividiu-se em dois campos de aplicação distintos, embora com os mesmos pressupostos (sistemas de controlo de acessos físicos, e sistemas de controlo de acessos destinados a sistemas e redes de computadores). Hoje em dia, pelo nível de de convergência e centralização de sistemas e serviços, os sistemas de controlo de acessos já são integrados, com outros de outra função, embora geridos no mesmo sistema global (servindo como grande exemplo, a grade variedade de sistemas distintos que se integram na área da domótica).

## 1.2 Motivação

Segundo um estudo do INE (Instituto Nacional de Estatística) o número de habitações em Portugal aumentou para os 5,5 milhões em 2005. Supondo que desde aí não ouve um aumento ou diminuição deste valor, conclui-se mesmo assim, que o volume de mercado disponível para estes tipo de sistemas é enorme, embora na realidade a sua aplicação seja

diminuta.

Os sistemas de controlo de acessos físicos, em termos de mercado nacional, podem até estar mais ou menos disseminados, porém será razoável afirmar que a nível doméstico a sua utilização é praticamente nula (principalmente soluções tecnologicamente mais avançadas), apresentando-se estes, mais ao nível de organizações e instituições de envergadura considerável. Este fato poderá dever-se à complexidade de implementação, difícil manutenção, custo elevado, e fraca interação com o utilizador. Assim, torna-se claro que a indústria destes sistemas, convirjam os seus produtos e recursos de desenvolvimento, em soluções que visam a prestação de produtos tendencialmente complexos, apresentando baixo nível de risco, na aposta em mercados que se revelam pouco flexíveis à adoção destes sistemas, ou seja, no limite, nesta conjuntura, o mercado influi num estado de baixo fornecimento de soluções alternativas para as comuns habitações domésticas.

Por outro lado, a sociedade tem demonstrado uma evolução tremenda na flexibilidade que apresenta em moldar-se rapidamente a novas formas de tecnologia e sistemas que veem substituir mecanismos e processos à muito cimentados. Este argumento consolida-se com a crescente aposta na centralização de serviços, em dispositivos que se tornaram uma ferramenta diária indispensável no dia-dia das pessoas, nomeadamente, os dispositivos móveis.

Posto isto, as circunstâncias estão criadas, abrindo oportunidades para a implementação de novas soluções que sejam simultaneamente capazes, de aproveitar as tecnologias emergentes para a execução de novas formas de prover um acesso (ou proteger um recurso), e de forma inteligente desenvolver esses produtos/serviços, centralizando-os em dispositivos previamente adotados e com alta capacidade de integração.

## 1.3 Objetivos

1. Explorar e caracterizar todo o conceito, mais propriamente, as mais recentes tecnologias passíveis de serem implementadas de forma a permitir, após sua análise, gerar uma solução viável e robusta, ao nível do funcionamento e implementação.

2. Desenvolver um protótipo funcional de um sistema de controlo de acessos físicos, para aplicação doméstica, onde por um lado, procurará fornecer as principais funcionalidades dum sistema deste tipo, como tentará simplificar o produto, tanto ao nível da arquitetura do *hardware*, como em termos de interação com o utilizador.

3. Validar uma tecnologia emergente, ou uma que já apresente um estado de maturação elevado, de forma inovadora. Esta deverá apresentar um caráter alternativo ao nível tecnológico para aplicações de autenticação em sistemas de controlo de acessos físicos, procurando também, oferecer um contributo na evolução e aceitação da tecnologia, e de produtos funcionais semelhantes no mercado.

## 1.4 Estrutura da dissertação

A dissertação encontra-se dividida em seis capítulos (incluindo o atual capítulo - Introdução), e quatro apêndices. De seguida faz-se uma breve descrição dos capítulos constituintes, da mesma forma sequencial que são apresentados no documento.

- **Revisão do Estado da Arte**

  O capítulo 2 apresenta uma breve introdução ao tema em análise, procurando evidenciar ao leitor os principais conceitos característicos de controlo de acessos. Aborda também alguns dos principais modelos de controlo de acessos, e os distintos mecanismos aplicados (autenticação, autorização, etc.). No seu término, faz uma revisão das principais tecnologias e mecanismos de identificação/autenticação, ou que apresentem características para tal, aplicáveis em sistemas de controlo de acessos. Este capítulo tem também como objetivo, apresentar o tema de uma forma conceptual, que permita a sua interpretação numa perspetiva de sistemas físicos, ou computacionais.

- **Sistemas de Controlo de Acessos Físicos: Revisão**

  O capítulo 3 pretende revisar de uma forma mais evidenciada os sistemas de controlo de acessos físicos, não de uma forma tão conceptual, centrando a sua descrição, nos componentes tipicamente constituintes de um sistemas deste tipo, tipos de leitores aplicados, topologias/arquiteturas dos sistemas, riscos de segurança mais comuns, e finalmente, uma breve descrição dos mais comuns protocolos de comunicação implementados nas diferentes topologias abordadas, ou soluções, que o autor considere passível de implementar.

- **Sistemas de Controlo de Acessos Físicos: Especificação**

  O capítulo 4 tem como objetivo principal providenciar ao leitor, numa primeira fase, recorrendo a mecanismos de decisão e posterior breve estudo de mercado, a justificação à tecnologia de autenticação selecionada para a implementação. Exposta esta informação, no final do capítulo, é apresentada a solução proposta.

- **Implementação**

  O capítulo 5 contêm toda a descrição da implementação realizada. Como ferramenta de suporte ao entendimento do leitor, são apresentados diagramas e esquemas, como, diagramas de atividade, e diagramas de sequência (previstos no UML2.0). Com recurso a estes, e a uma apresentação comummente por tópicos, procura-se que o leitor, facilmente entenda os algoritmos de funcionamento, interações entre os diferentes subsistemas, e aspetos mais específicos da implementação.

- **Considerações Finais**

  Por fim, no capítulo 6, são apresentadas conclusões e observações relativas ao trabalho realizado na dissertação, propondo trabalhos futuros que induzam interatividade, robustez, e novas funcionalidade ao sistema.

- **Apêndices**

  No final da dissertação são apresentados quatro apêndices. Um contêm material genérico de suporte para a implementação, e também, material de consulta para o leitor. O segundo contêm os esquemas elétricos referentes à implementação. O terceiro, diagramas de casos de uso feitos no início de desenvolvimento da implementação, e o quarto, um diagrama de sequência.

# Capítulo 2

# Estado da Arte

Este capítulo pretende apresentar o estado da arte relativamente ao tema abordado, tal como todos os conceitos mínimos para a compreensão da informação exposta nos seguintes capítulos. Começa por descrever os conceitos de identificação, autenticação, autorização e auditoria. Superficialmente descreve em que se baseiam os principais modelos de controlo de acessos. Descreve de forma clara e sucinta em que se baseiam os mecanismos de autenticação e autorização, e explora o conceito de fator múltiplo e multimodalidade.

De seguida descreve as várias tecnologias e mecanismos usados em sistemas de controlo de acessos, desde os mais primordiais aos mais avançados tecnologicamente.

## 2.1 Controlo de Acessos

Controlo de acessos pode-se definir como o conjunto de funções que permitem apenas utilizadores autorizados, programas ou processos de um dado sistema a aceder a dados, espaços ou objetos físicos, com base num dado modelo de segurança. Estes podem permitir ou negar o acesso, verificando o nível de permissões dessa identidade a um dado recurso. Pode-se dizer ainda que é um conjunto de procedimentos efetuados ao nível de *hardware*, *software* e administradores de um dado sistema que monitorizam os acessos, identificam e gerem pedidos de utilizadores, registam os acessos e tentativas destes, e que levam a cabo autorizações ou negações com base em regras pré-estabelecidas. O grande objetivo é então o de limitar as ações de operações que um utilizador legítimo de um dado sistema pode executar, impedindo toda a atividade ilegítima de tentar corromper o modelo de segurança imposto.[1; 2]

Posto isto, e de acordo com [1], nesta fase é importante explicitar alguns conceitos que muito serão referenciados, definindo-se os seguintes:

- **Sujeito** - Entidade ativa que requer acesso a um objeto ou dados contidos em objetos.
- **Objeto** - Entidade passiva a que se tem acesso, ou o item sobre o qual se realiza uma ação.
- **Acesso** - Capacidade de um sujeito fazer algo, como ler, criar, eliminar ou modificar. O acesso também é considerado como o fluxo de informações entre o sujeito e o objeto.

- **Controlo de Acessos** - São os recursos de segurança que controlam a forma de como os sujeitos e os objetos comunicam e interagem uns com os outros, e a forma como o fluxo de informação se dá entre eles.

## 2.2 Etapas de Controlo de Acessos

Nesta secção exploram-se os principais conceitos relativos ao controlo de acessos em computação, podendo estes ser transpostos para o âmbito desta dissertação mais direcionada para controlo de acessos físicos. Mesmo assim estas definições não deixam de ser transversais às duas vertentes e poderão ajudar a entender a metodologia na aplicação de segurança em tudo o que é sistemas de proteção físicos ou não físicos. Desta forma tentar-se-á direcionar a explicação dos conceitos numa perspetiva de os contextualizar com o tema abordado nesta dissertação.

### 2.2.1 Identificação

Identificação é a atividade de um sujeito que se traduz no fornecimento da sua identidade junto de um sistema de controlo de acessos (físico ou não físico) para posterior serviço de autenticação. É um conjunto de procedimentos a que um utilizador se deve submeter quando solicita o acesso a um dado serviço, espaço físico, ou dados de um sistema de informação.[3; 1].

É relevante dizer que a identificação no seu sentido lato não prova a veracidade da informação fornecida por um dado sujeito. Por exemplo, imagine-se que num dado sistema de controlo de acessos que o mecanismo de identificação passa pelo fornecimento, da parte de quem tenta aceder, de um *username*, número de conta, cartão de identificação ou outro método. Nestas circunstâncias é de rápida compreensão que um sujeito mal-intencionado se possa passar por um outro, seja qual for o método ilícito para tal. Então, para a sua autenticação será necessário o fornecimento de um ou vários dados adicionais que façam o *match* com a identificação fornecida.

### 2.2.2 Autenticação

Autenticação é a segunda parte do processo de credenciação para verificar a identidade do utilizador. Estes mecanismos podem ser palavras-chave, códigos *Personal Identification Number* (PIN), *tokens*, entre outros. Basicamente é um processo pelo qual o utilizador é obrigado a provar a sua identidade, fazendo corresponder a esta uma outra forma de validação com correspondência única ao objeto identificador, provando-se assim este genuíno e credível perante o sistema de autenticação (sendo o acesso autorizado ou negado dependendo da análise do modelo de decisão, implementado no sistema de controlo de acessos). Este tipo de informação deve ser guardada em base de dados remotamente ao ponto de acesso, onde este último sempre que solicitado para permissão oe acesso, comunica com o sistema preferencialmente centralizado, e processa o requisito de validação.[3; 1].

Suponha-se um utilizador **A** a tentar aceder a um dado objeto protegido com um sistema de controlo de acessos físico. Este sistema é dotado de um mecanismo de identificação biométrico. É requisitado que ele insira o seu nome de utilizador através de um ecrã táctil com interface gráfica e posteriormente que confira a sua identidade com a provação da sua impressão digital. Poder-se-á dizer que a primeira etapa de inserção

do nome de utilizador corresponde à identificação, e a posterior, o processo que levará o sistema a um estado de autenticação.[3].

A filosofia por detrás deste conceito é bastante expressiva com a seguinte afirmação: "*You may tell me your name, but I have no proof that you are who you say you are until you demonstrate the secret handshake. Only then will I be convinced of your identity*".[1].

Como se pode verificar as duas etapas acima descritas estão intrinsecamente ligadas. Por esta mesma razão muitas vezes são confundidas ou referenciados ambos os significados como sendo apenas um dos conceitos.

#### 2.2.2.1 Mecanismos

Como revisto nos pontos anteriores os utilizadores devem prover o sistema de controlo de acessos de informação que prove a identidade fornecida. Neste ponto caracterizar-se-á os distintos mecanismos de autenticação que os utilizadores podem ser solicitados a fornecer a um sistema que detenha como recursos de autenticação apenas um, ou uma conjugação dos apresentados de seguida. Posto isto, com base na informação disponível em [3; 4]:

- **No Conhecimento**: O mecanismo de autenticação baseado no conhecimento do sujeito, baseia-se tal como o nome indica, na necessidade deste memorizar um conjunto de dados, ou apenas um, tipicamente uma *password*. É bastante utilizado devido à sua facilidade e custos reduzidos de implementação, podendo-se dizer que estas são as suas vantagens. Por outro lado o facto de ser um ou vários dados de acesso que dependem da memória do utilizador, existe sempre a possibilidade de esquecimento ou noutras circunstâncias, por exemplo, através do furto da informação confidencial recorrendo a violência física ou psicológica. Também o facto do utilizador ter poder de escolha sobre a *password*/objeto de autenticação, também vulnerabiliza o sistema, na medida em que a "força" inerente à escolha pode ser mais ou menos forte, e consequentemente a segurança intrínseca ao acesso do utilizador pode estar condicionada.

- **Na Posse**: O mecanismo de autenticação baseia-se no facto do utilizador possuir um elemento físico na sua posse que sirva como elemento de reconhecimento, por exemplo, *smart card* ou uma *tag*[1] de RFID. Normalmente este mecanismo é acompanhado com um requisito com base no conhecimento do utilizador, sendo que existindo apenas este, ainda mais vulnerável se torna este mecanismo relativamente aos que usam apenas o atrás mencionado. A mais clara desvantagem é que os sistemas que funcionem com base neste mecanismo serão à partida mais dispendiosos, mas por outro lado apresentam uma maior segurança e simplicidade na modelização apresentada sob a forma de produto, no mercado.

- **Nas Características**: Estes mecanismos processam a autenticação com base na biometria, que se baseia nas características físicas e/ou comportamentais do ser humano. A este nível o problema de esquecimento, perda de dados ou elementos físicos de validação são irrisórios. As vantagens é a singularidade associada ao utilizador e o fato das características biométricas serem intransmissíveis e praticamente

[1]Entenda-se a palavra "tag" como o conceito pelo qual, comummente, se designa uma *proximity integrated circuit card* (PICC).

implagiáveis. Por outro lado, os sistemas de controlo de acessos físicos que implementam este tipo de sistemas de autenticação têm tendência a ser dispendiosos e de requererem espaços de implantação seguros e de maiores dimensões.

- **Na Localização** : "O mecanismo de autenticação baseado na localização tem como base a localização geográfica do utilizador a ser autenticado. Devido à complexidade de implementação deste tipo de autenticação, são, ainda, poucos os sistemas que o utilizam. Por mero exemplo, cita-se a autenticação, através da comunicação GPS, da utilização de endereços *Transmission Control Protocol* (TCP)/IP, número de série de placas de rede, etc."[3]

#### 2.2.2.2 Tipos

Nesta secção serão descritos os diferentes tipos de autenticação relativamente à sua forma de funcionamento.

##### 2.2.2.2.1 Estáticos

Autenticação estática baseia-se num funcionamento por parte do sistema de validação, não variável ao longo do tempo. Um exemplo é sistemas de controlo de acessos que requerem apenas uma *password* registada previamente no sistema, sendo que esta não sofre alterações em seguintes tentativas de acesso, quando poderia aumentar a segurança dinamicamente, sob a forma de interação com o utilizador no momento de acesso, mudando os dados deste com base no conhecimento do utilizador.[5]

##### 2.2.2.2.2 Dinâmicos

Autenticação dinâmica utiliza criptografia ou outras técnicas que permitem o sistema detetar tentativas de acesso fraudulentas, mesmo em casos em que elementos físicos de autenticação são clonados. Estes autenticadores dinâmicos modificam ou encriptam o acesso a cada sessão. Este processo é gerido entre o requerente e o verificador, e pode ser implementado das mais variadíssimas formas.[5] Uma forma clara de entender este conceito é imaginar uma situação em que um dado individuo só abrirá a porta ao seu amigo se este bater à sua porta com um dado ritmo, nunca podendo ser o mesmo, pressupondo que a cada vez que a porta lhe é aberta eles combinam um novo ritmo para o próximo encontro. Posto isto, basta transpor esta conceptualização para sistemas automáticos e eletrónicos de interação com o utilizador, ou com o seu elemento identificativo de "posse".

Muitas vezes surge na literatura o conceito de **"Autenticação forte"** que geralmente é transversalizado, ou na verdade confundido com sistemas de fator múltiplo ou multimodais. De acordo com [4] frequentemente esta definição está associada à tecnologia *One-Time Password* (OTP), que é um método de autenticação que transmite ao utilizador uma nova password, por exemplo, via tecnologia *Global System for Mobile Communications* (GSM), sempre que este pretende iniciar nova sessão ou dar entrada num dado acesso controlado. Nesta perspetiva o autor desta dissertação considera que a "formulação" encaixa melhor neste tópico.

##### 2.2.2.2.3 Fator Múltiplo e Multimodalidade

Sistemas de controlo de acessos físicos biométricos muitas vezes têm de lidar com percentagens de erro inaceitáveis, servindo de exemplo o facto de cerca de 5% da população não ter impressões digitais legíveis.[6]

Nos sistemas de controlo de acessos de tecnologia única, alguns exemplos das consequências a si inerentes é que as *passwords* podem ser adivinhadas, cartões de identificações furtados e impressões vocais gravadas. Por essa razão algumas normas de segurança recomendam o uso de sistemas com implementação de sistemas de fator múltiplo.[7]

A referência a acessos multimodais ou autenticação por fator múltiplo aparece muitas vezes divididos na literatura, mas as suas definições poucas diferenças apresentam, sendo que a primeira aponta sempre no sentido da aplicação prática da sua conceptualização no uso de sistemas de reconhecimento com base em biometria, e a segunda, num sentido da utilização de sistemas de identificação-autenticação mais gerais, em que a vantagem assenta na combinação dos mecanismos apresentados em 2.2.2.1. Posto isto, a explicação é exposta como se do mesmo conceito se tratasse já que o fundamento é o mesmo. Apenas para clarificar esta ideia apresentam-se os seguintes exemplos que definem a linha de separação entre os conceitos:

- **Sistemas Multimodais:** Um esquema muito comum utiliza o reconhecimento facial, de voz e dos movimentos dos lábios do utilizador. [6]

- **Sistemas de Factor Múltiplo:**

  1. Um cartão de identificação (na posse) e um PIN (no conhecimento);[7]
  2. Uma impressão digital (nas características) e uma password(no conhecimento).[7]

Assim, multimodalidade ou autenticação por fator múltiplo é a capacidade de combinar no mesmo sistema de controlo de acessos, distintos tipos de verificação por diferentes tecnologias na mesma interacção com o utilizador ou sessão. Na verdade, estritamente, eles implicam a capacidade das tecnologias conjugadas processarem e adquirirem a informação necessária em paralelo e não de forma sequencial, sendo obviamente os primeiros mais atrativos para os utilizadores já que apresentam uma maior velocidade de resposta por parte do sistema na altura do processo de validação. Sintetizando, e exemplificando com o uso de biometria, é a recolha de uma ou mais características fisiológicas ou comportamental para identificar e validar um acesso a um individuo. Pode-se dizer que envolve a fusão de tecnologias de reconhecimento, mesmo estas podendo ser com base em mecanismos de verificação extra-fisiológicos/comportamentais como referido atrás.[6; 8; 7; 5; 4]

Fortalecendo ainda a ideia, é muito importante entender que a autenticação por fator múltiplo não significa simplesmente que está s ser usada mais do que uma técnica de autenticação. Na verdade o fator múltiplo requer o uso de diferentes categorias tecnológicas. Por exemplo, exigir que um utilizador responda a uma pergunta secreta e digite uma password, não é autenticação de fator múltiplo. Pelo contrário, é a implementação que requisita pelo menos dois mecanismos distintos dos referidos atrás, por exemplo, o uso de PIN (no conhecimento) e uma *tag* identificativa (na posse).[7]

Numa perspetiva do acesso que se quer assegurar e do nível de segurança pretendido o planeamento das tecnologias a usar devem ser tidas em conta aspetos como o custo, capacidade da implantação física assegurar uma boa manutenção aos equipamentos de autenticação, e desempenho e aceitabilidade destes. Além disso, o utilizador a ser autenticado deve passar por todos os testes, em que cada um pode ter um peso diferente no algoritmo de decisão, conforme o nível de conformidade dos *templates* obtidos por cada

um dos tipos de verificação utilizados.[8] A Figura 2.1 representa o aumento de segurança com a multiplicidade de tecnologias conjugadas.

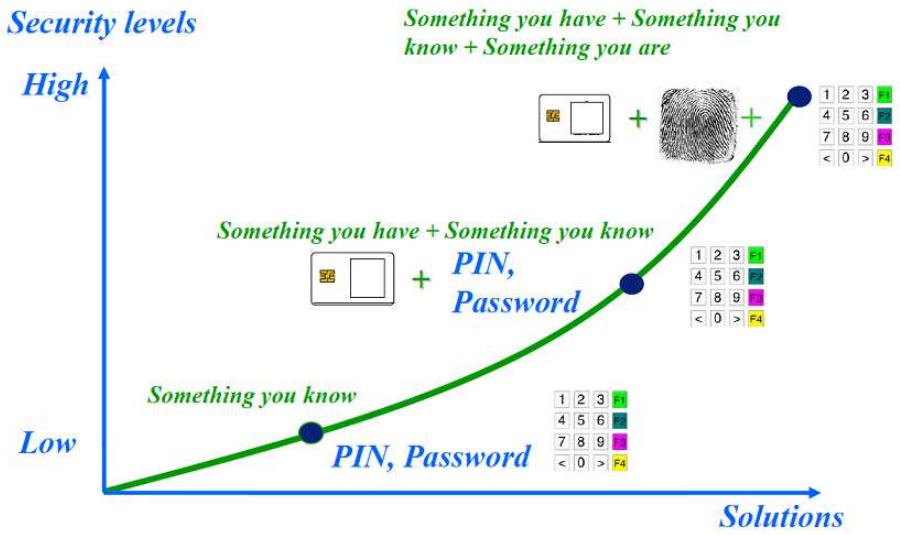



Figura 2.1: Representação da evolução do nível de segurança com o aumento do nível de conjugação de tecnologias de autenticação em sistemas de controlo de acessos[9]

### 2.2.3 Autorização

Autorização é o processo que consiste em determinar o que é que o sujeito autenticado pode realmente aceder, e que operações podem levar a cabo sobre o sistema. A processo de autorização é baseado em alguns tipos de critérios pré-definidos, que é imposta através de listas de controlo de acessos, rótulos de segurança, perfis de utilizadores, entre outros. Pode-se dizer que quando um utilizador é autorizado passa a estar licenciado para praticar uma determinada operação. Dependendo do recurso/operação a que o utilizador está a tentar aceder, o sistema deve de forma automática gerir o pedido, e garantir a autorização ou negação a este. Estas permissões são geralmente superintendidas pelo administrador do sistema que pode adicionar, remover ou alterá-las.[3; 1].

#### 2.2.3.1 Mecanismos

Por mecanismos de autorização entenda-se os tipos de processos ou funções, na forma de modelo de atuação para validar um dado utilizador. Segundo [5] apresentam-se os seguintes tipos:

- **Local**: Autorização local é realizada para cada aplicação e sistema em que um utilizador requer acesso. Os mecanismos do sistema de controlo de acessos e as aplicações locais que o constituem são designados para configurar e manter as autorizações para os indivíduos, no local.

- **Rede**: A autorização é realizada em um servidor de autorização central, proporcionando o acesso à conta de um utilizador a partir de uma ou mais estações da rede. A chave aqui, é que o acesso é apenas para uma conta de utilizador. Se o

utilizador requerer múltiplas contas, então uma destas representa uma autorização distinta, sendo gerida da mesma forma para múltiplos utilizadores.

- ***Single Sign-on***: *Single sign-on* utiliza um servidor de autorização central para permitir que um utilizador seja apenas autenticado uma vez, com vista a conseguir o acesso a múltiplos objetos num sistema que opera com diversos mecanismos de autenticação. Por exemplo, uma implementação *Kerberos*® contida em uma rede heterogénea com *Windows 2000*® e *Unix*®. Mesmo assim, não implica que para um distinto objeto conceptual alheio ao sistema geral não necessite de pós-verificação.

- ***Single Log-on***: *Single log-on* é semelhante ao anterior com a ressalva de que o mecanismo de autenticação do servidor central, é o mesmo usado por todos os objetos, sejam estes ficheiros, acessos físicos ou qualquer outro item com que o utilizador necessite de interagir. Em vez de guardar o resultado da validação para cada verificação, a única efetuada é aceite por todos os recursos como a única necessária. Este mecanismo elimina a necessidade do utilizador ter de se sujeitar ao processo de validação a cada recurso que pretenda aceder, após ter sido validado.

### 2.2.4 Auditoria

É também importante perceber que, para garantir um bom sistema de controlo de acessos, as etapas de identificação, autenticação e autorização não são suficientes. Elas devem ser complementadas com procedimentos, preferencialmente automáticos, de auditoria que consistem num conjunto de processos que *a posteriori* devem monitorizar todos os pedidos e atividades do utilizador do sistema.[2]

Como é lógico, para que isto aconteça, estes processos requerem que um utilizador esteja registado e tenha tido parte ativa no sistema, ao nível de acesso a espaços ou dados protegidos pelo sistema, ou conforme o seu nível de permissões ter efetuado operações sobre o sistema que podem ter consequências ao nível do funcionamento deste. Por exemplo, imagine-se um utilizador, funcionário de uma empresa **X**, com alto nível de permissões que tem aprovação para gerir as de outros colaboradores da corporação para além de adicionar novos utilizadores que sejam funcionários na mesma. Por razão imprópria este funcionário regista uma pessoa alheia à companhia. Auditar é registar e avaliar este tipo de situações, neste caso em específico, a situação seria detetada por auditoria com um cruzamento de dados dos funcionários e colaboradores da empresa com o nome da pessoa alheia registada, sendo assim este detetado. Este elemento do sistema acaba por ser uma potencialidade desencorajadora a tentativas ilícitas sobre o sistema, já que todos os pedidos e ações são registadas, monitorizando assim o comportamento dos utilizadores de forma permanente e automática até que uma violação do sistema seja efetuada e os administradores notificados.

Além disso, a auditoria pode ser útil para determinar possíveis falhas no sistema de segurança. Finalmente, auditar é essencial para garantir que os utilizadores não autorizados giram os seus privilégios. Por outras palavras, induzir aos utilizadores responsabilidades pelas suas ações.[2]

## 2.3 Modelos de Controlo de Acessos

Modelos de controlo de acesso são criados para garantir e forçar as regras e objetivos de uma política de segurança instaurada, e para ditar como os utilizadores podem aceder aos objetos, entendendo-se estes como acessos físicos, dados de um sistema computacional, ou outros.[1]

Noutra perspetiva, eles são definidos como um conjunto de critérios que o administrador utiliza para definir e gerir as permissões dos utilizadores. Existem muitos modelos deste tipo, mas essencialmente três se demarcam de todo o resto, sendo eles o *Discretionary Access Control* (DAC), *Mandatory Access Control model* (MACM), e o *Role-Based Access Control* (RBAC).[10]

Mais uma vez, estes modelos foram desenvolvidos para sistemas computacionais para gerir pedidos e a ações sobre objetos de sistemas de informação, estando na base da gestão de controlo de acessos de alguns dos mais conhecidos sistemas operativos, na maior parte das vezes sendo o objeto um dado ficheiro. Repare-se que da mesma forma que na secção anterior, estes modelos são aplicáveis em sistemas de controlo de acesso físicos, pensando-se no objeto como um ponto na rede de acessos destes. Seja cada porta de uma corporação, às fechaduras dos carros de um parque automóvel de uma empresa, aos cacifos de um dado polidesportivo, a verdade é que estes acessos podem ser geridos com a mesma metodologia, da mesma forma que existem diferentes ficheiros, caracterizando-se as suas permissões pela sua importância ou confidencialidade, existem portas numa corporação que dão acesso a espaço mais ou menos importantes, carros no parque automóvel da empresa de mais alta gama apenas para administradores, e cacifos de maior dimensão nos polidesportivos para sócios privilegiados.

### 2.3.1 *Discretionary Access Control* - DAC

Deve definir e controlar o acesso de utilizadores a objetos, possibilitar que um utilizador permita ou revogue o direito de acesso de outros utilizadores sobre os recursos controlados pelo primeiro, e, por fim, proteger os objetos contra acessos não autorizados.[11] Basicamente este modelo baseia-se no facto de um utilizador definir e gerir as permissões a um objeto que ele originou, sendo o acesso inteiramente definido com base na identidade do utilizador que tenta aceder, ou no papel deste dentro da empresa/instituição/corporação. [12]

Uma abordagem comumente utilizada para prover este modelo prevê a utilização de uma matriz de controlo de acessos. Essa matriz tem, em uma das suas dimensões, os sujeitos que desejam aceder a um objeto, ou seja, indivíduos ou grupos destes, e na segunda dimensão tem a lista de objetos que podem ser acedidos.[11]

Na prática essa matriz é decomposta e utilizada no sistema em uma das seguintes formas: *Access Control List's* (ACL's) ou "*capabilities-lists*". ACL's são obtidas ao se dividir a matriz em colunas, ou seja, para cada objeto a lista de controlo de acesso fornece o sujeito e o nível de permissão ao acesso. Além disso, as ACL's podem possuir uma entrada padrão ou pública, permitindo que ela contenha apenas os utilizadores que de facto possuem permissões diferenciadas, e uma única entrada para todos os outros.[11]

- Exemplo 1: "*Dan creates a share on his system containing documents and WAVEform audio format (WAV) files, he can control and dictate who can access this share*

*and the items within it. This is typically done through ACL's, where permission is granted on a "need-to-know" basis.*"[1]

- Exemplo 2: "O Alberto adquire um cofre para o gabinete de contabilidade da sua empresa que é implementado como um objeto do sistema de controlo de acessos modelizado por DAC. Apenas os integrantes deste gabinete têm permissões registadas pelo Alberto nas ACL's para aceder a este objeto."

### 2.3.2 *Mandatory Access Control* - MAC

Este modelo é distinto do anterior porque cada objeto tem um "rótulo" associado, muitas vezes designado na literatura por "*security labels*", em que estas são designadas com base na classificação da importância do objeto (e.g. informação, acesso físico), por exemplo, "*top secret*", "*secret*", e outros níveis que possam ser especificados. Por isso se diz que MACM é muito popular em ambientes altamente secretos, como por exemplo a indústria da defesa, onde a fuga de um arquivo pode comprometer a segurança nacional.[10] Ao nível dos utilizadores o processo é semelhante, designando-se a estes um nível de acesso dentro da corporação que aplica modelos deste tipo nos seus sistemas de controlo de acessos.

A validação é feita comparando o nível designado ao objeto de acesso com o nível apontado ao utilizador que o tenta aceder, sendo que, por exemplo, um sujeito com permissões de acesso a dados "*top-secret*" tem automaticamente permissão para todos os outros de confidencialidade mais baixa.

Posto isto, os MACMs não permitem que os acessos sejam geridos diretamente pelo proprietário do objeto, mas em vez disso o modelo compara diretamente o nível de autorizações dos utilizadores e a classificação do objeto no sistema. Com base nessa comparação o nível de acesso é verificado e garantido se o "*match*" for apurado.

### 2.3.3 *Role-based Access Control* - RBAC

Modelos RBAC, ou modelos não discricionários, criam as decisões de acesso baseadas nos direitos e permissões atribuídos a um papel ou grupos. Não a um único utilizador. Os administradores definem papéis ou grupos, que funcionam como um contentor de utilizadores. Os administradores conferem direitos de acesso e permissões a um dos dois tipos de contentores e não diretamente a um utilizador. Os utilizadores são associados a um papel ou grupo e herdam as permissões e direitos designados pelos administradores a estes.[1]

Este modelo de controlo de acesso funciona eficazmente em organizações reais, pois aos arquivos e recursos são atribuídas permissões de acordo com os papéis que necessitam destes. Por exemplo, um administrador do sistema pode criar uma função de acesso para gerentes, exclusivamente. Assim, um utilizador precisaria ser atribuído ao papel de um gerente para ter acesso aos recursos a estes atribuídos.[10]

Outra vantagem é que a nível empresarial, ou de instituições que tenham de gerir o mais variado tipo e número de permissões, definidos os papéis ou grupos da organização, este modelo permite flexibilizar as operações de troca, atribuição e remoção de permissões. Por exemplo, quando uma empresa contrata um novo trabalhador ou pretender mudar o posto de trabalho de um empregado, basta associar a sua identidade ao papel

que ele representa na empresa, obtendo este de imediato acesso a todos os recursos que a sua função carece para o seu bom desempenho.

## 2.4 Tecnologias/Mecanismos de Identificação/Autenticação

Este sub-capítulo pretende dar a conhecer os diversos tipos de tecnologias ou mecanismos de identificação e autenticação utilizados nos sistemas de controlo de acessos, dando mais ênfase às tecnologias RFID e NFC. Poderão também ser apresentados mecanismos puros de acesso, como a chave metálica.

Existem alguns mecanismos e tecnologias deste tipo que não serão explorados nesta dissertação devido ao baixo nível de aplicação no contexto de controlo de acessos, tais como, o recurso às *Data Matrix* - comummente designadas por "código de barras bi-dimensionais", que tal como estes últimos, são normalmente utilizados para funções de identificação de mercadoria/produtos e, por exemplo, conhecimento posicional de um dado objeto numa linha de montagem; o recurso a dispositivos *plug-and-play* como as muito em voga *Pen Drives* com conexão *Universal Serial Bus* (USB) (muito utilizado na autenticação de *softwares*), e PINs e chaves acessos (pela sua simplicidade). O *Bluetooth* não vai ser especificado, embora também represente ser uma solução inovadora. Porém, pelas suas características de configuração pré-comunicação não apresenta a flexibilidade pretendida.

### 2.4.1 Chave Metálica

A chave metálica, muito provavelmente, foi o mecanismo pioneiro em sistemas de controlo de acessos físicos, desprezando-se as comumente designadas "trancas" muito utilizadas no resguardo de animais domésticos e/ou de criação, muito antes de alguém as considerar como tal nestes termos, servindo-se destas com o único intuito de proteger a sua habitação e os seus bens.

Como qualquer outro mecanismo, e apesar de apresentar a solução mais simples do mercado continua a ser bastante utilizada, mesmo em aplicações imensamente exigentes, tais como cofres. Desta forma, verifica-se que as chaves sofreram, tal como outros mecanismos mais versáteis e avançados tecnologicamente, uma evolução tremenda, apresentando-se no mercado hoje soluções praticamente impossíveis de contrafazer, embora por vezes, acompanhadas de mecanismos complementares (não claramente percetíveis).[13]

Na Figura 2.2 apresenta-se algumas soluções para este tipo de mecanismos, e embora não seja claro entre algumas delas, destacam-se evoluções claras ao nível da complexidade das ranhuras e elementos que as compõem, entre a primeira imagem da esquerda e as seguintes, tal como entre a última e as restantes, que aparenta ter uma mecanismo adicional desencadeado pelo botão azul.

Figura 2.2: Algumas soluções já adotadas para chaves metálicas

### 2.4.2 Cartão Magnético

Os cartões magnéticos são a solução mais difundida no mercado, não requer bateria, é uma tecnologia simples, e apresenta baixo custo de fabricação. Têm capacidade para armazenar aproximadamente 100 *bytes*, e a leitura dos dados é feita através de dispositivos desenvolvidos para essa finalidade, comumente vistos nos postos de multibanco e zonas de pagamento de estabelecimentos comerciais.[14]

Apesar disso é uma tecnologia que não apresentou grande avanço tecnológico ao longo do tempo, e por isso se tem verificado a sua vulnerabilidade em termos de segurança, sendo esta a principal razão de que num mecanismo de autenticação seja praticamente sempre necessário um mecanismo paralelo de identificação/validação. A grande lacuna passa por esta tecnologia não ter capacidade de processar informação e consequentemente não conseguir implementar mecanismos de encriptação de dados, apresentando apenas a funcionalidade de armazenamento de dados.

Na Figura 2.3 apresenta-se um exemplo de um cartão magnético, como as suas dimensões *International Organization for Standardization* (ISO) em polegadas, posição comum da banda magnética(*Magnetic Stripe* na imagem), entre outras características. Mais pormenores relativos à normalização ISO em [15].

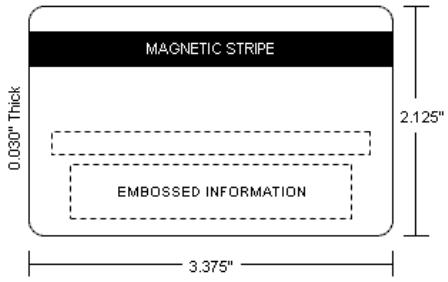



Figura 2.3: Estrutura típica de um cartão magnético [15]

### 2.4.3 *Smart Card*

Os *smart cards* não passam de um pequeno circuito integrado que normalmente está alocado num objeto de maior dimensão (e.g. maioria dos cartões bancários, cartões *Subscriber Identity Module* (SIM), etc.), que pode prover um nível de identificação/autenticação segura, por meio, da alocação de dados e processamento de algoritmos. É por esta razão que os *smart cards* não são designados como comuns cartões de memória, pois na

sua arquitetura contêm no *chip*[2] um *Central Processing Unit* (CPU) capaz de processar dados.[16]

Relativamente à solução anterior apresenta um maior nível de segurança, sendo que tem a possibilidade de implementação de funções de encriptação, utilizando processamento lógico para isso. É também bastante utilizado em funções de identificação, mas a sua aplicabilidade em sistemas de controlo de acessos físicos ainda não tem visibilidade - essencialmente os cartões de contacto, talvez por ser pouco prático no ponto de vista do utilizador.

Os *smart cards* pressupõem dois tipos de cartões - com e sem contacto. A diferença entre os dois tipos de cartões inteligentes é encontrado na forma como o microprocessador no cartão comunica com o mundo exterior. Um *smart card* de contacto possui oito pontos de ligação, que devem tocar fisicamente os contactos no leitor para transmitir informações entre eles. Um cartão inteligente sem contacto usa a mesma tecnologia baseada em rádio-frequência, tal como um cartão de proximidade[3] com exceção da gama de frequência utilizada. A frequência mais elevada (13,56 em vez de 125 kHz) do cartão inteligente permite que o cartão possa transferir mais dados por unidade de tempo, e comunicar com vários leitores em simultâneo. Ambos os tipos, aplicam-se em diversas áreas de interesse, tais como, financeira, identificação, transportes públicos, segurança computacional, saúde, entre outras.

A Figura 2.4 pretende representar a arquitetura típica do circuito interno de um *smart card* de contacto, tal como, a sua dimensão e posição típica, como no caso específico, num cartão de plástico onde estes são tipicamente aplicados(e.g. cartões bancários). Faz-se referência aos diferentes módulos do circuito por meio de acrónimos, que podem ser verificados na lista referente aos mesmos no início do documento.

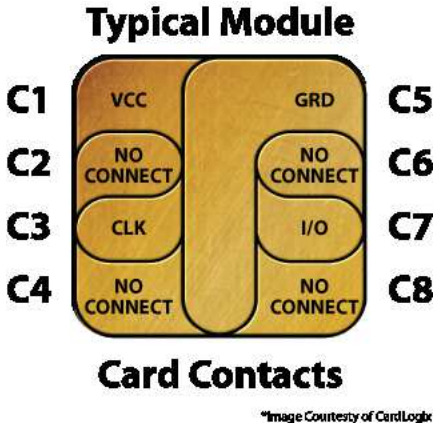



Figura 2.4: Arquitetura típica de um *smart card*(de contacto)[17]

### 2.4.4 Tecnologias/Sistemas Biométricos

Biometria é a ciência e a tecnologia de medição e análise estatística de dados biológicos ou comportamentais do ser humano. Em sistemas de controlo de acessos, a biometria

[2] Circuito eletrónico miniaturizado construído sobre uma fina superfície que contém materiais semicondutores e outro tipo de componentes

[3] Ao contrário dos *smart card's* sem contacto, o seu *chip* apenas permite fornecer ao leitor o seu número de identificação

refere-se geralmente a tecnologias automatizadas para autenticação e verificação de um individuo com base nas características do corpo humano - características biológicas, tais como impressões digitais, retinas, íris, padrões de voz, padrões faciais e medição das mãos. Nesta perspetiva biometria é um tipo de mecanismo de controlo de acesso que pode ser utilizado para verificar a identidade de um individuo com base num atributo único e pessoal.[6; 19; 1; 18]

Estes tipos de sistemas de autenticação reúnem grande quantidade de informações que podem ser difíceis de reproduzir, assim, eles fornecem um nível mais elevado de proteção quando em comparação com tecnologias de autenticação diferentes - por exemplo, cartões magnéticos.[1]

De acordo com [6], estes dispositivos devem incidir na deteção de características que sejam:

- Distintas de pessoas para pessoas;
- Não variam ao longo do tempo;
- Fáceis de recolher.

São equipamentos de resposta rápida, embora isso dependa como o sistema está programado para implementar o processo de identificação (tempo de procura na base de dados), mas tipicamente são bastante eficientes principalmente pelo facto de muitas vezes se implementar um sistema paralelo de identificação - associação a um nome de utilizador ou qualquer outra função a inserir que faça diretamente o *match* com o *template* recolhido por biometria. Uma única característica humana fisiológica ou comportamental pode ser usada como um identificador biométrico, desde que satisfaça certas especificações:

- **Universalidade**: Todas as pessoas devem ser capazes de se submeterem ao processo de verificação (excluindo indivíduos com carência de membros ou defeitos de nascimento);
- **Distinção**: Quaisquer duas pessoas devem sempre apresentar versões diferentes da mesma característica;
- **Permanência**: As características fisiológicas a avaliar devem ter um tempo de subsistência alargado, ou por outras palavras, não mudarem ao longo do tempo;
- **Adquiribilidade**: Facilidade e rapidez na obtenção das características a mensurar.

Outro aspeto importante na aplicação destes tipo de sistemas é a necessidade de ter em atenção alguns fatores que normalmente tomam menor relevância na implementação de outras soluções, tais como:

- Tempo de operação do sistema;
- Tempo de verificação do *template* obtido com a base de dados;
- O ambiente de validação;
- Tamanho da base de dados necessária;

- Precisão;
- Aceitação por parte das pessoas.

Antes de se usar um dispositivo biométrico para verificar a identidade de um indivíduo, este deve estar registado no sistema. Durante este processo, o sistema mede a característica biométrica do indivíduo, e um modelo é construído para comparação futura. Esta etapa requer alguns segundos a vários minutos, dependendo da tecnologia utilizada. Estes dispositivos de controlo de acessos extraem as medições da característica, constroem um modelo matemático a partir dessas medições e comparam-no com os já registados em base de dados.

Na maioria dos casos, a imagem total ou a impressão digital obtida após processo de autenticação não é utilizada para comparação. Apenas os dados do *template*, que consistem nos elementos necessários à identificação com determinada tecnologia deste tipo. Problemas de privacidade são minimizados, porque o parâmetro biométrico que foi medido não pode ser recriado a partir dos dados do modelo. Ao implementar um sistema biométrico, aplicam-se as seguintes considerações:

- Espaços físicos de validação requerem espaço e recursos adequados;
- Modelos criados durante a inscrição devem ser protegidos, e a segurança da comunicação entre o sistema e base de dados deve ser assegurada.

Para obter acesso a uma instalação, o indivíduo deve apresentar a fonte da característica física (e.g., mão,olho,etc.) a ser analisada. O sistema gera um resultado da análise efetuada e vai comparar com o mesmo obtido no processo de inscrição do utilizador. A validação é feita se o *threshold* entre os dois estiver entre o limite mínimo e máximo pré-definidos no sistema.

#### 2.4.4.1 Impressão Digital

O reconhecimento ou identificação por impressão digital, em biometria, é dos processos mais antigos utilizados na indústria e nas suas mais distintas implantações. Começou por ser utilizada na China antiga, junto da assinatura, em documentos que a relevância do seu conteúdo fosse manifestamente importante. A análise era efetuada, obviamente, sem recurso à tecnologia.

Por volta dos anos 70 o governo dos Estado Unidos da América (E.U.A) autorizou um estudo à *Sandia Labs* com o objetivo de determinar qual a melhor tecnologia de identificação por biometria em termos de precisão. A identificação por impressão digital obteve o melhor resultado. Muitos anos passaram desde o estudo, e talvez o panorama tenha mudado, mas o avanço desta tecnologia também sofreu os seus claros avanços, nomeadamente ao nível de algoritmos de decisão inerentes à análise dos *templates* obtidos pela tecnologia.[20; 6; 19]

Segundo [19] a identificação por impressão digital envolve a recolha do padrão caracterizado pelo relevo epidérmico formado pelas cristas papilares e pelos sulcos interpapilares. Recolhido este padrão a diferenciação ou identificação é efetuada, após a aquisição digital do conteúdo numa imagem representada por uma matriz dimensional processada por tratamento de imagem, com base na análise das chamadas *minutiae* e/ou com base

na orientação e disposição do relevo epidérmico no *template* obtido. As *minutiae* representam algumas características sempre presentes nos *templates* recolhidos, tais como, descontinuidades de cristas papilares, terminações abruptas destas, bifurcações, ilhas, cruzamentos, entre outras.

Simplificando, este modo de identificação torna-se tão eficaz porque simultaneamente analisa e caracteriza um *template* recolhido com base na orientação e disposição do contraste entre as cristas papilares e pelos sulcos interpapilares, tal como define neste, pontos de interesse bastante específicos e distintos(ao nível do posicionamento e quantidade) conhecidos como *minutiae*.[21; 19]

Analisando a Figura seguinte(2.5), fica-se com uma ideia mais clara do que em realmente consiste um *template* de uma impressão digital. Repare-se na binarização a níveis de cinzento onde se demarca claramente a separação entre as cristas e os sulcos papilares, sendo estes últimos as regiões esbranquiçadas. Além disso a Figura identifica algumas das possíveis *minutiae* que podem surgir durante a análise e codificação das características obtidas do *template* para o modelo matemático.


Figura 2.5: Representação de um *template* comum, obtido por tecnologia de reconhecimento por impressão digital, com descrição dos pontos característicos da análise[22]

Ao nível das tecnologias de aquisição, destacam-se as seguintes:

- **Tecnologia Ótica**: É o mais antigo método de aquisição de *templates* para identificação por impressão digital,surgiu no inicio dos anos 90 e é amplamente utilizada. O dedo do utilizador deve ser colocado sobre uma superfície de leitura, normalmente transparente, e a aquisição é efetuada a partir daí. O principio de funcionamento baseia-se no facto da superfície ser capacitiva. A capacitância entre o leitor e o dedo é convertida numa imagem digital de 8-bit em escala de cinzento;[19]

- **Tecnologia com base em Silicone**: Geralmente produz melhores resultados ao nível da qualidade dos *templates* obtidos do que a tecnologia acima apresentada;[19]

- **Tecnologia com base em Ultra-sons**: Utiliza ultra-sons de alta frequência para medir a impedância do dedo, ar e superfície de contacto para criar um sinal. As ondas de som penetram em diversos tipo de contaminantes que o utilizador poderá

conter no dedo identificador, tal como terra e tinta, que no caso das outras tecnologias poderia rapidamente invalidar a correta leitura e aquisição do *template* do dedo, ou negar o acesso por o resultado sair fora do *threshold* definido.[19]

#### 2.4.4.2 Reconhecimento Facial

Reconhecimento facial é uma tecnologia de controlo de acessos biométrico que utiliza uma ou mais imagens fotográficas para reconhecer uma pessoa através de pontos de medição específicos em condições controladas, por exemplo, ao nível da iluminação. Sistemas de reconhecimento facial não são invasivos, não requerem contacto físico com o utilizador e tem grande aceitação por parte dos utilizadores. Estes sistemas podem ser utilizados para ambos os requisitos de identificação ou autenticação.[6]

Existem algumas soluções ao nível das tecnologias de reconhecimento facial. Destacam-se as duas principais categorias [6]:

- **Imagens de Vídeo**: Analisa a forma original da face, padrões e posicionamento das características desta, incluindo estes resultados num modelo matemático para o efeito. Estas imagens são adquiridas e processadas em tempo real. Existem tipicamente duas formas de fazer a aquisição de imagem. A mais simples consiste na implementação de uma única câmara de vídeo que cria um modelo digital bidimensional, enquanto outras soluções implementam duas câmaras e integram os dados da dupla aquisição de forma a gerar um modelo digital tridimensional que naturalmente acrescenta resolução e fiabilidade ao sistema.
- **Imagens Térmicas**: Utiliza uma câmara de infravermelhos para produzir um *template* térmico facial. Os sistemas que implementam esta solução registam o padrão posicional dos vasos sanguíneos sob a pele que é um dado fisiológico irrepetível no ser humano.

O funcionamento dos sistemas que implementam esta tecnologia tipicamente implicam a realização de quatro passos essenciais para completar o processo de autenticação [6]:

1. **Captura de Imagens**: O sistema, com recurso a uma ou mais câmaras, adquire o número de imagens necessárias para completar o passo seguinte;
2. **Recolha de Características**: Através de software de tratamento de imagem são recolhidas as características contempladas no modelo matemático, definindo assim o *template* a comparar com os já registados no sistema, associados a todos os utilizadores;
3. **Comparação de *Templates***: Uma rotina do software consulta e compara o *template* obtido com os outros já associados a utilizadores registados, por exemplo, numa base de dados;
4. ***Matching***: O sistema verifica as características do *template* criado, dentro de um determinado *threshold*. Basta existir uma característica que ultrapasse o limite, o utilizador já não é autenticado no sistema. Caso contrário o utilizador é identificado ou autenticado, dependendo de como o sistema de controlo de acessos foi arquitetado.

#### 2.4.4.3 Reconhecimento Geométrico da Mão e Dedos

Sistemas de controlo de acessos físicos com base no reconhecimento geométrico da mão e dedos vêm a ser usados desde à cerca de 30 anos, encontrando-se no mercado normalmente sob duas formas. A primeira baseia-se na aquisição dos dados geométricos de toda a mão, enquanto a segunda baseia-se apenas na geometria do dedo central e do indicador de uma das mãos. Este reconhecimento é sempre efetuado com base na recolha de características dimensionais de uma imagem 3-D. Um leitor ou uma câmara para esta aplicação normalmente é capaz de recolher até 96 características associadas à mão ou dedos, tais como, a forma, largura, comprimento dos dedos e das partes articuladas destes, largura, entre outras. Este tipo de reconhecimento à semelhança de outras tecnologias biométricas examina a geometria espacial da mão e dedos. Têm também a vantagem de estarem preparados para desprezar todas as características contaminantes ou naturais inerentes ao indivíduo, tal como cicatrizes, impressões digitais, sujidade, entre outras. Por esta mesma razão os leitores ou *scanners* associados a este tipo de reconhecimento são frequentemente usados em ambientes *outdoor*, já que resistem a múltiplos fatores ambientais, como poeira, variações térmicas e de iluminação.[6]

Apesar das referidas vantagens, ao nível desta tecnologia de reconhecimento poder-se-á dizer que o sistema é menos fidedigno do que os anteriores, pois as características da mão humana não são unipessoais tal como no caso da impressão digital, padrão vascular da face, íris, e outras. Também, com recurso a um molde, facilmente é obtida uma mão ou unicamente dedos, com características dimensionais e de superfície que facilmente ludibriam o sistema.[23; 3] Por esta razão esta tecnologia é normalmente aplicada em sistemas ou áreas que não sejam consideradas "críticas".[24; 3]

#### 2.4.4.4 Padrão Vascular da Mão

Tal como algumas das outras tecnologias biométricas o reconhecimento do padrão de vasos sanguíneos da mão é único, mesmo em gémeos idênticos. Todos os padrões vasculares, tal como neste caso, apresentam sempre uma enorme quantidade de recursos surgindo daí a fiabilidade deste. Este modelo biométrico tem como base o padrão vascular do dorso de uma das mãos. Uma característica relevante deste processo é assente no facto de que os padrões vasculares, e mais especificamente o do dorso das mãos, são desenvolvidos e definidos antes do nascimento, e por isso, das poucas características que podem e de facto sofrem alteração ao longo do tempo são unicamente as dimensionais, e não as relações entre elas.[25; 26]

Como exemplo, imagine-se um esqueleto impresso numa folha, e um segundo igual com uma escala aplicada de *1:1.5*. Garantidamente os comprimentos para o mesmo osso têm dimensões diferentes devido ao fator de escala aplicado, mas a relação dimensional entre o comprimento, por exemplo, do fémur e da tíbia serão equivalentes. É com base nesta metodologia de análise dos *templates* obtidos, que as características são recolhidas para aplicação no modelo matemático em que a caracterização é efetuada com base num dado padrão recolhido.

As tecnologias que implementam esta análise são das mais recentes no campo da biometria, e o seu princípio baseia-se na exposição, do membro ao qual o sistema reconhece o padrão vascular, a radiação infravermelha. Dá-se a desoxidação da hematina contida nos vasos sanguíneos, durante a exposição da radiação, que no processo absorve alguma desta reduzindo o efeito da refletividade nessas zonas. Os sistemas, com base

no nível de reflexão da radiação aplicada, geram um *template* para registo, análise e/ou validação.[25]

Como vantagens associadas a este modelo podem-se apontar as seguintes [25]:

- Os sistemas só são capazes de recolher *templates* de membros vascularizados pertencentes a seres humanos com vida;
- Os elementos físicos no qual o sistema age para recolha das características, não são passíveis de sofrer danos e têm uma capacidade de permanência praticamente efetiva, ou seja, tratam-se de tecnologias de análise a características internas do ser humano;
- Os sistemas são altamente seguros pela dificuldade de reproduzir por contrafação, elementos físicos internos do ser humano;
- A universalidade inerente à análise, já que se trata de uma característica física presente em todo e qualquer ser humano.

Muito embora, como referido, estes sistemas são relativamente recentes e ainda lidam com alguns problemas ao nível da segmentação e outras formas de tratamento de imagem, principalmente associados a fatores circundantes a algumas zonas de implantação, onde facilmente é adicionado ruído difícil de desprezar computacionalmente, durante o processo de definição dos padrões.

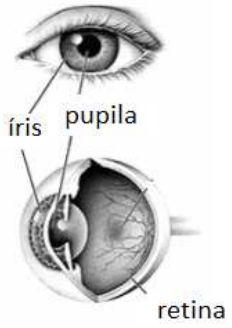
#### 2.4.4.5 Reconhecimento da Íris

Este modelo de reconhecimento é relativamente recente, surgindo a primeira patente no ano de 1994. O reconhecimento da íris é um processo de reconhecimento de um indivíduo através da análise do padrão deste elemento do olho humano.

A íris é basicamente um músculo ocular que regula o tamanho da pupila, controlando assim a quantidade de luz que entra no olho. A íris tem uma dada coloração que depende da quantidade de pigmentos da melatonina dentro do músculo. Esta coloração, tal como a própria estrutura da íris, tem fatores genéticos associados, embora os padrões não o sejam.

Á semelhança do padrão vascular das mãos, a íris desenvolve-se durante o período pré-natal através de um rigoroso processo biológico de formação de tecidos. Ainda nesta fase inicia-se o processo de degeneração que resulta na abertura da pupila e formação de características únicas ao ser humano. Por esta razão, e apesar de estarem fatores genéticos associados às propriedades da íris, as características são únicas e estruturalmente distintas para cada pessoa, permitindo assim ser um ótimo recurso físico para fins de reconhecimento.[28] Pela Figura 2.6 pretende-se clarificar através da sub-Figura 2.6(a) que com recurso a uma análise rápida, claramente se denotam distinções fisiológicas facilmente distinguíveis por um sistema complexo de reconhecimento, e na 2.6(b) uma demonstração dos elementos físicos principais associados ao olho e a este modelo.

(a) Exemplos de íris de estrutura distinta




(b) Representação dos elementos do olho humano relacionados com o reconhecimento da íris

Figura 2.6: Imagens relacionadas com reconhecimento da íris [28]

As tecnologias de reconhecimento por análise de íris normalmente aplicam a seguinte metodologia [29]:

1. **Aquisição de Imagem**: As imagens da íris são normalmente adquiridas usando uma câmara de infravermelhos (*Near Infrared* (NIR)), porque a refletividade da íris humana é alta na banda NIR. No entanto, se a cor da íris não for demasiado escura, a sua textura pode ser revelada quando se utiliza um sistema de imagens de luz visível;

2. **Segmentação da Região da Íris**: Através de software de tratamento de imagem é efetuada a segmentação/separação da região da íris de todos os outros elementos na imagem adquirida no passo anterior;

3. **Normalização do Padrão da Íris**: Nesta fase é normalmente aplicado um método de normalização proposto por Daugman [30] que tem como objetivo aliviar os efeitos(negativos) da variação de tamanho da pupila no momento de aquisição. Previamente, esta etapa também pressupõem uma melhor delimitação da região da íris com a finalidade de garantir uma boa aplicação do método de Daugman e de outros procedimentos mais específicos, posteriores, necessários nesta etapa;

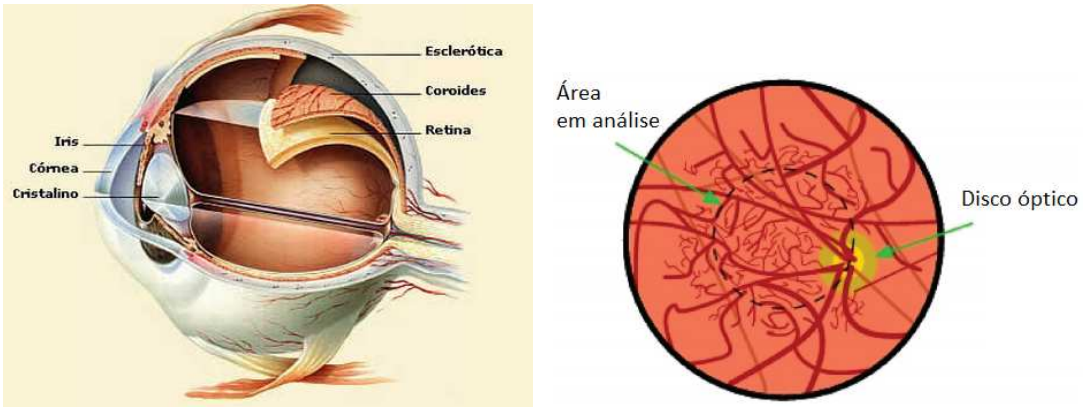
4. **Recolha de Características**: Momento de aplicação de algumas ferramentas de tratamento de imagem, que permitem obter dados relacionados com as características do modelo de decisão, tais como filtros de eliminação de ruído, binarizações, entre outros mecanismos;

5. **Classificação**: Aplicação dos valores representativos das características recolhidas no modelo matemático de decisão. Esta análise é efetuada com recurso à abordagem de "*nearest neighbor approach*", ou seja, a procura é efetuada computacionalmente com uma ordem que é definida com base na proximidade dos dados caracterizantes do *template* obtido com os presentes no sistema com características próximas.

#### 2.4.4.6 Reconhecimento da Retina

A retina, outro elemento do olho humano, é constituído por várias camadas de tecido sensorial e milhões de fotorreceptores cuja funcionalidade consiste em transformar a radiação visível em impulsos elétricos. Estes estímulos são enviados para o cérebro através de uma rede nervosa e lá convertidos em imagens. Tal como outros elementos do corpo humano foi sustentado em uma publicação, por volta dos anos 50, pelo Dr. Paul Tower, que a retina tal como outros elementos e padrões do corpo humano são únicos e distintos entre estes, mesmo no caso de gémeos semelhantes. Este estudo vem corroborar um outro publicado em 1935, pelo Dr. Carleton Simon e o Dr. Isodore Goldstein. Na Figura 2.7(a), uma representação do olho humano em corte onde facilmente se identifica a retina, sua localização e forma aproximada.[31]

O principio de funcionamento segue a mesma linha da maioria das outras tecnologias de reconhecimento por biometria. Os *scanners* têm como objetivo recolher o *template* vascular da retina e para isso fazem uso de radiação infravermelha. A caracterização dos padrões estão relacionados com a refletividade da radiação emitida sobre a retina, e o processamento destes sinais pelos sistemas deste tipo. A Figura 2.7(b) à primeira vista não contém nenhum elemento esclarecedor relativamente à forma de funcionamento das tecnologias de reconhecimento da retina, mas repare-se por exemplo, na zona a tracejado que representa na sua zona interna a área em análise pelos sistemas de aquisição e processamento do padrão da retina. Daqui conclui-se que os *templates* são obtidos numa perspetiva frontal à face do utilizador, e que apenas uma dada região da retina é estudada. Verifica-se ainda, no interior da zona referida, linhas com orientação e forma aleatoriamente distribuídas e carregadas. Estas são as linhas que constituem o padrão vascular da retina e que vão ser caracterizadas com base num modelo de análise e definição de características, que vão permitir o sistema validar um utilizador. O lado externo do círculo a tracejado representa na sua maioria a área afeta à íris, estudada no ponto anterior, daí a imagem definir uma região de interesse a tracejado que coincide com a zona "interior" da íris onde é regulada e posicionada a pupila, que facilita em princípio o processo de recolha e a definição dos padrões.




(a) Vista lateral e em corte do olho humano

(b) Vista frontal do padrão sanguíneo dentro da retina [31]

Figura 2.7: Imagens relacionadas com reconhecimento da retina

Como principais vantagens associadas ao reconhecimento por análise de padrões da retina, destacam-se os seguintes [31]:

- Os padrões sanguíneos da retina raramente se modificam ao longo da vida de uma pessoa, a menos que estas sejam afetadas por doenças como cataratas, glaucomas, ou outras;
- Os *templates* recolhidos são normalmente muito pequenos o que se traduz num tempo bastante curto de processamento e análise destes;
- Os *templates* contêm até cerca de 400 pontos de dados que podem caracterizar um individuo. Esta quantidade está associada à estrutura e forma única do padrão sanguíneo da retina;
- A retina não está exposta ao ambiente externo, e por isso está mais protegida a ameaças que possam meter em causa a sua integridade estrutural e/ou modificar os *templates* recolhidos.

Como desvantagens [31]:

- Tem pouca aceitação pelas pessoas;
- Necessita que pessoas com óculos os retirem antes de qualquer verificação;
- Sistemas dispendiosos.

#### 2.4.4.7 Reconhecimento da Voz

Reconhecimento por voz refere-se à identificação de pessoas através da análise de padrões vocais previamente associados no sistema, a um individuo. Este tipo de reconhecimento é também bastante fiável pois atualmente existe tecnologia e processos capazes de caracterizar a voz de uma pessoa com bastante detalhe e definição recorrendo à análise de diferentes particularidades associadas à voz humana, tal como, a pronúncia, timbre, escolha de vocabulário(parâmetro não diretamente relacionado ás características da voz), entre outras. [32]

O processo de identificação ou autenticação consiste, numa primeira fase, obter o *template* vocal do utilizador, gravando-o, e numa segunda fase comparar, através de algoritmos para o efeito, o modelo recolhido com os já registados/associados a utilizadores. Este processo de comparação gera um *output* que quantifica o nível de proximidade dos parâmetros em análise, ou seja, quanto maior a afinidade entre os *template* recolhido e os outros a comparar, mais provável é que o utilizador a validar corresponda ao que obtiver melhor valor do parâmetro qualitativo - *matching factor*.

Como principais vantagens associadas ao reconhecimento por análise dos padrões de voz, destacam-se os seguintes [33]:

- Baixo custo de implementação pois o processo depende quase unicamente da qualidade do software(poucos recursos ao nível de hardware);

- Tem grande aceitabilidade dos utilizadores pois estes sistemas não necessitam de grande predisposição dos utilizadores, por exemplo, para expor membros dentro de máquinas de reconhecimento biométrico, ou aproximar um olho de um dispositivo que emite radiação;
- Talvez a única forma de reconhecimento biométrico que pode ser feita remotamente;
- Os *templates* são rapidamente recolhidos (entre 2-8 segundos);
- Os *templates* recolhidos ocupam muito pouco espaço de memória, normalmente menos de 1*Kilobyte* (kB), comparativamente com outras tecnologias de reconhecimento.

Como desvantagens [33]:

- Não é das mais seguras formas de reconhecimento, pelo que deve ser inserida em sistemas multimodais;
- As características da voz humana alteram-se ao longo do tempo, já que os órgãos que são parte ativa na voz, tal como, a laringe, nariz, dentes, entre outros, vão modificando, principalmente sob processo de deterioração. Posto isto, a necessidade de se recolher *templates* identificativos ao longo do tempo, torna-se uma necessidade destes sistemas.

#### 2.4.4.8 Dinâmica da Assinatura

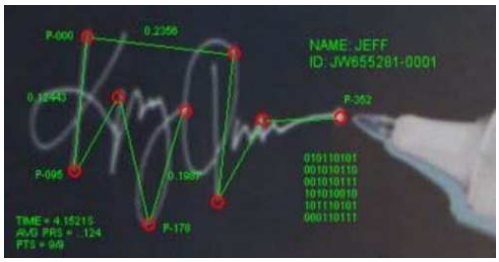
Reconhecimento com base na dinâmica de assinatura é um campo da biometria que utiliza as características anatómicas e comportamentais de uma pessoa ao assinar o seu nome ou a escrever qualquer outro texto. Dispositivos de reconhecimento pela dinâmica de assinatura não devem ser confundidos com sistemas eletrónicos de captura de assinatura que são usados para recolher uma imagem digital da assinatura e não as características dinâmicas obtidas durante o ato de assinar.

Dados, tais como a direção, forma das linhas/segmentos de ligação, forma das letras, a pressão exercida, ângulo de escrita, entre outros, de um indivíduo são propriedades que bem caracterizadas pelo modelo de verificação e definição dos *templates*, garante uma fiabilidade considerável a este tipo de sistemas de identificação ou autenticação.[28]

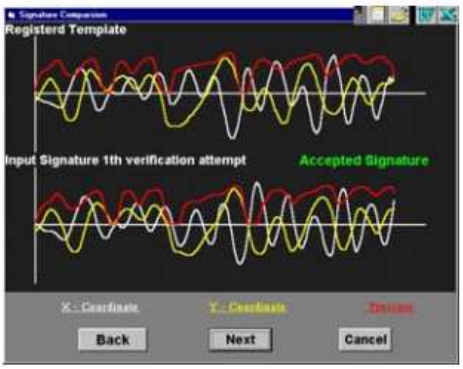
Os produtos disponíveis no mercado podem apresentar soluções bastante distintas quanto aos modelos de análise que implementam. Alguns baseiam a sua decisão recorrendo principalmente a características estáticas, como particularidades geométricas da escrita, enquanto outros recorrem a hardware mais avançado tecnologicamente para implementar funcionalidades ao sistemas, tais como, a perceção destes à pressão, velocidade, aceleração e ângulo de escrita, recorrendo a dispositivos como *Personal digital assistant*s (PDAs) e *tablets*. Uns recorrem à análise do máximo de características(sejam estas só estáticas, só dinâmicas, ou um misto), enquanto outros recorrem a modelos mais simplistas não necessariamente falíveis ou menos capazes. Basicamente, a qualidade do modelo de decisão e dos algoritmos aplicados para recolha das características dos *templates* são determinantes na qualidade do sistema.

Na Figura 2.8(a), uma representação geral de como funciona o processo de recolha de características durante o ato de assinatura num dispositivo sensível à pressão(e.g.

*tablet*), onde em tempo real são processadas tanto características estáticas, representadas pelos segmentos verdes unidos por círculos vermelhos, que devem ser processadas por cálculo adimensional, ou seja, relações entre comprimentos e não diretamente o seu valor escalar, e características dinâmicas. Na Figura 2.8(b), uma representação gráfica de características dinâmicas recolhidas no ato de assinatura. Algumas destas propriedades dinâmicas, tais como, velocidade, pressão, aceleração, *timings*,entre outras, podem ser analisadas segundo as orientações cartesianas. A posição X e Y são normalmente usadas para representar a variação de velocidade nas direções respectivas (representado pela linha branca e amarela), enquanto a direção Z(linha vermelha) é utilizada para indicar as variações de pressão ao longo do ato de assinatura ou escrita.




(a) Representação da dinâmica da assinatura: Enquanto um índividuo assina sobre a superfície de um tablet, várias características são registadas e processadas para comparação com *templates* já recolhidos no ato de registo do utilizador




(b) Rpresentação gráfica de características da dinâmica de assinatura

Figura 2.8: Imagens relacionadas com reconhecimento com base na dinâmica de assinatura [28]

#### 2.4.4.9 Dinâmica de Escrita em Teclado

A dinâmica de escrita em teclado baseia o seu critério nos tempos de pressão de um tecla(*key down event timing*), e o tempo até a "soltar" (*key up event timing*). Por exemplo, se a password de um utilizador for "password", então os tempos referidos são registados para cada letra.[34]

Registados os *timings* destes eventos define-se os seguintes padrões [34]:

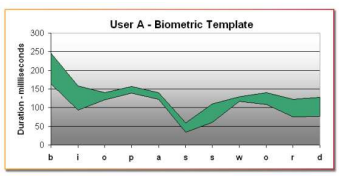
- **Tempo de Permanência/*Dwell Time***: Tempo entre o tempo de pressão e o de levantamento, basicamente, o tempo de pressão numa dada tecla. Verificar a Figura 2.9 para melhor entendimento;

- **Tempo de voo/*Flight Time***: É o tempo entre o *release* de uma tecla até ao pressionar/*key down* da seguinte.Verificar a Figura 2.9 para melhor entendimento.

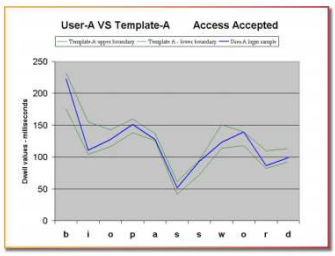

Figura 2.9: Tempo de permanência e tempo de voo[34]

Processos de identificação ou autenticação que recorrem a esta tecnologia seguem o mesmo princípio de funcionamento dos outros géneros de tecnologias de reconhecimento por biometria. Inicialmente é recolhido o *template*, de seguida a recolha das características através de algoritmos neuronais que determinam um padrão comparável, e finalmente, a comparação e validação do utilizador.

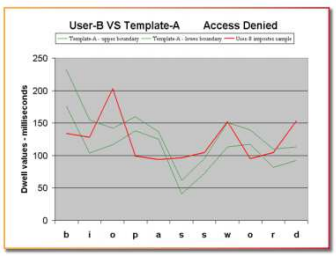
Na Figura 2.10(a), uma representação gráfica exemplo de um *template* em que a palavra inserida foi "biopassword". A região a verde é definida com base em várias recolhas efetuadas no ato de registo, para contemplar um comportamento padrão na topologia de uma palavra específica, neste caso, a referida atrás. Na Figura seguinte, 2.10(b), está delimitada uma linha azul contida dentro da zona admissível do *template* associado ao utilizador A, ou seja, a linha referida define e caracteriza o comportamento típico do utilizar A ao digitalizar a palavra "biopassword", por isso o acesso seria-lhe permitido. Por último, na Figura 2.10(c), está representado por via da linha a vermelho o comportamento do utilizador B ao digitar a palavra de acesso. Como facilmente se pode verificar a linha representa um padrão completamente distinto ao do que o utilizador A apresentou na fase de registo, saindo esta fora do *threshold* em grande parte do caracteres. O acesso seria-lhe negado.




(a) Exemplo de *Template* de dinâmica de escrita em teclado




(b) Template de escrita do utilizador A - Acesso garantido




(c) Template de escrita do utilizador B - Acesso não garantido

Figura 2.10: Imagens relacionadas com reconhecimento com base na dinâmica de escrita em teclado [34]

### 2.4.5 RFID

*Nota: O conteúdo desta sub-secção tem como fonte quase integral a referência em [35]. Todo o conteúdo que não lhe diz respeito, é normalmente referenciado.*

RFID é uma tecnologia de reconhecimento automático e recolha de dados. Esta recorre a ondas rádio para estabelecer a comunicação entre as "etiquetas" RFID e as estações de leitura. Estas etiquetas ou simplesmente *tags*, são conhecidas como "rótulos eletrónicos", operam como base de dados portáteis, e o meio de comunicação entre os leitores e as "tags" é sem fios. Estas últimas contêm memória, que pode ser lida e escrita remotamente a grandes velocidades.

Relativamente aos seus campos de aplicação, podem-se apontar uma vastidão, tais como, controlo de acessos, bilheteiras, dispositivos de imobilização de carros, rastreamento industrial, gestão de stocks, entre outros.

A grande revolução ao nível dos processos associada a esta tecnologia deveu-se essencialmente, por exemplo, face à utilização em massa dos códigos de barra, ao facto desta ser completamente viável, fácil de implementar, e apresentar um nível de fiabilidade bastante satisfatório, quer ao nível da durabilidade e resistência dos elementos móveis do sistema( *tags* RFID), quer ao nível das novas possibilidades, como a de escrita na memória das etiquetas, leitura simultânea de várias *tags* a grande velocidade e de forma autónoma(sem necessidade de cooperação humana com o sistema), entre outras.

Neste texto não vão ser especificadas nenhumas normas associadas à tecnologia RFID, sendo que a dimensão e o teor das mesmas não apresentam valor acrescentado no presente estudo, porém citam-se as seguintes referências para consulta:[36; 37; 38].

#### 2.4.5.1 Funcionamento

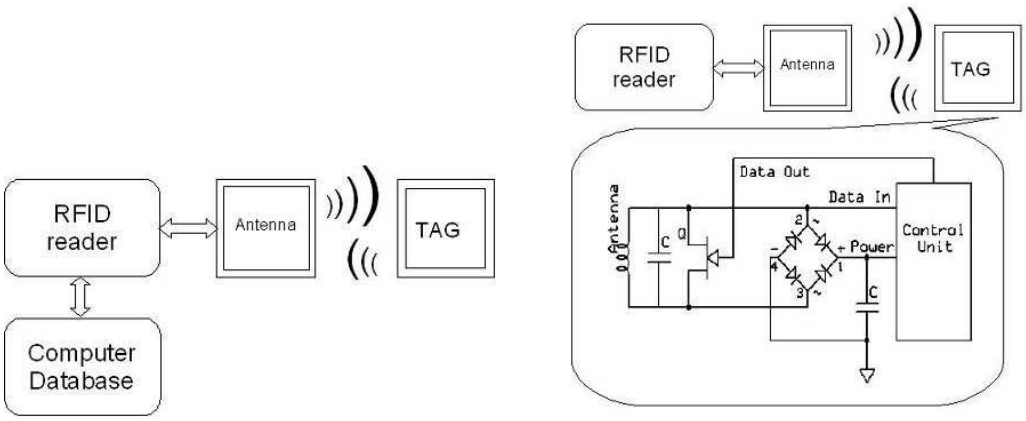
Os sistemas que implementam esta tecnologia são necessariamente compostos por três elementos chave, sendo estes, o denominado "leitor" que na maioria dos casos também consegue realizar operações de escrita na memória da etiqueta, a *tag*, e um computador remoto. A Figura 2.11(a) pretende clarificar através de um simples diagrama a disposição e interação entre os elementos ativos principais.

- ***Tag* RFID**: Consiste num circuito integrado ligado a uma antena. Este circuito é o coração da etiqueta. É ele que define a funcionalidade e a capacidade de memória da *tag*. A antena é uma estrutura condutiva desenhada para emitir e receber energia eletromagnética. A sua forma e tamanho ditam a frequência de operação, e o alcance máximo de interação entre a *tag* e o *leitor*. Na Figura 2.11(b) encontra-se o circuito típico, simplificado, de uma etiqueta RFID.

- **Leitor/Estação de Leitura RFID**: Apresentam uma arquitetura um pouco mais complexa do que as *tags* pois são tipicamente dotados, igualmente de uma antena, um microcontrolador(gere e processa as leituras efetuadas, serve de ponte de comunicação entre o computador remoto e o *chip* que processa as suas ordens de leitura ou escrita, e simultaneamente é o *master* da comunicação com o *chip* RFID que implementa as tais ordens do sistema remoto);

- **Computador Remoto**: Tem como função coordenar, monitorizar, registar e atuar, sobre o sistema global, sendo a arquitetura destes "gestores" bastante particular dependendo do caso de aplicação dos recursos RFID. Estes "gestores" remotos

não são necessariamente automáticos, sendo que, normalmente, são dotados de uma interface gráfica para interacção com operadores, existindo assim a possibilidade de operar sobre o sistema de forma manual, e não apenas de forma automática. De facto é uma tecnologia que permite criar sistemas, na sua globalidade, altamente flexíveis e versáteis no que toca à área de aplicação.




(a) Representação da interacção entre os elementos básicos de um sistema RFID

(b) Representação do circuito típico de uma *tag* RFID

Figura 2.11: Imagens relacionadas com o funcionamento de sistemas RFID [39]

#### 2.4.5.2 Frequências

A tecnologia RFID pode ser implementada usando diferentes frequências, para através de um meio sem fios(*wireless*), estabelecer a transferência de dados e comandos, entre o leitor e a etiqueta. Estas bandas de frequência foram definidas para colmatar as limitações de uma dada banda numa séries de aplicações. Assim, foram especificadas quatro gamas de funcionamento:

- **Baixa Frequência/*Low Frequency* (LF) 125-134 kHz**: Não é sensível à presença da água nem às interferências metálicas. Alcance máximo comum de 1,5m metros com baixa taxa de transmissão de dados. Tipicamente utilizada nos campos da identificação animal, sistemas de imobilização de veículos, e controlo de acessos;
- **Alta Frequência/*High Frequency* (HF) 13,56 MHz**: O alcance máximo de funcionamento é menor relativamente ao caso anterior, permite maiores taxas de transferência e tem um comportamento altamente previsível na presença de metais e orientações aleatórias das *tags* no momento de leitura. Tipicamente utilizada em sistemas de identificação automática de livros em bibliotecas, lavandarias e linhas automáticas de seleção e fornecimento de materiais;
- **Muito Alta Frequência/*Ultra High Frequency* (UHF) 860-960 MHz**: Permite alcances superiores às outras alternativas mas é altamente prejudicada pela humidade, barreiras físicas(mesmo o corpo humano) e presença de metais. As aplicações RFID neste gama de frequências não apresentam uma diversidade e quantidade de implementações como nos casos da baixa e alta frequência, destacando-se

algumas aplicações específicas, como o rastreamento para fins logísticos na indústria automóvel e outras;

- **Microondas 2,45 GHz**: É mais usada do que a anterior, mas é totalmente inadequada na presença de líquidos(absorve praticamente toda a radiação nesta gama). Apesar de tudo a sua aplicação não é amplamente utilizada, e requer implementações algo complexas. O controlo de acessos em veículos é um dos principais campos de aplicação desta banda de frequência.

#### 2.4.5.3 Tipo de *Tags*

Embora a arquitetura base da etiquetas/*tags* RFID já tenham sido atrás descritas, elas tomam diferentes formas de funcionamento, associadas a diferenças na sua arquitetura do circuito interno. Naturalmente, estas alternativas e diferenças funcionais, foram implementadas para colmatar necessidades ao nível de certas aplicações. Posto isto, postulou-se três tipo de *tags*:

- **Passivas**: São as mais comuns ao nível da aplicabilidade. Não têm bateria ou qualquer outra forma autónoma de alimentar o seu circuito. A alimentação é feita com base na energia recolhida do campo eletromagnético gerado pelo leitor no momento de interacção. São mais baratas, oferecem um tempo de vida de operação quase ilimitado, e a distância de comunicação é relativamente inferior às *tags* ativas;

  Na Figura 2.12 apresenta-se um exemplo de um *tag* passiva. Na parte frontal da etiqueta pode-se verificar uma série de elementos descritivos relativamente ao objeto identificado, tal como a empresa a que pertence, e um elemento identificativo complementar(código de barras). O circuito RFID encontra-se na zona de colagem, também com intuito de protecção do circuito, onde se verifica de forma clara, com geometria rectangular, a antena, e o circuito interno numa zona mais escura junto a esta.

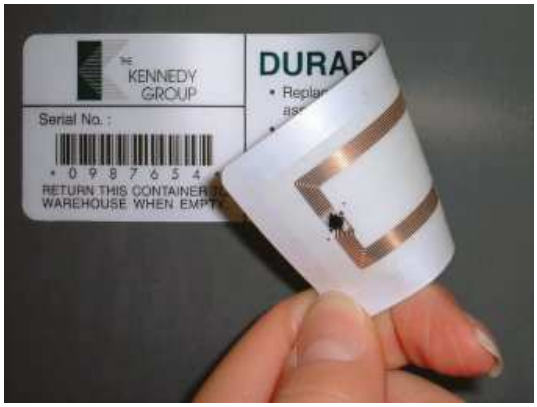



Figura 2.12: Exemplo de uma *tag* passiva [40]

- **Ativas**: No caso anterior os dados são transmitidos para o leitor, descrevendo-se de uma forma simplista, refletindo o sinal de volta para este(recorre à energia do estímulo do sinal recebido do leitor). Por outro lado, as *tags* ativas são normalmente auto-suficientes energeticamente, querendo isto dizer que são capacitadas de bateria

interna. A vantagem é que o seu conteúdo pode ser lido a distâncias que podem atingir os 100 metros, mas por outro lado, o seu custo é exponencialmente maior relativamente às anteriores. A necessidade de substituição de bateria também revela ser uma desvantagem. Como exemplo, as etiquetas ativas são bastante utilizadas nas forças armadas norte americanas no rastreamento de conteúdos de contentores em portos marítimos.

Na Figura 2.13 apresenta-se um exemplo de um *tag* ativa. Como se verifica pela imagem a sua constituição é bastante mais robusta, e a arquitetura também consideravelmente diferente. Na verdade, o princípio é o mesmo, mas o facto destas *tags* terem alimentação própria, pressupõe automaticamente um circuito auxiliar, tal como a necessidade de um sistema microcontrolado mais complexo, com recurso a um oscilador externo, pela necessidade do envio cíclico de sinais para o leitor remoto. Para a *tag* ser capaz de enviar sinais a mais longa distância, também a antena precisa de sofrer ligeiras modificações para o executar. Verificando a Figura observa-se que esta agora não está impressa/contida na *Printed Circuit Board* (PCB)/rótulo, mas sim ligada externamente, com uma dimensão muito maior. De referir que o exemplo da Figura abaixo, não passa meramente disso, existindo *tags* deste tipo como uma aparência bastante similares às passivas, dependendo esta característica, do fim para os quais elas são utilizadas.

Figura 2.13: Exemplo de uma *tag* ativa [39]

- **Sensor e Semi-Passivas**: Estes dois conceitos aparecem referenciados singularmente na literatura por distintos autores, mas as suas definições parecem assemelhar-se consideravelmente. Tipicamente, no primeiro caso, refere-se simplesmente que estas incorporam sensores nos seus circuitos. São utilizadas no mercado automóvel na medição de pressão dos pneus, no mercado alimentar para leitura de temperaturas em câmaras frigoríficas, entre outras aplicações.

  Já a definição associada às tags semi-passivas cinge-se mais ao fato destas apresentarem uma forma de funcionamento praticamente igual às passivas, embora também sejam dotadas de bateria interna, apesar de neste caso, essa energia não ser aplicada para funções de constante envio de sinais, característica das *tags* ativas. A bateria serve para alimentar elementos do circuito com funções de monitorização(e.g.

humidade, pressão, temperatura, etc.) e para aumentar o ganho da antena para transferência de dados por Radiofrequência (RF), se necessário. Resumindo, a diferença assenta no fato da energia disponibilizada na bateria não ser estritamente utilizada para funções de transmissão de dados e amplificação de sinal, mas sim, para funções de alimentação de sistemas auxiliares.

Na Figura 2.14 apresenta-se um exemplo de um *tag* semi-passiva. A linha descritiva assenta basicamente no que foi dito relativamente às *tags* ativas, analogamente à complexidade do circuito e robustez deste.

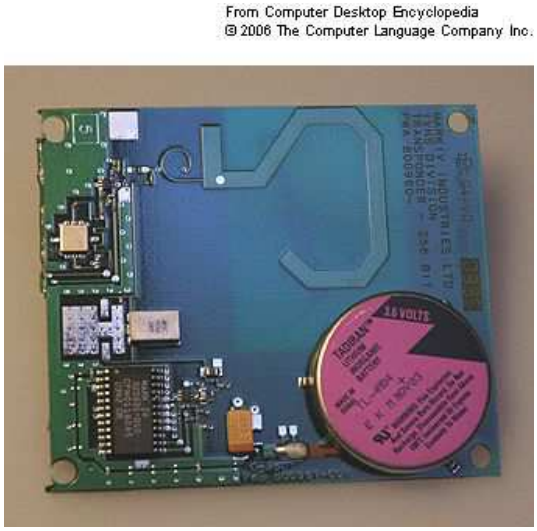



Figura 2.14: Exemplo de uma *tag* semi-passiva [39]

#### 2.4.5.4 Tipos de Memória

Existem dois tipos de memória nas etiquetas RFID: Apenas Leitura/*Read Only* e Leitura/Escrita(*Read/Write*). O primeiro tipo refere-se às *tags* em que apenas são escritos dados, ou programadas, no processo de fabricação, sendo que, posteriormente só pode ser lido o seu conteúdo.

O segundo tipo refere-se às etiquetas em que os seus blocos de memória não vêm protegidos de fábrica, e podem ser constantemente efetuadas operações de leitura ou escrita. Dentro deste tipo ainda se pode destacar uma sub-categoria denominada *Write Once/Read Many (WORM)*, que consiste num estado de funcionamento forçado pelo utilizador, e não pelo fabricante, onde o primeiro recorrendo a comandos específicos para o efeito consegue bloquear operações de escrita em determinadas posições de memória, autenticando-se devidamente, também através de comandos para o efeito, nos blocos de memória respetivos.

Após esta operação de escrita e bloqueio(*Write Once - WO*), os registos respetivos apenas poderão ser lidos indefinidamente(*Read Many - RM*).

### 2.4.6 NFC

NFC é uma tecnologia *wireless* de curto alcance que permite dispositivos móveis interagirem ativamente sobre objetos físicos passivos ou outros dispositivos móveis, criando uma

ligação entre o mundo físico e os dispositivos móveis, de forma a beneficiar os utilizadores sob a forma de facilitar os processos entre estes.[41]

O NFC é desenvolvido com base em muitos pressupostos do RFID e das tecnologias *smartcards*, que permitem de forma ativa, guardar e ler dados a uma certa distância. Como referido atrás, o RFID teve e continuará a ter um papel preponderante nas muitas aplicações onde foi consistentemente revolucionário, ao nível da automação, e rapidez que induziu nos mais distintos processos. Por outro lado, surgiram alguns problemas associados à segurança(ao nível da interceção de dados, clonagem de *tags*, etc.), sendo que o NFC, em algumas aplicações, vem colmatar estas desvantagens associadas ao RFID.[41]

Todas as referências relativas ao NFC apresentadas neste sub-capitulo estarão de acordo com as especificações do *NFC Forum*[4]. Este acaba por ser uma associação industrial global que representa os interesses do "ecossistema NFC"[5]. Na Figura 2.15 podem-se verificar algumas das áreas de interesse que tomam parte ativa na evolução desta tecnologia, através de grupos industriais que os representam, e assim perpetuar os bons resultados inerentes a esta dinâmica evolutiva que tanto representa o funcionamento do *NFC Forum*. A tecnologia NFC abordou algumas das preocupações levantadas ao nível das implementações RFID, logo numa fase inicial, limitando a separação física de interacção entre dois dispositivos(*tags* ou outros dispositivos móveis), para uma distância muito mais curta, impossibilitando assim, intercepções(de dados) por dispositivos alheios às implantações de uso destas tecnologias.[41]

É apresentado de seguida, alguns exemplos demonstrativos da potencialidade e da flexibilidade do NFC(não trata diretamente os modos de operação)[42; 43]:

- **Iniciador de Serviços**: A tecnologia é utilizada para fins de configuração e inicialização automática de outras, tal como o Bluetooth. Nestas circunstâncias apresenta-se como uma tecnologia de suporte. A Figura 2.16 torna percetível esta característica. Verifica-se através desta, que o NFC é das tecnologias com menor taxa de transmissão de dados, e de mais baixo alcance. Esta vantagem está associada às especificações do NFC que o caracterizam em regime de funcionamento como uma tecnologia automática, ou seja, sem necessidade de operações de inicialização e configuração. Esta funcionalidade do NFC tem sido amplamente aplicada, por exemplo, ao nível dos jogos *multiplayer* entre dispositivos móveis, em que existe a necessidade de transferência de dados entre os mesmos, e o NFC através de um simples, comummente designado "Tap ´n Go"[6], configura de ambos os lados de forma autónoma, os parâmetros, por exemplo do *Bluetooth*(permite uma taxa de

[4]O *NFC Forum* foi criado para promover o uso da tecnologia NFC, através do desenvolvimento de especificações, garantindo a interoperabilidade entre dispositivos e serviços. Este revelou ser preponderante na normalização da tecnologia, e da célere aceitação e implementação por parte das grandes corporações, pioneiras nas mais distintas áreas de aplicação, implementando esta tecnologia. Ver `http://www.nfc-forum.org/aboutus/`

[5]Este conceito representa a dinâmica com que o *NFC Forum* rege as suas especificações. O *NFC Forum* tem como membros influentes, companhias, das mais distintas áreas, que constantemente vão apresentando o seu trabalho desenvolvido, soluções e novas aplicações. Todas as decisões são aprovadas pelo voto destes membros, de forma a garantir flexibilidade e solidez das novas especificações, para o saudável e consistente desenvolvimento da tecnologia. Ver `http://www.nfc-forum.org/aboutnfc/ecosystem/`

[6]Ação de aproximação entre dois dispositivos móveis, ou entre um destes e uma *tag* NFC, para perfazer uma ação em qualquer um dos modos de funcionamento da tecnologia - implica sempre transferência de dados [41]


Figura 2.15: 'Ecossistema" do *NFC Forum* [44]

transferência mais apropriada para o bom funcionamento de jogos), sem necessidade dos utilizadores estabelecerem manualmente a comunicação segundo este protocolo, antes de iniciarem a aplicação, sendo todos estes processos efetuados em *background* pelo sistema operativo e o *chip* NFC;

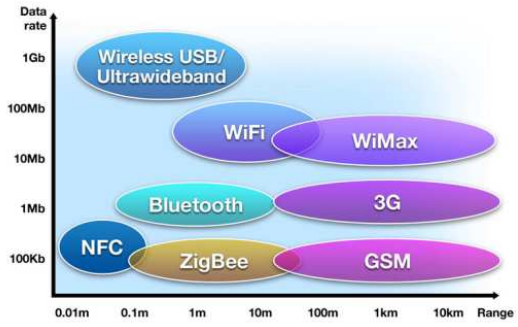



Figura 2.16: Tecnologias sem-fios e as suas regiões de funcionamento - taxa de transmissão de dados e alcance[44]

- **Ponto a Ponto/P2P**: Permite a comunicação(transferência de dados) entre dois dispositivos móveis dotados de tecnologia NFC;
- **Pagamentos e Bilheteiras Eletrónicas**: A tecnologia permite flexibilizar a forma de pagamentos e criar uma alternativa, por exemplo, ao nível dos sistemas de bilheteiras nos transporte públicos, entre outros serviços.

  Ambos, *MasterCard*® e *Visa*®, membros pioneiros do *NFC Forum*, já desenvolve-

ram aplicações para pagamento automático através de dispositivos móveis eletrónicos(e.g. telemóveis e *tablets*), pois esta tecnologia garante a segurança necessária para efetuar transações seguras, em grande parte devido ao funcionamento de curto alcance.[43]Ver sub-Figura 2.17(a).

Aquisição de bilhetes de avião, transportes públicos comuns, eventos, entre muitos outros serviços, é outra funcionalidade que tem vindo a ser desenvolvida e aplicada nos mais diversos meios, pela flexibilidade e simplicidade que induz nos processos deste tipo.[43]Ver sub-Figura 2.17(b).


(a) Uso do NFC, e de uma aplicação específica(pertencente à *MasterCard*® ou *Visa*®), para pagamento automático

(b) Equipamento de bilheteira electrónica onde o utilizador aproxima o dispositivo para validar a entrada, ou comprar o bilhete

Figura 2.17: Imagens relacionadas com o uso do NFC em sistemas de pagamento e bilheteiras automáticas [43]

De forma mais simplista, nos cenários de uso mais comuns, os dispositivos móveis irão analisar, adquirir e atuar sobre os dados disponíveis em cartazes publicitários e pontos de venda, conectar e trocar dados entre dispositivos de outras pessoas, emular os *chips* NFC em *tags* RFID/NFC para operações de pagamentos, controlo de acessos, entre outros.

Na Figura 2.18 ilustra-se as áreas de interesse, serviços, e aplicações com dispositivos móveis inerentes às mesmas, em que o NFC tem vindo a tornar-se parte ativa, desenvolvendo soluções e otimizando processos.

#### 2.4.6.1 Funcionamento

Como já referido, o NFC é uma tecnologia de comunicação sem fios de curto alcance, com o princípio de funcionamento do RFID, que recorre à indução de campos eletromagnéticos para permitir a comunicação entre dois dispositivos eletrónicos a curta distância.[42]

Opera numa gama de frequência não licenciada , 13,56 *megahertz* (MHz), a uma distância de até 20 *centímetros* (cm)[7].Suporta três valores de taxas de transferência de dados, sendo estes, 106 *Kilobits*/segundo (kbit/s), 212 kbit/s e 424 kbit/s. Maiores taxas são esperadas para o futuro.[42]

[7]A distância de operação desta tecnologia não é consensual na literatura, nem ao nível dos fabricantes de soluções NFC. Tipicamente aparecem referências, limitando o funcionamento aos 7cm e 10cm. É provável que esta disparidade esteja associada ao ambiente de "medição", ou seja, os ensaios são efetuados, no fim da montagem do produto, onde já existem interferências provocadas por barreiras físicas, etc.


Figura 2.18: Representação das áreas de interesse/aplicação do NFC, casos de uso respetivos, e genericamente, os serviços de interesse alvo [44]

Para se estabelecer comunicação entre dois dispositivos NFC, pelo menos um deles precisa de ser capaz de perfazer operações de leitura/escrita(read/write), ou seja, é necessário existir um "leitor"[8] e uma *tag*, ou no caso do último modo de funcionamento atrás especificado, dois dispositivos dotados de um *chip* NFC. Estas *tags*, têm na sua maioria, a mesma arquitetura das *tags* RFID. Destas, existem mesmo, exemplos compatíveis entre as duas tecnologias.

Existem dois modos de funcionamento, passivo e ativo, que serão descritos mais pormenorizadamente nas seguintes secções. As especificações relativas ao modo de funcionamento vêm do fato da crescente preocupação pelos consumos energéticos dos sistemas, e sua autonomia.

#### 2.4.6.2 Modos de Comunicação

*Nota: O conteúdo desta sub-sub-secção tem como base informações recolhidas nas referências [42; 45; 46]*

Um dispositivo NFC pode funcionar em dois modos distintos, no modo ativo e no modo passivo. Tal como no RFID, o primeiro caso implica a existência de uma bateria que alimenta o circuito, no que toca ao requisito energético destinado a induzir o campo eletromagnético que permite estabelecer comunicação com outros dispositivos. O modo passivo é caracterizado por o circuito ser alimentado pela energia contida na onda eletromagnética(especificamente ondas rádio à frequência referida acima) do dispositivo iniciador/*initiator*.

Paralelamente à descrição destes modos, é importante referir a designação que corresponde aos dispositivos em funcionamento. Como já indiciado em cima, o dispositivo

[8] Ao contrário do *RFID*, no NFC não faz tanto sentido descrever um subsistema como "leitor", sendo que no limite, esta unidade, será capaz de operar em qualquer um dos modos especificados nas normas de funcionamento - leitura/escrita(*read/write*); modo de emulação(*emulation mode*) e P2P

iniciador/*initiator* funciona no modo ativo e caracteriza-se por ser ele o indutor de energia para outro dispositivo e o responsável por despoletar o inicio da comunicação. O dispositivo estimulado, é designado o alvo/*target*, e normalmente são aplicados em etiquetas, porta-chaves, cartazes, publicidade genérica, entre outros.

Assim, de forma mais clara, descreve-se os dois modos de comunicação da tecnologia NFC:

- **Comunicação em Modo Ativo/*Active Mode***: Ambos os dispositivos, *initiator* e *target*, comunicam, gerando alternadamente os seus próprios campos eletromagnéticos. Um dos dispositivos desativa o seu campo RF enquanto espera pela receção de dados. Neste modo, tipicamente, ambos os dispositivos são energeticamente autónomos.

- **Comunicação em Modo Passivo/*Passive Mode***: O dispositivo iniciador providencia a energia necessária para o *target*, modelando este último o campo induzido para retransmissão de dados. O funcionamento do dispositivo alvo/*target* é bastante percetível, quando comparado, por exemplo, como o funcionamento de um *transponder*[9].

#### 2.4.6.3 Modos de Operação

Os modos de operação são as diferentes formas de funcionamento, possíveis de implementar com um dispositivo dotado de um chip NFC. A existência de cada um permite flexibilizar a tecnologia nas mais diversas áreas de interesse, na medida em que, embora diferentes modos de operação sejam passíveis de aplicar para uma dada finalidade, existe sempre vantagens e desvantagens associadas à escolha. Algumas características relativas a estes modos de operação serão especificadas nas secções 2.4.6.4 e 2.4.6.5. A imagem 2.19 exibe um esquema que numa fase inicial pode conter excesso de informação, mas que contém os mais importantes elementos ao funcionamento e modo de operação das três soluções possíveis, podendo ainda ser uma imagem de consulta posterior para melhor compreensão destes. A imagem é editada de outra, disponibilizada no NFC *Forum*, sendo a sua referência apresentada por ser uma fonte opcional de informação útil.

[9]É um dispositivo de comunicação eletrónico complementar de automação e cujo objetivo é receber, amplificar e retransmitir um sinal

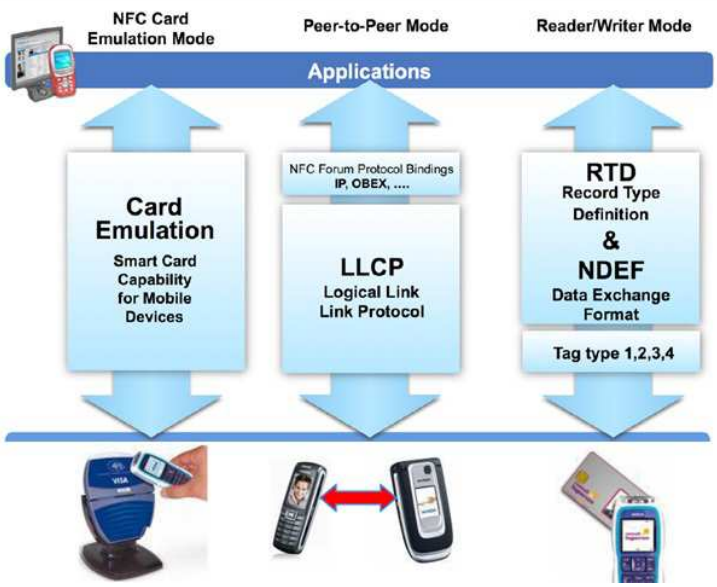



Figura 2.19: Esquema dos modos de operação definidos pelo NFC *Forum* com referência a algumas especificações inerentes ao seu funcionamento[47]

Posto isto, os três modos de operação do NFC são:

- **Leitura/Escrita(*Read/Write*)**

  Assemelha-se em muito ao funcionamento do RFID. Permite ler o conteúdo(dados) pré-gravados em *tags*[10] RFID/NFC contidas em panfletos, cartazes, pontos turísticos, e outros.

  A vantagem clara, relativamente ao RFID, é que o *NFC Forum* especifica o formato de encapsulamento de dados nas mensagens trocadas entre dispositivos NFC, além de diversos tipos de registos[11] que, por exemplo, no uso de dispositivos móveis com sistema operativo Android®[12], lido o conteúdo de uma *tag*, eventos são despoletados com base na interpretação de um dado *NFC Record Type* (NRT). Por exemplo, chegando a um ponto turístico e aproximando um dispositivo móvel dotado deste SO, a um ponto de leitura *NFC*, é de forma automática é aberto um *web site* com diversas curiosidades relativamente ao espaço visitado. Na verdade as aplicações são infindáveis, desde que, os eventos NFC associados a uma ação do utilizador no mundo real, sejam orientados para tal. Sintetizando, para além das simples operações de leitura e escrita não normalizadas que podem ser efetuadas(tal como no RFID), este modo permite transmitir mensagens definidas pelo *NFC Forum*, e é suportado pelas *Application Programming Interfaces* (APIs) de desenvolvimento de aplicações direcionadas a dispositivos móveis sem fios, permitindo conectar os utilizador ao mundo virtual de forma bastante interativa.[41; 42; 45]

[10] Estas *tags* devem ser de um dos quatro tipos suportados e especificados pelo *NFC Forum*

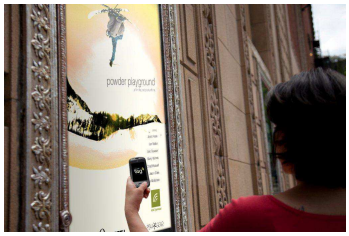
[11] Disposição seguindo uma estrutura pré-definida para guardar diferentes tipos de registos na memória de uma *tag*, tais como, *Uniform Resource Identifiers* (URIs), simplesmente texto com recurso a registos **MIME, etc.!** (**MIME, etc.!**)

[12] Sistema operativo da Google® para *tablets* e *smarthpones*

Genericamente a grande função deste modo de operação, do ponto vista do utilizador, é aceder a informação em "movimento"(de forma intuitiva e rápida). A necessidade de quem pretende prover acesso a qualquer tipo de informação/conteúdo publicitário, acaba também por ser facilitada, na medida em que simplifica e embaratece os processos inerentes aos modos de disponibilização da informação, tendo como base, os dados que indicam para a centralização destes, para dispositivos móveis e tecnologias que suportam NFC.


(a) Proposta de um URL de um *web site*[48]


(b) Detalhes de um filme, num *web site*, proposto pela leitura de uma *tag* na capa do DVD do mesmo[43]



(c) Aproximação a uma *tag* contida num panfleto publicitário que conterá informação extra sobre o mesmo[49]

Figura 2.20: Alguns exemplos de aplicação, do modo leitura/escrita(NFC)

- **Modo de Emulação(*Emulation Mode*)**

Este modo permite um dispositivo com tecnologia NFC comportar-se, e perfazer os serviços até agora concebidos pelas tecnologias *smartcards* e por *tags*. Um dispositivo móvel, dotado de um chip NFC é capaz de ser sujeito a operações de leitura e escrita, por outro, em modo leitura/escrita.[48; 50]

É bastante utilizado em sistemas de pagamentos, tais como, aquisição e validação de bilhetes associados a transportes, previamente desenvolvidos, e baseados nas tecnologias *Mifare*®, *Calypso*® e *Felica*®, parques de estacionamento, eventos desportivos, e tal como já referido atrás, nas aplicações desenvolvidas pela *MasterCard*®e *Visa*®, respetivamente, *PayPass* e *ExpressPay*. Embora outros modos sejam aplicáveis para fins de controlo de acessos, o modo de emulação também é uma solução bastante válida.[50] Na Figura 2.21 algumas imagens de aplicações e tecnologias que aplicam este modo de operação.


(a) Leitor para pagamentos através do modo de emulação NFC[52]

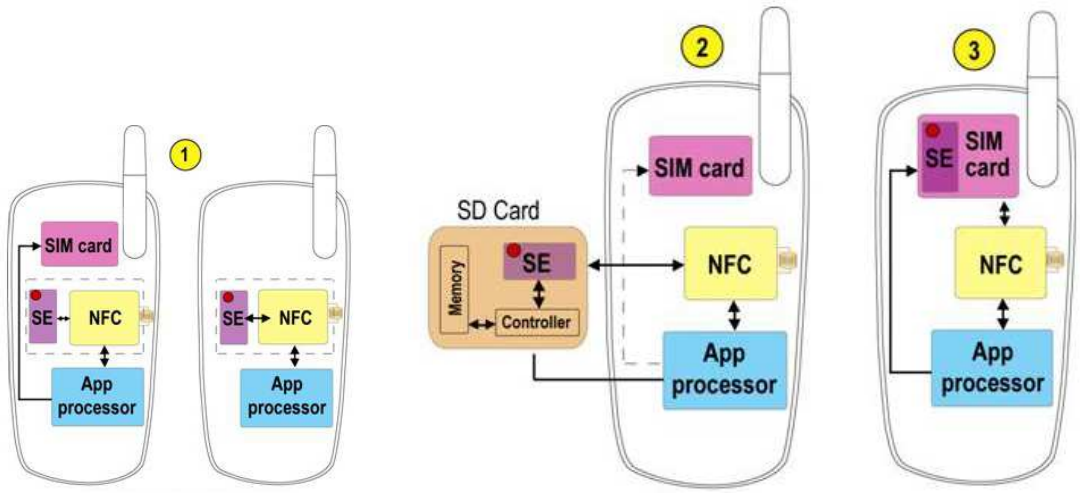

(b) Leitor para pagamento e validação de bilhetes numa rede de transportes ferroviária japonesa - utiliza a tecnologia desenvolvida pela Suica®[53]


(c) Posto de passagem automatizado, por validação das credenciais, pela tecnologia *NFC*[54]

Figura 2.21: Alguns exemplos de aplicação, do modo emulação(NFC)

Estas aplicações tendem a aplicar este modo de funcionamento, pois a necessidade de garantir a segurança ao nível do código das aplicações, dos dados guardados por estas(dinamicamente no decurso do funcionamento das mesmas), das credenciais dos utilizadores, entre outros dados, é por si garantida. Esta potencialidade está associada ao fato desta recorrer a um módulo incorporado de segurança, tipicamente designado na literatura como *secure element*[13], que induz confiança ao nível dos responsáveis pelo desenvolvimento de soluções(*hardware* ou *software*), e garantias e fiabilidade, ao nível dos utilizadores.[51] Na Figura 2.22 estão representados os tipos comuns das arquiteturas de dispositivos móveis com diferentes soluções ao nível da posição dos elementos de segurança. O círculo vermelho, comum nas sub-figuras, diz respeito à localização da aplicação segura. A arquitetura correspondente à sub-Figura 2.22(a), designada "Tipo incorporado/*Embedded Type*", é normalmente aplicada, por preferência, pela Apple®e Google®. A sub-Figura seguinte, 2.22(b), arquitetura baseada em cartões microSD(*MicroSD Based Type*), é tipicamente aplicada por bancos e companhias de cartões de crédito, ou seja, instituições financeiras. O último caso, referente à utilização do *Secure Element* (SE) dos cartões SIM, caracteriza-se por ser o modelo mais aplicado pelas marcas que recorrem à sua utilização.[55]

[13]Também designado, Ambiente de Execução e Memória Segura/(*Secure Memory and Execution Environment*), que reside nos denominados *crypto chips*, e que consiste num ambiente dinâmico em que o código das aplicações e seus dados possam ser guardados e administrados de forma segura, e onde as aplicações em causa, são executadas(não se trata apenas de um módulo auxiliar de execução). A arquitetura associada a estes módulos apresenta diferentes soluções. Alguns fabricantes desenvolvem-no incorporado nos próprios *chips* NFC, enquanto outros recorrem aos mesmos já existentes em hardware disponível no dispositivo eletrónico em questão(e.g. incorporados nos SIM/*Universal Integrated Circuit Card* (UICC), cartões *Secure Digital* (SD)).[51]




(a) *Chip* NFC como *router*, com as aplicações localizadas no elemento de segurança incorporado

(b) *Chip* NFC como *router*, com as aplicações seguras num elemento de segurança externo, num cartão SD

(c) *Chip* NFC como *router*, com as aplicações seguras num elemento de segurança externo, no cartão SIM

Figura 2.22: Tipos de elementos de segurança/*secure elements*[55]

- **Ponto a Ponto(P2P)**

  Neste modo de operação, comunicação P2P, a tecnologia NFC é utilizada para estabelecer a comunicação entre dois dispositivos, para estes, localmente transmitirem dados entre si, criando uma nova forma de interação entre dispositivos móveis. Como já referido atrás, quando a quantidade de dados atinge um valor alto(tipicamente acima de 1*kilobyte*), capaz de induzir um tempo de transferência de dados não expectável por partes dos utilizadores(face a outras tecnologias já existentes), o NFC tem funções de ativação e configuração de outras tecnologias sem fios, como *Wi-Fi* ou *Bluetooth*, sendo estes depois, os responsáveis pela transmissão de dados para o outro dispositivo.[41; 42; 45]

  O método de interacção passa simplesmente, depois de ter ativado o NFC em ambos os dispositivos, aproximá-los à distância mínima de funcionamento[14]. Ao estabelecer-se a comunicação, após a interacção inicial(configurações), é proposto o envio de dados, normalmente necessitando de uma interacção física de confirmação. No caso dos dispositivos móveis com sistema operativo *Android*®, o processo passa, por exemplo, por um dos utilizadores ter um contacto da lista telefónica, imagem, vídeo, *website*, ou outro (no ecrã), efetuar o processo descrito acima, carregando no ecrã para gerar o evento que inicia a transferência. A *Google*® definiu este processo, para induzir facilitismo linguístico na descrição do processo entre os utilizadores, como um "Android Beam"[15].

[14]Na maior parte dos dispositivos disponíveis no mercado é necessário que a distância entre estes seja ínfima, sendo que, na maior parte dos casos, é necessário encostá-los

[15]É uma característica do sistema operativo *Android*®que permite a troca de dados via NFC,que facilita a troca rápida, através de uma comunicação de curto alcance, de contactos, vídeos do *YouTube*®, direções, entre outros dados. Consultar `http://en.wikipedia.org/wiki/Android_Beam`


(a) Representação do evento do sistema operativo *Android*® no momento em que o utilizador deve validar o envio/*Beam*, através de um toque no ecrã[56]

(b) Imagem retirada do vídeo de apresentação da Google®(Google I/O: *How to NFC*); *Beam* de vídeo do *Youtube*® numa secção avançada do *stream*[57]

Figura 2.23: Imagens relacionadas com o modo de operação P2P, mais especificamente, referentes ao "*Android Beam*"

#### 2.4.6.4 *NFC Forum* - Especificações dos Tipos de *Tags*

O *NFC Forum* especifica quatro tipos de *tags* operáveis por dispositivos NFC. Estas contêm dados(posições de memória contentora de dados) e são normalmente apenas de leitura, sendo que nalguns casos, principalmente em ambiente de desenvolvimento de produtos ou serviços, sejam passíveis de ser reescritas. Elas podem ser codificadas de forma personalizada pelos fabricantes, embora devam seguir as especificações do *NFC Forum*. Estas *tags* são utilizáveis em qualquer aplicação que recorre ao modo de operação *read/write*, com alguns dos usos já exemplificados. As especificações definidas por este organismo, insere-se num grupo de resoluções que permitiram ao *NFC Forum* induzir interoperabilidade entre dispositivos e serviços NFC. Estes fatores, associados ao bom desenvolvimento da tecnologia, induzidos pela normalização(organizada) imputada ao *NFC Forum*, assenta no fato destas especificações terem conseguido abranger as soluções já existentes[16].[45; 50] A Figura 2.24 pretende demonstrar as especificações inerentes a cada tipo, e de que forma estas assentam sobre elas, sendo que umas caracterizam a tecnologia ao nível das camadas mais baixas de funcionamento, até às mais superiores(que definem a estrutura das mensagens).

[16]Para consulta mais pormenorizada das especificações, consultar `http://www.nfc-forum.org/specs/`

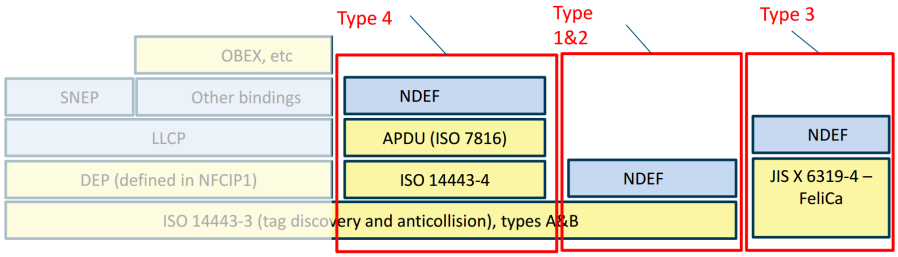



Figura 2.24: Pilha protocolar para as especificações dos tipos de *tags* definidos pelo *NFC Forum* [58]

Posto isto, as quatro especificações definidas pelo *NFC Forum* são:

- **Tipo 1(*NFC Forum Type 1 Tag*)**

  Estas *tags* têm como característica principal, o fato de serem relativamente mais baratas do que as outras soluções. Têm uma capacidade de 96*bytes*(expansíveis para 2*kiloBytes*), são passíveis de serem reescritas, configuráveis para limitar a sua utilização a apenas leitura, não têm proteção contra colisão de dados, e apresentam um taxa de transferência de dados de 106 *kbit/s*. Esta especificação tem como base a ISO/*International Electrotechnical Commission* (IEC) 14443A, e tem como produtos compatíveis, as Topaz®(marca exclusiva da *Innovision Research & Technology*) e as *tags* da Broadcom®, BCM20203.[45; 50; 58; 59]

- **Tipo 2(*NFC Forum Type 2 Tag*)**

  Esta especificação define a mesma estrutura protocolar do que o caso anterior, ISO/IEC 14443A, e segue a especificação NDEF[17], relativamente ao formato de encapsulamento das mensagens durante a troca de dados de dispositivos NFC. A diferença mais aparente, face ao caso anterior, é o fato destas suportarem funcionalidades de anti-colisão de dados. Suportam 98*bytes* (expansíveis para 2*kiloBytes*), são passíveis de serem reescritas, configuráveis para limitar a sua utilização a apenas leitura, e apresentam um taxa de transferência de dados de 106 *kbit/s*. Esta especificação tem como produtos compatíveis, as *tags* produzidas pela NXP® : *NXP Mifare Ultralight, NXP Mifare Ultralight C, NXP NTAG203*.[45; 50; 58; 59]

- **Tipo 3(*NFC Forum Type 3 Tag*)**

  A especificação para as *tags* tipo 3 são baseadas numa norma definida pelo organismo japonês de normalização, *Japonese Industrial Standard* (JIS), e são configuradas pelos fabricantes para funcionarem apenas no modo de leitura, ou leitura-escrita, podendo ainda serem posteriormente configuráveis pelos utilizadores para funcionar no primeiro modo. O tamanho de memória é teoreticamente variável, sendo que, podem atingir até 1*MegaByte* por serviço. Apresentam duas taxas de transferência de dados passíveis de serem aplicadas, 212 *kbit/s* e 414 *kbit/s*, tal como os mecanismos de anti-colisão. O produto compatível no mercado foi desenvolvido pela *Sony*®, denominado *Felica*.[45; 50; 58; 59]

[17]Formato de mensagens binário que pode ser usada para encapsular um ou mais, conjuntos de registos(*message records*), de tipo e tamanho arbitrário, numa mensagem de construção única.

- **Tipo 4(*NFC Forum Type 4 Tag*)**

  Pela imagem 2.24 rápido se conclui as tecnologias que assentam nesta especificação são ligeiramente mais complexas, ou que pelo menos as normas existentes em que se baseiam são em maior número, e por isso induziram uma maior complexidade na sua formulação. Esta afirmação pode ser suportada, também, pelo fato de entre as 4 especificações técnicas neste ponto referidas, apenas esta ir na versão 2.0(Novembro de 2010), enquanto as outras mantém-se na versão 1.1.

  A diferença face às outras soluções deve-se a esta ser compatível com ambas as interfaces de comunicação definidas na norma ISO/IEC 14443, Tipo A e Tipo B. A diferença entre eles está relacionada com os métodos de modulação, esquemas de codificação e procedimentos de inicialização. Esta norma é composta por quatro partes, cada uma referindo-se a grupos de especificação diferentes, tais como, características físicas da tecnologia(Parte 1), protocolo de transmissão de dados(Parte 4), definições de inicialização e anti-colisão(Parte 3), e especificações relativas à interface de sinal e energia no campo RF(Parte 2). Pela figura atrás referida vê-se mais claramente quais foram as partes ativas da norma que serviram de base para a especificação do *NFC Forum*. Como penúltima camada característica da tecnologia verifica-se a referência à *Application Protocol Data Unit (APDU)(ISO 7816)*, que define também nas suas quatro partes constituintes especificações relativas a características físicas dos circuitos integrados, dimensões e localização dos contactos elétricos dos mesmos, protocolos de transmissão e sinais elétricos.[60; 61]

  As *tags* deste tipo caracterizam-se por também poderem ser apenas de leitura(ou pós-configuráveis para tal) e de leitura/escrita, dimensão da memória variável com limite até 32*kiloBytes* por serviço, suportam taxas de transferência de dados de 106 *kbit/s*, 212 *kbit/s* e 414 *kbit/s*, suportam mecanismos de anti-colisão de dados, e são compatíveis com os produtos *NXP DESFire* e *SmartMX-JCOP*.[45; 50; 58; 59]

#### 2.4.6.5 *NFC Forum* - Especificações Técnicas

O NFC *Forum* além de ter criado as especificações apresentadas em 2.4.6.4, definindo-as no grupo "NFC *Forum Tag Type Technical Specifications*", definiu também e continua a revisar, o conjunto de especificações que denominou "Protocol Technical Specification", que é constituída por um total de seis. Este grupo pretende normalizar e esclarecer a indústria e seus fomentadores, das especificações que estão diretamente relacionadas com o funcionamento da tecnologia, desde os mecanismos de segurança que garantem o fluxo de dados, à forma como este fluxo se dá, do processo de estabelecimento de ligação nas camadas de funcionamento mais baixas, aos mecanismo anti-erro na transferência de tramas entre dispositivos, etc.

- **NFC *Logical Link Control Protocol* (LLCP)**

  Define um protocolo de segunda camada *Open Systems Interconnection* (OSI) que permite o NFC suportar o modo de operação P2P, sendo estas especificações de suma importância para qualquer aplicação NFC que involva comunicação bi-direcional. O LLCP define dois tipos de serviços: sem conexão/*connectionless* e orientado à conexão/*connection-oriented*, organizados em três classes de serviços de ligação. O primeiro consiste, em apenas, serviços sem conexão; o segundo, apenas

serviços orientados à conexão; e serviços tanto sem conexão e orientado à conexão. O serviço "sem conexão" oferece uma configuração mínima, sem confiança, ou garantias de controlo de fluxo oferecidas pela *ISO/IEC 18092* e a *ISO/IEC 14443*. O outro apresenta um funcionamento mais consistente, suportado por mecanismos, tais como, controlo de fluxo, serviços de multiplexação de camada(*session-based service layer multiplexing*), etc.

Este protocolo é bastante compacto, baseado nas normativas industriais *Institute of Electrical and Electronics Engineers (IEEE) 802.2*, pensada para suportar, tanto aplicações com limitadas capacidades de transporte de dados(e.g. pequenos ficheiros), tal como, protocolos de rede, como *OBject EXchange* (OBEX)[18] ou TCP/IP, que por seu lado providenciam ambientes de serviços mais robustos para aplicações(ao nível de taxas de transferência e de fiabilidade qualitativa destas, com ficheiros de grande dimensão). O LLCP ainda proporciona uma base sólida para aplicações P2P, melhorando as funcionalidades básicas oferecida pela *ISO/IEC 18092*, sem afetar a interoperabilidade das aplicações e *chipsets*[19] NFC.[44]

Concluindo, o LLCP é responsável pela ativação da comunicação, sua supervisão e desativação da mesma; especifica como dois dispositivos *NFC Forum* dentro de uma distância de comunicação, reconhecem a versão LLCP compatível entre ambos; define os passos necessários para o estabelecimento da comunicação, sua supervisão, e posterior desativação; caracteriza os conceitos de dispositivo iniciador /*initiator* e alvo/*target*, e as características protocolares inerentes aos dois; de que forma ele está apto a acomodar várias instâncias de protocolos de mais alto nível, ao mesmo tempo; entre outras especificações. Consultando a imagem 2.25 fica-se com uma ideia mais clara, onde estas especificações assentam, e de que forma, e conjunto de normativas são necessárias, para se estabelecer uma comunicação P2P(já atrás descrita em 2.4.6.3).[62]

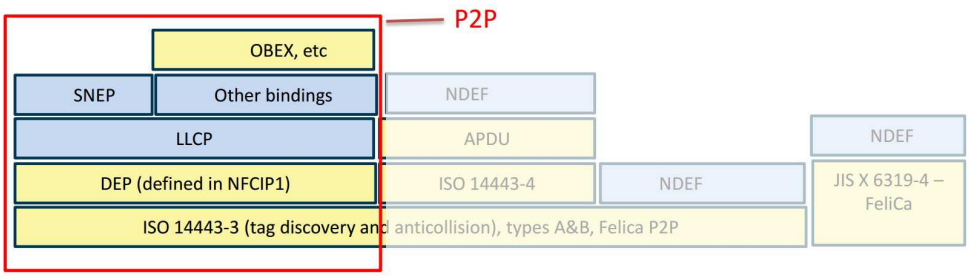



Figura 2.25: Pilha protocolar com especificações do *NFC Forum* a azul, e protocolos de apoio já existentes, com evidenciação no modo P2P [58]

- **Protocolo Digital NFC/*NFC Digital Protocol***

  Esta especificação trata o protocolo digital para comunicação de dispositivos com a tecnologia NFC, oferecendo uma especificação de implementação sob a camada

[18]Protocolo de comunicação que facilita a trocar de objetos binários entre dispositivos. Este protocolo tem a particularidade do *Modbus* - protocolos de comunicação não interferentes ao nível do *hardware*. O OBEX serve de base, por exemplo, a algumas especificações *Bluetooth*

[19]Conjunto de componentes eletrónicos, num cirguito integrado, que gere o fluxo de dados entre o processador, memória e outros periféricos

protocolar regida pela *ISO/IEC 18092* e a *ISO/IEC 14443*, permitindo harmonizar as tecnologias integradas, especificar as opções de implementação, e os limites de interpretação das normas. Na essência, pretende demonstrar aos engenheiros de desenvolvimento como as normas direcionadas ao NFC, *ISO/IEC 14443* e *JIS X6319-4*, juntas, podem garantir a interoperabilidade global entre diferentes dispositivos NFC (e entre os próprios equipamentos semelhantes), tal como as infraestruturas onde são aplicados.

O que pretende esta especificação, é definir o conjunto de características comuns que podem ser usadas de forma consistente e sem modificações para as principais aplicações NFC, em áreas como serviços financeiros e transportes públicos. A especificação abrange a interface digital e o protocolo de transmissão *half-duplex*[20] do dispositivo com tecnologia NFC nos seus quatro papéis como objeto iniciador/*initiator*, alvo/*target*, "leitor/escritor" e *smartcard*/*tag* emulada. Inclui codificação de bits, taxas destes, formatos das tramas de mensagens, protocolos e conjuntos de comandos, que são usados por dispositivos habilitados para troca de dados, e vinculáveis ao protocolo LLCP.[44]

- **Protocolo de Atividade NFC/*NFC Activity Protocol***

  A especificação de atividade explica como a especificação anterior pode ser usada para configurar o protocolo de comunicação com outro dispositivo ou *tag* NFC *Forum*. Descreve os blocos de construção/*building blocks*(Atividades), para a definição do protocolo de comunicação. Estas atividades podem ser usadas, tal como presentes na memória descritiva do documento, ou podem ser modificadas para definir outras formas de configuração do protocolo de comunicação, cobrindo os mesmos ou outros casos de uso. As atividades são combinadas em perfis. Cada perfil tem parâmetros de configuração específicos e aborda um caso de uso particular. O documento respetivo a esta especificação define os perfis de deteção/pesquisa/sondagem(*polling*) e o estabelecimento de uma comunicação P2P, *polling* e leitura de mensagens NDEF de uma NFC *Forum tag*, ou o processo de *polling* em simultâneo de um dispositivo e tag NFC.

  A combinação de atividades e perfis define um comportamento previsível de um dispositivo NFC *Forum*. Isto não limita os mesmos de implementar outros blocos de construção ou definir outros perfis (para distintos casos de uso), sobrepostos noutros já existentes.

- **NFC *Simple NDEF Exchange Protocol* (SNEP)**

  O SNEP permite uma aplicação em um dispositivo habilitado para NFC trocar mensagens NDEF com outro dispositivo NFC *Forum*, quando estes, em funcionamento P2P. Este protocolo faz uso do transporte orientado à conexão LLCP para providenciar uma troca de dados fiável.[44]

- **Protocolo Analógico NFC/*NFC Analog Protocol***

  Esta especificação aborda as características analógicas da interface de RF do aparelho habilitado para NFC. O objetivo da especificação é caracterizar e especificar

[20] É apenas usado um canal de comunicação, o que implica que o dispositivo não pode enviar dados e recebê-los simultaneamente, implicando que só possa fazer uma das coisas de cada vez, ao contrário do modo *full-duplex*

os sinais observáveis externamente para um aparelho habilitado para o uso de NFC, sem especificar o design da antena destes. Isto inclui os requisitos de transmissão, energia, receção e formas de sinal(tempo, frequência, e características de modulação).

O documento respetivo a esta especificação é destinado ao uso, por parte dos fabricantes que querem implementar soluções com recurso à tecnologia NFC. Este documento aborda conceitos como, a interface analógica dos aparelho habilitados com NFC nos seus quatro modos de operação: iniciador/*initiator* em modo P2P, alvo/*target* no mesmo modo, modo leitura/escrita, e de emulação, para todas as três tecnologias(NFC-A,NFC-B, NFC-F), a todas as taxas de transferência mencionadas( 106 kbit/s, 212 kbit/s e 424 kbit/s).[44]

- **Controlo de Interface NFC/*NFC Controller Interface* (NCI)**

  A especificação NCI define uma interface padrão dentro de um dispositivo NFC, entre um controlador deste e o dispositivo processador principal da aplicação(*master* da comunicação). Esta normativa facilita o desenvolvimento por parte dos fabricantes de soluções NFC, principalmente ao nível da integração de diferentes *chipsets*(de outros fabricantes), e define um nível comum de funcionamento e interoperabilidade entre os componentes dentro de um aparelho habilitado para o uso desta tecnologia. Consultando o NCI, os fabricantes e engenheiros de desenvolvimento têm acesso a uma interface padrão que pode ser usada para o desenvolvimento de qualquer tipo de dispositivo com tecnologia NFC(e.g. computadores, *tablets*, telemóveis, etc.), permitindo aumentar o fluxo de produtos que se baseiem nesta tecnologia, para o mercado. O NCI fornece aos utilizadores uma interface lógica que pode ser usada com diferentes meios de comunicação(protocolos), tais como, *Universal Asynchronous Receiver/Transmitter* (UART), *Serial Peripheral Interface* (SPI) e *Inter-Integrated Circuit* (I2C).

Além deste grupo de especificações, o NFC *Forum* classificou um novo grupo, que contém apenas uma normativa. Este já foi mencionado atrás, sendo-o agora melhor caracterizado. Foi denominado *Data Exchange Format Technical Specification*, e determina o formato de intercâmbio de dados através da especificação NDEF.

- **Formato de Intercâmbio de Dados/NDEF**

  Especifica um formato comum de dados para dispositivos e *tags* compatíveis com o NFC *Forum*.[44] Estas mensagens, no seu conteúdo, ainda podem conter diversos tipos de mensagem, com um formato específico, também definidas pelo NFC *Forum*. Estes diferentes registos pretendem direcionar os eventos das aplicações, que se regem por estas especificações, de forma a flexibilizar a interação com os utilizadores, sob a forma de eventos espontâneos, através do automático reconhecimento dos registos pré-definidos/gravados pelos fabricantes.

  A imagem 2.26 exibe a estrutura simplificada de uma mensagem NDEF, que é composta por registos/*records*, tendo estes um número limitado, e sendo também, os seus tamanhos variáveis e igualmente limitados. O primeiro registo é obrigatoriamente distinto, pois tem funções de caracterização de toda a mensagem, sendo este constituído por um cabeçalho que prevê a definição de alguns valores para esse

fim, tal como bytes disponíveis para a mensagem em si, na zona disponível para o *payload*. Na figura seguinte, 2.27, um diagrama de atividade/comportamental de como o SO Android® opera, dependendo do conteúdo lido de uma *tag*.

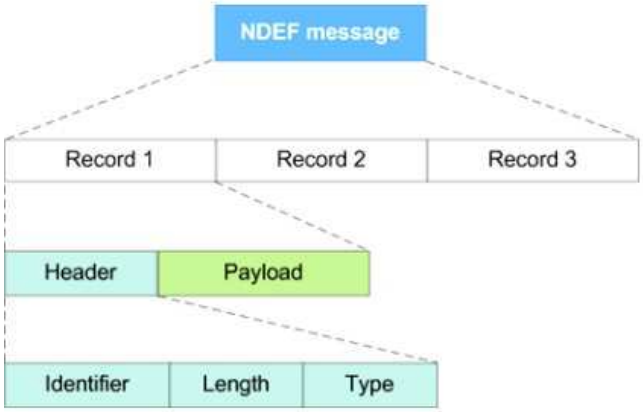



Figura 2.26: Arquitetura básica de uma mensagem NDEF [58]

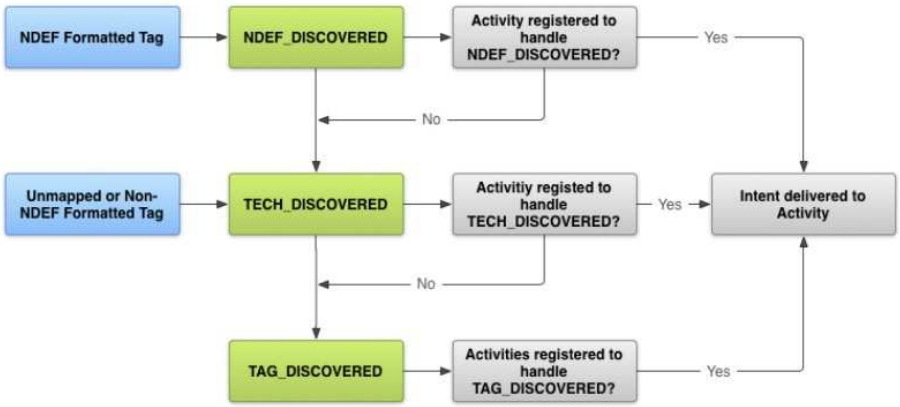



Figura 2.27: Diagrama de atividade simplificado do SO Android®, durante o evento de descoberta e leitura de uma *tag*[58]

Outro grupo de especificações denominado, *Record Type Definition Technical Specifications*, referido no grupo anterior, contém as especificações singulares para cada tipo de registo que podem conter uma mensagem NDEF, tendo sido estes criados para facilitar os eventos, das principais aplicações da tecnologia.

- ***NFC Record Type Definition (RTD)***

  Especifica o formato e as regras para a construção de tipos de registos padrão, usado pelo NFC *Forum*, e definições de aplicações de terceiros, que são baseados no formato de dados NDEF. A especificação RTD fornece uma maneira eficiente para definir formatos de registo para novas aplicações e dá aos utilizadores a oportunidade de criar as suas próprias aplicações com base em especificações definidas pelo organismo de normalização.[44]

- ***Text RTD***

  Fornece uma maneira eficiente de armazenar sequência de texto(*strings*) em vários idiomas, usando o mecanismo RTD e o formato NDEF.[44]

- ***URI RTD***

  Fornece uma maneira eficiente de armazenar URIs, usando o mecanismo RTD e o formato NDEF.[44]

- ***Smart Poster RTD***

  Utiliza as RTDs de texto e de URIs, como blocos construtores dela. É indicada para guardar conteúdos como, URLs, *Short Message Service*s (SMSs) ou números de telefone, numa *tag* ou em mensagens entre dispositivos em modo P2P.[44]

Finalmente, é também importante referir, o último grupo de especificações, designado *Reference Application Technical Specification*, que contempla as seguintes especificações técnicas:

- ***Tranferência(Handover de Conexão)***

  Define a estrutura e sequência de interações que permitem dois dispositivos habilitados com tecnologia NFC, estabelecerem uma conexão com outras tecnologias de comunicação sem fios. De forma simplista, esta especificação define os modos e formas de interação da tecnologia NFC com as outras referidas, como *WI-FI* ou *Bluetooth*, quando necessário implementar nas aplicações, por partes dos fabricantes, este recurso a tecnologias de suporte, quando tal seja vantajoso e necessário. O benefício está associado ao fato do NFC ser dotado de mecanismos de "negociação" e configuração, com estas tecnologias de forma automática. A especificação define ainda um "handover" estático, que consiste em gravar numa *tag* o conteúdo associado à configuração/ativação duma destas tecnologias, de forma automática, ou de gerar um evento em que tal seja necessário(onde inclua igualmente a ativação).

- **Comunicação de Dispositivos Pessoais de Saúde/*Personal Health Device Communication***

  Esta especificação cingiu-se na necessidade de normalizar a troca de dados, entre dispositivos NFC aplicados no campo da saúde. O objetivo desta é providenciar a interoperabilidade da transferência de dados entre dispositivos pessoais de saúde em conformidade com a norma *ISO/IEEE Std. 11073-20601* e as especificações do NFC *Forum*.

# Capítulo 3

# Sistemas de Controlo de Acessos Físicos: Revisão

Este capítulo pretende revisar aspetos mais focados, nos sistemas de controlos de acessos físicos, não de forma tão conceptual como o anterior, centrando a sua descrição, mais propriamente, nos componentes principais de uma implantação de sistemas de controlo de acessos físicos: topologias, tipos de leitores, riscos associados a este tipo de tecnologias-implantações de segurança, e tecnologias/protocolos de comunicação de suporte.

## 3.1 Conceito

Quando se faz referência a sistemas de controlo de acessos físicos, menciona-se um campo de controlo de acessos bastante específico, pois deixa-se de se generalizar os modelos, tecnologias de identificação e/ou autenticação, ou qualquer outro conceito, numa perspetiva de tentar validar um acesso a um dado objeto, seja este físico ou não. Verifica-se então, neste panorama, a clara divisão entre a aplicação deste tema ao nível computacional, relativamente ao mundo físico, sendo que, as arquiteturas dos sistemas, embora tipicamente suportadas nos mesmos modelos, apresentam uma clara distinção na arquitetura.

Neste caso, a barreira de acesso é física, tipicamente uma porta ou torniquete (maioritariamente em implantações com grande fluxo de indivíduos), sendo o acesso autorizado por sistemas automatizados ou por meios humanos(e.g. segurança, porteiro, rececionista). De realçar, no entanto, que embora as arquiteturas de sistemas de controlo de acessos físicos sejam bastante distintas, de um associado a um sistema computacional, os primeiros recorrem aos segundos para suportar as suas implantações. Este fato está associado à crescente necessidade de automatizar, flexibilizar, induzir rapidez no processo de decisão, e implantar modelos cada vez mais robustos, nos sistemas físicos.

O processo de análise das credenciais do utilizador, e do processo de decisão, em nada sofrem distinção neste caso. Os algoritmos de decisão, nas suas fases mais gerais, seguem exatamente o mesmo protocolo, já que os mesmo estão associados aos modelos já revistos, e como salientado, são transversais aos dois "mundos" de sistemas de controlo de acessos. Da mesma forma a operação dos sistemas no que toca ao requisito destes perante os utilizadores, é bastante semelhante, tal que algumas das tecnologias aplicadas para reconhecimento e validação, são aplicadas em sistemas computacionais e sistemas de controlo de acessos físicos. Portanto, o processo de identificação apresenta os mesmo

procedimentos ao nível dos indivíduos.

Ao nível das características que preveem junto da sociedade em geral e corporações, a confiança nestes sistemas, baseia-se no fato de serem sistemas praticamente ou completamente autónomos; terem taxas de erro ínfimas ou inexistentes; garantirem uma proteção de 24h/dia sem interrupções (ao contrário do recurso a meios humanos); terem associadas baixos consumos energéticos e consequentemente poupança de dinheiro; permitirem ao nível dos *softwares* de gestão, monitorizar e controlar acessos em tempo real; implementar sistemas de notificação de eventos muito específicos associados ao comportamento dos utilizadores ou do sistema; prevenir falsos alarmes; integrar sistemas de notificação baseados nos mais diversos serviços (e.g. *email*, SMSs, etc.); gerir mais facilmente o comportamento do sistema em situações de evacuação, férias, e feriados (entre muitas outras funcionalidades).

## 3.2 Componentes

A arquitetura típica mais simplista destes sistemas apoia-se no uso, junto ao acesso físico a ser controlado, de um leitor, uma fechadura elétrica, um botão de saída, e de um sistema de fecho automático do acesso. Estes estão normalmente ligados a um painel de controlo (com um CPU) que pode ou não comunicar com um sistema remoto de controlo e gestão, podendo este estar incorporado no mesmo, ou no próprio leitor. Com estes elementos base, existem algumas soluções que se distinguem nos modos de comunicação, protocolos dos mesmos, meio de comunicação com o gestor global do sistema, ligações elétricas, entre outros.

Além dos elementos físicos chave, referidos atrás, os sistemas de controlos de acessos físico recorrem ainda a dispositivos extra, que potenciam o bom funcionamento da instalação, fornecendo ao sistema dados adicionais que podem ser considerados relevantes dependendo da implantação em causa. Monitores de temperatura, detetores de movimento, detetores "glass-break", botões de pânico, são alguns exemplos. Ainda, noutra classe de dispositivos, denominados *output devices*, se especificam dispositivos que reagem sob ordens do sistema (e não fornecendo dados a este), como por exemplo, *buzzers* de alerta, luzes (e.g. ao ser cedido um acesso pouco iluminado), controladores de elevador (caso a implantação em causa permita um acesso a todo um andar de um edifício), entre outros.[63]

A imagem 3.1 exibe os principais elementos funcionais associados a um dado nó de um sistema de controlo de acessos físicos. Apresenta ainda um esquema simplista das ligações entre os diferentes componentes e sua possível posição relativa ao ponto de acesso. A imagem seguinte, 3.2, é um pouco mais complexa, pretendendo demonstrar um exemplo de uma arquitetura simplificada de um sistema deste tipo, com uma variedade de dispositivos passíveis de ser indexáveis nestes, tal como uma câmara de vigilância, um *buzzer*, entre outras possibilidades. Esta imagem é bastante representativa da capacidade dos sistema eletrónicos serem facilmente integráveis, e na perspetiva dos sistemas em estudo, este pormenor é mais significativo, sendo que, quando maior a integração de sistemas complementares, maior a fiabilidade e menor a percentagem de erro no processo de validação, muito embora, a probabilidade de falha do sistema possa aumentar com a sua complexidade.

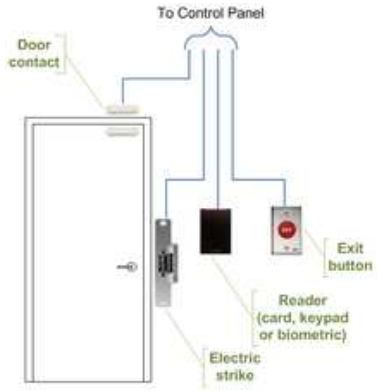



Figura 3.1: Representação dos elementos principais num ponto de acesso [68]

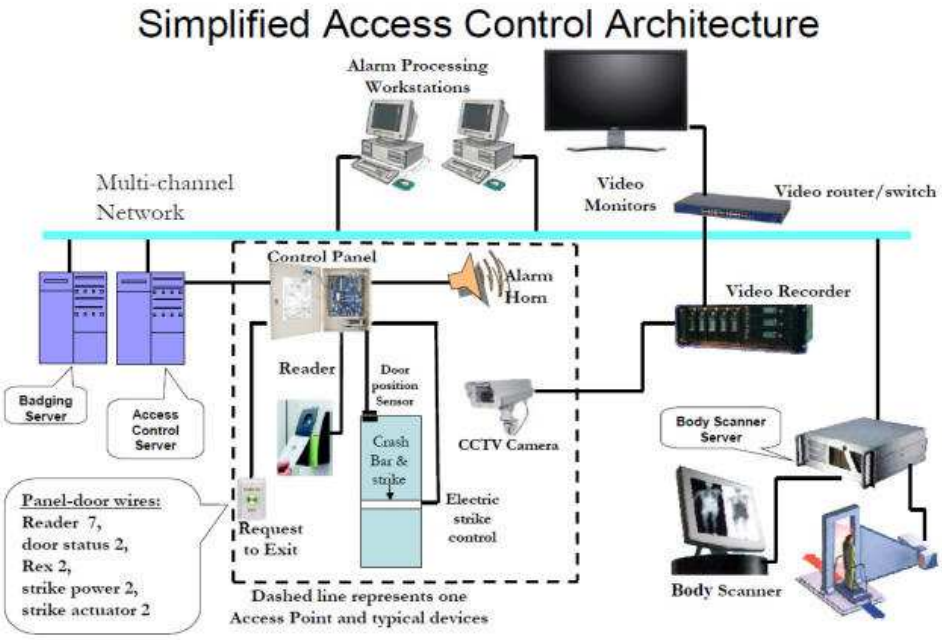



Figura 3.2: Exemplo de uma arquitetura simplificada de um sistema de controlo de acessos físico[65]

## 3.3 Tipos de Leitores

*Nota: O conteúdo desta sub-secção tem como fonte quase integral a referência em [66]. Todo o conteúdo que não lhe diz respeito, é normalmente referenciado.*

Sistemas de controlos de acessos físicos têm evoluído consideravelmente ao longo dos anos, tal que, as unidades respetivas aos sistemas mais antigos, eram bastante difíceis de instalar. O seu funcionamento baseava-se no uso de cartões inteligentes/*smart cards* e a inteligência do sistema(unidade de controlo e processamento) era normalmente aplicada no painel de controlo. Com o passar do tempo os dispositivos foram melhorados, e

atualmente, as soluções *state-of-the-art*, localizam na maior parte destas, a unidade de processamento no próprio leitor. Os mais recentes leitores do "tipo IP" fazem uso de uma rede *Ethernet* e são facilmente instalados nas implantações de uso. Neste tópico abordar-se-ão os diversos tipos de leitores passíveis de implementação, sendo que não se fará referência a dispositivos complementares de entrada ou saída típicos destes sistemas.

- **Leitores Básicos, não inteligentes**

  Este tipo foi aplicado nos primeiros sistemas de controlo de acessos físicos de portas automatizadas, utilizando leitores designados "não inteligentes", que se ligavam diretamente a um painel de controlo. Todos os requisitos de entrada e processamento de dados necessários é efetuado no painel de controlo. A aplicação de barramentos de comunicação *RS-232* ou *RS-485* entre os leitores, e o painel de controlo, também são muito comuns quando aplicado este tipo. Um exemplo de leitor deste tipo é desenvolvido pela *RFLOGICS*®, designado *RD Tiny*®.

- **Leitores Semi-inteligentes**

  Esta geração de leitores, que surge posteriormente aos anteriores, têm o seu destaque associado aos *upgrades* relativos aos leitores, sendo estes dotados de alguma "inteligência". Nesta fase eles já são capazes de controlar o *hardware* de ativação das fechaduras elétricas. Todas as outras funções continuam a necessitar do auxilio do painel de controlo, sob a forma, de reencaminhamento de dados do primeiro para este, e posterior re-envio da ordem a ser processada pelo leitor(abertura da fechadura, evento de notificação da negação de entrada, ou qualquer outro mais específico associado ao sistema). Neste tipo, os leitores são conectados aos painel central via barramento *RS-485*. Como exemplos deste tipo de leitores pode-se referir o *InfoProx Lite IPL200*®da *CEM Systems*®e o *AP-510*®da *Apollo*®.

- **Leitores Inteligentes**

  Estes leitores são capazes de autenticar os utilizadores recorrendo apenas ao uso dos mesmos, pois estes são dotados de memória e de unidade de processamento. Em termos de arquitetura, todos eles, são ligados via barramento único *RS-485*, ao painel de controlo. Este último, neste modelo, tem funções de processamento de eventos gerados pelos leitores; e providencia o sistema global com novas atualizações de configurações, e registo no histórico, dos acessos aos nós da rede.

- **Leitores e Controladores Inteligentes(IP)**

  Esta solução é a mais atual, sendo similar e um caso específico do tipo anterior, diferindo no aspeto do uso do painel de controlo. Esta configuração é a mais visivelmente aplicada ao nível de grandes edifícios, recorrendo ao uso de um computador remoto que gere todo o sistema através de um *software* de gestão de controlo de acessos físicos. Além desta clara distinção, onde existe uma plataforma de interação com os administradores e/ou utilizadores dos sistemas, estes recorrem a uma implementação de infraestrutura de rede padrão, para a comunicação entre os leitores e o gestor remoto, com uma cablagem (*Category 5 cable* (CAT5) ou *Category 6 cable* (CAT6)). Estas influem com uma clara diminuição de complicações, associadas à instalação elétrica destes tipos de sistemas, e pela facilidade de instalação e manutenção quando aplicadas. *PowerNet IP Reader* da *Isonas Security Systems*,

*ID08* da *Solus*(ambas com *web* interface *user-friendly*), *Edge ER40 reader* da *HID Global*, *LogLock* e *UNiLOCK* da *ASPiSYS Ltd.*, *BioEntry Plus reader* da *Suprema Inc.* e *4G V-Station* da *Bioscrypt Inc.* são alguns exemplos de leitores ou serviços que os contemplam, deste tipo e do anterior especificado.

## 3.4 Topologias

Nesta secção serão descritas as diferentes topologias de comunicação e de rede, implementáveis em sistema de controlo de acessos físicos. Fazer-se-á referência aos componentes principais, dispositivos de comunicação de rede, características gerais de funcionamento, e suas arquiteturas. Como já introduzido na secção anterior o controlo do sistema pode ser efetuado por um painel de controlo, um servidor, ou um *host Personal computer* (PC). As topologias predominantes atualmente são os denominados *distributed hub and spoke systems*, controlados por um painel de controlo funcionando como um *hub*, sendo os leitores os "*spokes*". Esta designação está associada ao normal funcionamento dos *hubs* que ao contrário dos *switchs* ou *routers* enviam os dados para todos os equipamentos a ele ligados. Embora o uso de painel de controlo pareça obsoleto, e sendo referido como a principal topologia utilizada, continua a ser dos mais aplicados. Por outro lado, em implantações que têm menos pontos de acesso são normalmente aplicado leitores *stand-alone*. É provável devido ao teor deste tópico que sejam referidos aspetos já mencionados acima(os leitores também caracterizam as topologias). Os nomes destas são apresentados em Inglês pela difícil tradução, e por serem normalmente referidas na literatura deste modo.[67]

- ***Stand-alone Intelligent Readers***

  Esta é a topologia mais simplista. Utiliza um leitor auto-suficiente para o normal funcionamento do sistema, e por esta razão, os leitores aplicados são do tipo inteligentes. Mesmo existindo uma implantação com esta aplicação em diversos acessos, não invalida o fato de estes serem completamente independentes, e de gestão autónoma. Não é necessário a utilização de um painel de controlo, e a gestão do sistema, tal como a sua complexidade, são de baixo nível. Os leitores aplicáveis nestas soluções são normalmente integráveis em sistemas que contemplem múltiplos acessos, podendo nesses casos, apresentar o recurso a módulos integrantes, que servem de intermediários com o *host* PC.

- ***Host PC with Serial Controllers***

  Os painéis de controlo são ligados ao *host PC* via comunicação série RS-485. Conversores RS-232/485 podem ter de ser utilizados para interligação entre os diferentes módulos do sistema. Em sistemas maiores são utilizadas placas com multi-portas I/O para facilitar a implementação destes.[68] A imagem 3.3 representa este tipo de arquitetura.

  - Vantagens:
    - RS-485 permite a utilização de cablagens relativamente longas - até cerca de 1200 metros;

  - A comunicação neste tipo de barramento é considerada rápida ao nível desta aplicação, permitindo ainda um limite até 32 dispositivos ligados ao barramento, possibilitando *requests* constantes do controlador, e assim, *updates* praticamente em tempo real do estado do sistema global;
  - Alta confiança e segurança associada ao sistema por estes não compartilharem a linha de comunicação com outros (e.g. sistema integrado de domótica).
- Desvantagens:
  - RS-485 não permite um rede do tipo "Estrela", a menos que sejam adicionados *splitters* ao sistema;
  - RS-485 não permite que o *host PC* comunique com diversos painéis de controlo simultaneamente;
  - RS-485 não é apropriado para a transferência de grandes quantidades de dados (necessária na maior parte dos sistemas atuais), e apresenta limitações ao nível da taxa de transferência destes(limitado aos 115,2 kbit/s).

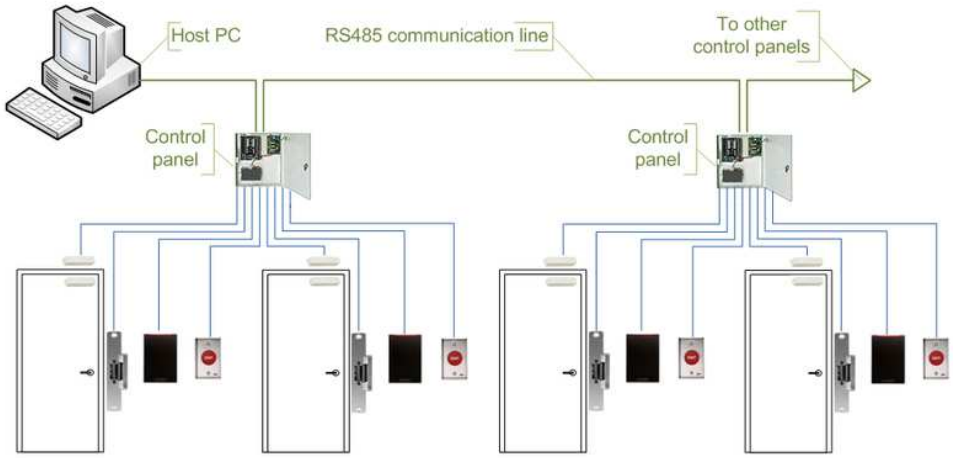



Figura 3.3: Topologia - *Host PC with Serial Controllers* em sistemas de controlo de acessos físicos [67]

- ***Host PC with a Serial Main Controller and Sub-Controllers***

  Todo o *hardware* associado ao ponto de acesso (e.g. porta) está ligado aos painéis de controlo associado a cada um. Nesta topologia cada acesso tem um painel de controlo independente (como no caso anterior), com a distinção que estes não comunicam diretamente com o o *host PC*, mas com um painel de controlo principal que tem essa finalidade. Podem existir vários deste tipo, onde estão ligados um conjunto de nós de acesso. Os painéis principais suportam entre 16-32 painéis, respetivos aos acessos, a eles ligados. Todos os pedidos junto aos pontos de acessos são reencaminhados pelos primeiros painéis para os principais, e posteriormente a ordem é devolvida e o comando processado.[68] A imagem 3.4 representa este tipo de arquitetura.

- Vantagens:
  - A carga de processamento ao nível do *host PC* é reduzida, pois só têm de comunicar com os painéis de controlo principais;
  - O custo geral dos sistemas é menor, sendo que a complexidade dos painéis primários é diminuta.
- Desvantagens:
  - A operação dos sistemas é fortemente dependente dos painéis de controlo principais. Caso um avarie, todos os *requests* associados aos eventos de todos os sub-painéis deixam de obter resposta, ou seja, na pior circunstância 32 pontos de acesso deixam de estar funcionais;
  - Os painéis de controlo principais tendem a ser caros, embora estes sistemas tendam a não ser aplicados em implantações de poucos acessos, pelo que, a relevância desta aspeto não é crítica.

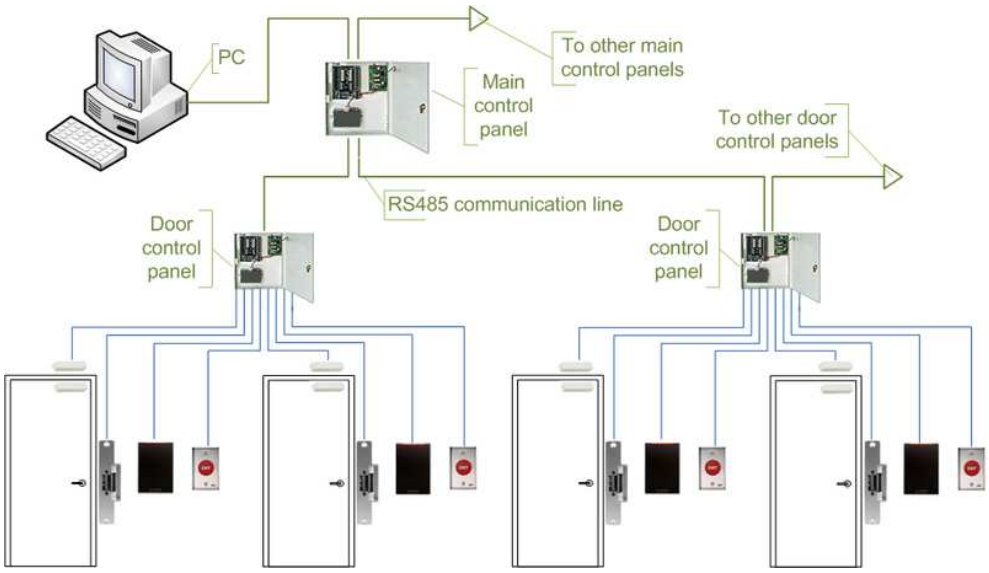



Figura 3.4: Topologia - *Host PC with a Serial Main Controller and Sub-Controllers* em sistemas de controlo de acessos físicos [67]

- ***Host PC with Serial Controllers and Intelligent Card Readers***

  Todo o *hardware* da porta está ligado diretamente a leitores semi-inteligentes ou inteligentes. Estes não costumam tomar decisões de acesso, e por isso reencaminham todas as solicitações para o painel de controlo principal. Se a conexão entre este e o leitor não estiver disponível, os últimos podem utilizar a sua memória e capacidade de processamento, para validar e processar os requisitos sobre o sistema. Caso se trate de leitores semi-inteligentes, não dotado de memória e unidade de processamento, estes devem ser apenas aplicados em acessos com requisitos de segurança mais baixos.[68] A imagem 3.5 representa este tipo de arquitetura.

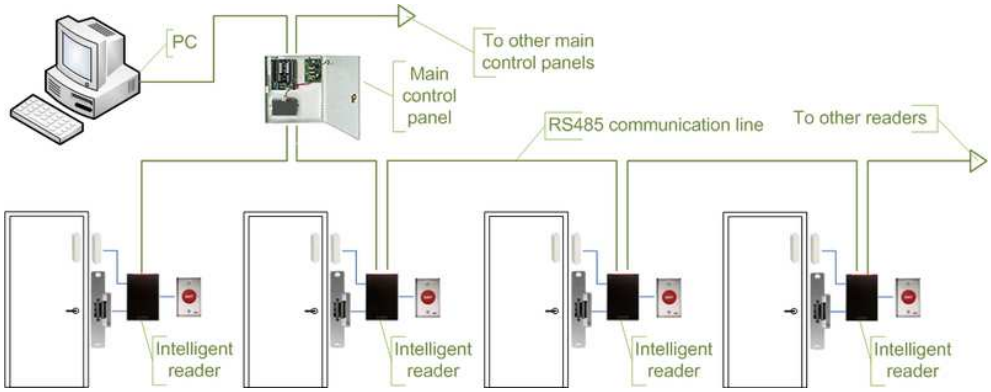



Figura 3.5: Topologia - *Host PC with Serial Controllers and Intelligent Card Readers* em sistemas de controlo de acessos físicos [67]

- ***Host PC Network with a Terminal Server and Serial Controllers***

  Apesar do rápido desenvolvimento e aumento do uso de redes de computadores, os fabricantes de soluções de controlo de acessos continuaram reticentes na aplicação destes sistemas, e não começaram a investir imediatamente nesta solução complementar. Quando requisitados para tal, optaram por simplesmente adicionar um servidor terminal, com o único intuito de converter os dados série/(*serial data*) para transmissão via *Local Area Network* (LAN) ou *Wide Area Network* (WAN). Isto é feito recorrendo à utilização de um *hub* ou *switch*, onde são ligados estes servidores terminais. Os servidores fabricados pela *Lantronix*® e da *Tibbo Technology*® são os mais populares na indústria de segurança.[68] A imagem 3.6 constitui alguns exemplos de aplicação destes terminais, nomeadamente aplicado nos tipos atrás descritos.

  - Vantagens:

    * Permite utilizar infraestruturas de rede existentes para conectar diferentes segmentos do sistema;
    * Providencia uma solução conveniente em casos em que a instalação de uma linha RS-485 é difícil ou impossível.

  - Desvantagens:

    * Aumenta a complexidade do sistema;
    * Aumenta o trabalho de instalação dos operadores: normalmente estes terminais têm de ser configurados independentemente, não através da interface do *software* de controlo de acessos físico.

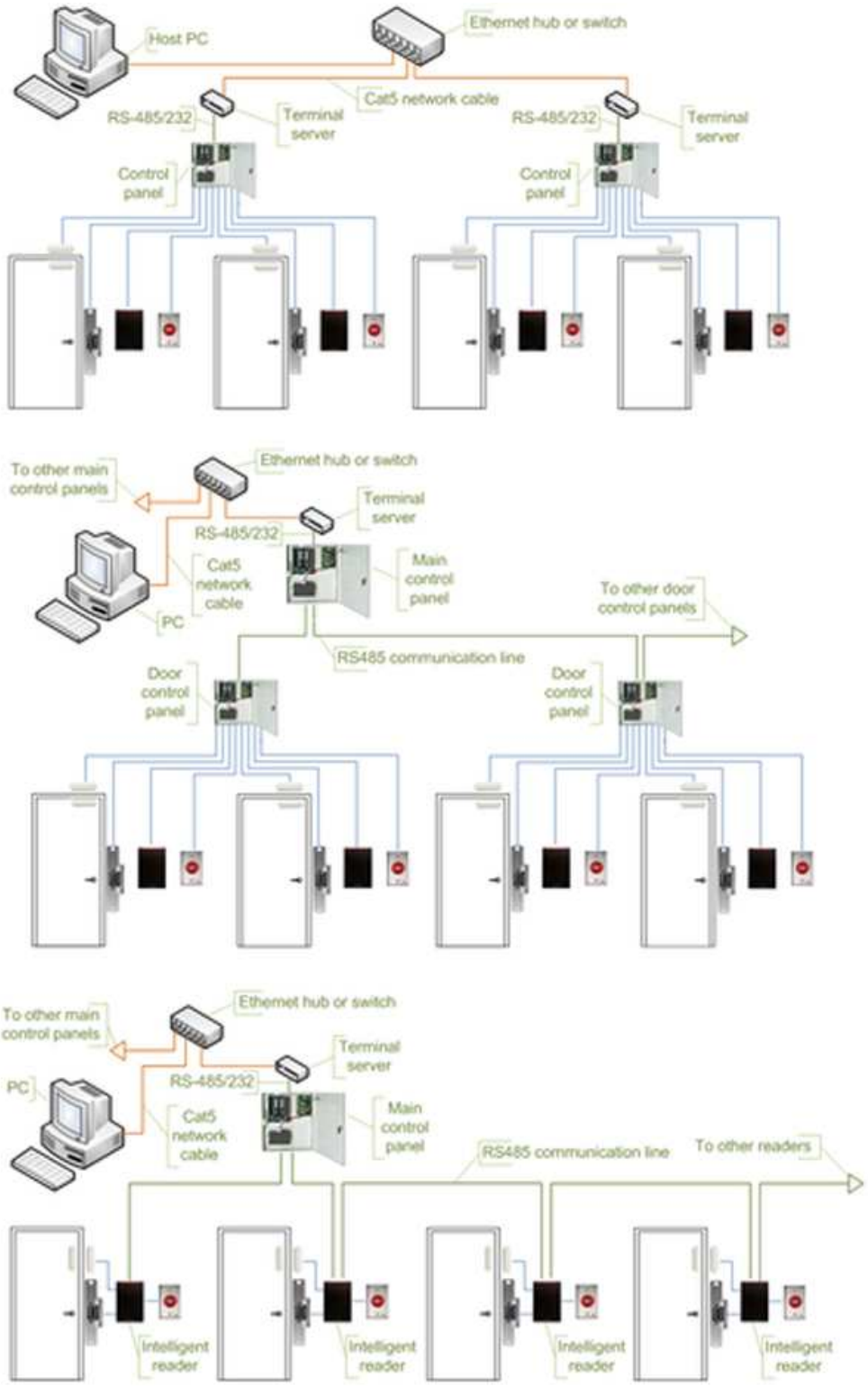



Figura 3.6: Topologia - *Host PC Network with a Terminal Server and Serial Controllers* em sistemas de controlo de acessos físicos [67]

- ***Host PC Network with Network-Enabled Serial Controllers***

  Estes sistemas baseiam o seu funcionamento no uso de uma interface de rede *on-board*. A transmissão de dados para configurações, e operações associadas aos utilizadores para os controladores principais é mais rápida, e pode ser feita em paralelo. Isto faz com que o sistema seja mais rápido a responder, não interrompendo funções normais de funcionamento. Não é necessário nenhum *hardware* em específico para obter a configuração "*redundant host* PC": No caso do primeiro falhar(*host* PC), um secundário pode começar a processar os eventos necessários ao bom funcionamento do sistema. Desvantagens associadas à utilização de servidores terminais, deixam também de existir.[68] A imagem 3.7 representa este tipo de arquitetura.

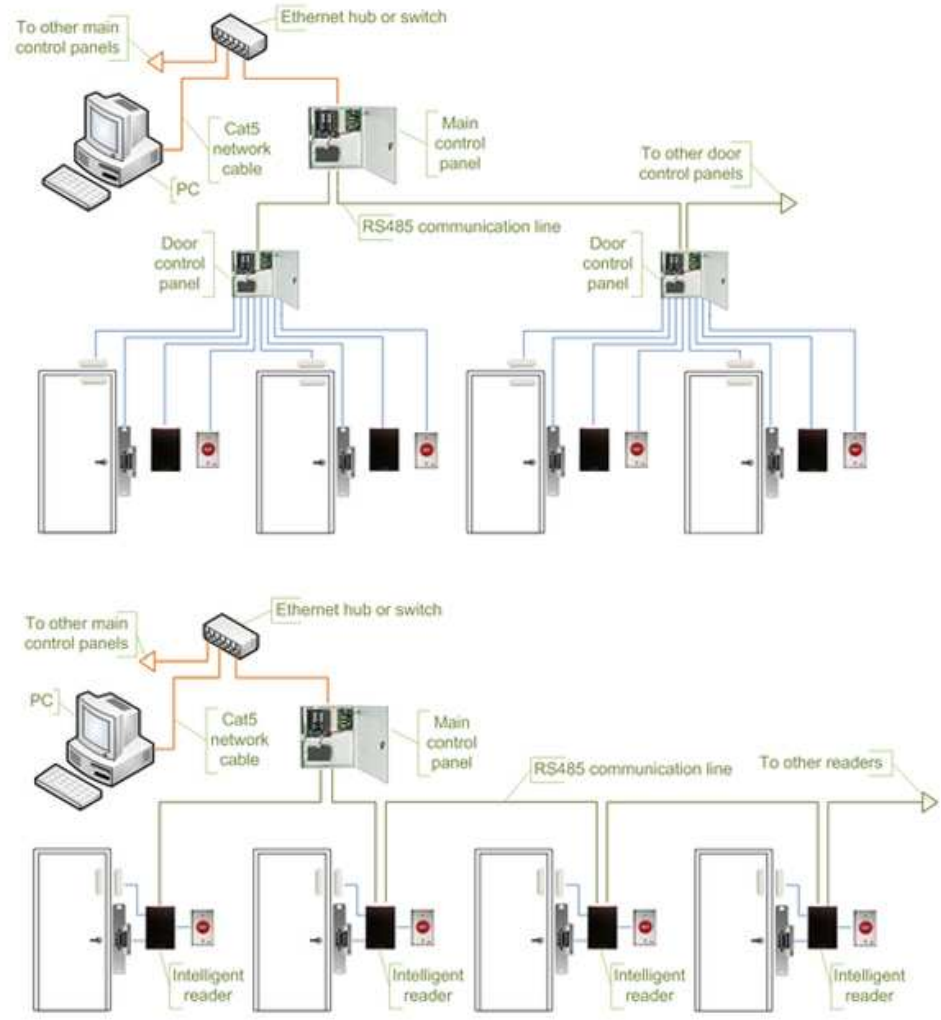



Figura 3.7: Topologia - *Host PC Network with Network-Enabled Serial Controllers* em sistemas de controlo de acessos físicos [67]

- ***Host PC Network with IP Controllers and/or IP Readers***

  Esta topologia apresenta a mesma arquitetura típica dos outros principais siste-

mas, com a diferença de que recorre ao protocolo *IP* para a transmissão de dados para o *host* PC. Existem três possibilidades de implementação. Uma recorrendo unicamente ao uso de controladores IP que gerem um conjunto finito de nós de acesso, ligados estes numa rede *Ethernet*, através de um *hub* ou *switch*, que depois comunica com o computador remoto. Outra possibilidade é os próprios leitores estarem preparados para implementar o protocolo IP e não haver necessidade da existência de controladores intermédios.[68] Ainda existem soluções que preveem um misto das soluções. Nas imagens 3.8 e na 3.9 estão representados os dois tipos.

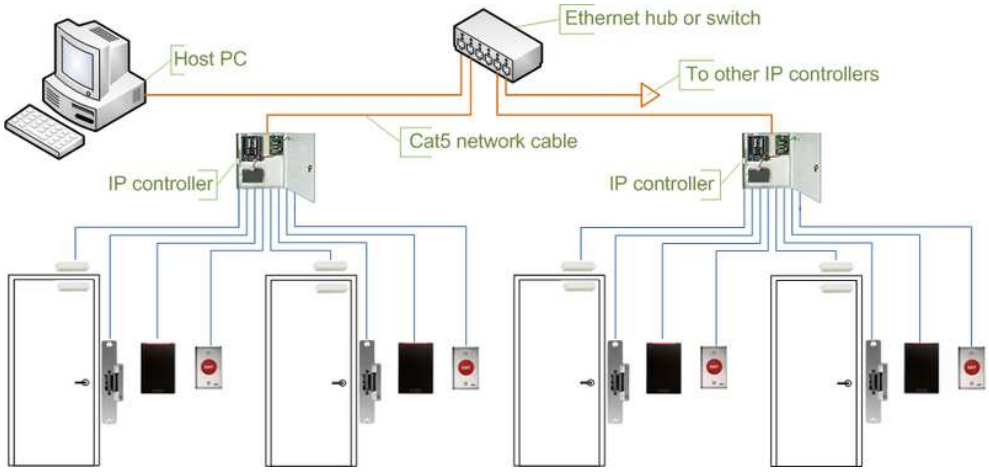



Figura 3.8: Topologia - *Host PC Network with IP Controllers* em sistemas de controlo de acessos físicos [67]

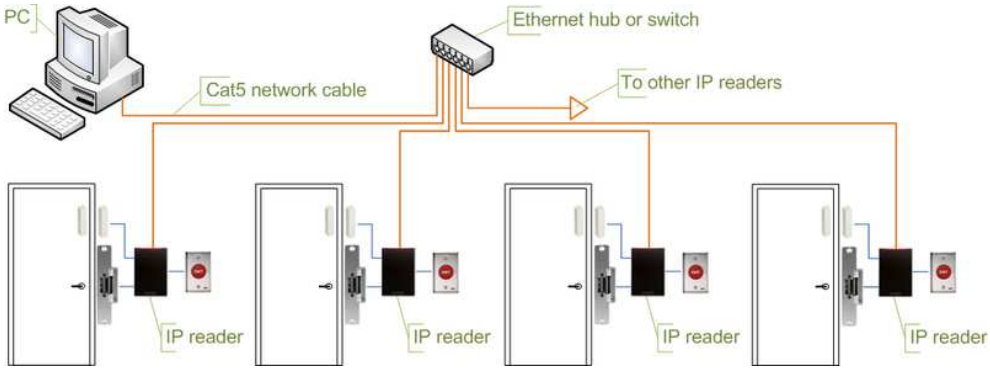



Figura 3.9: Topologia - *Host PC Network with IP Readers* em sistemas de controlo de acessos físicos [67]

## 3.5 Riscos de Segurança

Nesta secção aborda-se os riscos de segurança associados a sistemas de controlo de acessos físicos, numa perspetiva de compreender que preocupações se devem ter no desenvolvimento e instalação destas soluções. Na literatura alguns dos riscos a seguir apresentados, surgem dentro de classes. Tipicamente denominam-se "Ameaças externas", "Ameaças

internas", e "Ameaças humanas". As duas primeiras estão normalmente associadas a falhas provocadas por comportamentos/ações não intencionadas, quer seja por razões naturais, ou por falhas induzidas por outros sistemas na implantação que afetam diretamente os sistemas de controlo de acessos; enquanto os tópicos relativos à última classe, estão normalmente associada a comportamentos mal intencionados(com intuito de furto ou divulgação de dados confidenciais), ou devido a falha humana, quer seja, em erros ou *bugs* das aplicações de gestão dos sistemas, ou em atos de manutenção (e semelhantes), comprometendo o normal funcionamento do sistema.

Genericamente, as ameaças externas, contemplam fenómenos como tornados, cheias, trovoadas fortes, tremores de terra, fogo, gelo e frio extremo, ou seja, riscos principalmente associados a comportamentos da natureza, que afetam as partes físicas dos sistemas, ou as redes que os energizam. As ameaças internas devem-se a fatores internos ao edifício onde está instalado o sistema, seja fogo, fuga de líquidos de tubagens, falha elétrica, ou outro. Os riscos ou ameaças humanas estão relacionados com comportamentos de vandalismo, roubo intencionado, sabotagem, espionagem, ou erros.[69]

Riscos de segurança mais específicos em sistemas de controlo de acessos físicos incluem:

- **Divulgação Intencional/Acidental de Informação**

  Este é um dos maiores riscos em sistemas de controlo de acessos, quer seja físico ou não, pois o conceito é facilmente aplicável nas duas perspetivas. Deve-se essencialmente ao fato dos utilizadores não compreenderem o que está inerente às preocupações que levaram a implementar um dados sistema deste tipo. Este risco também está muito associado à psicologia humana, de conceptualizar níveis de importância/segurança a um dado objeto/informação, limitadas à compreensão e às perspetivas do "eu". Por isto, é flagrante acontecer situações em que um funcionário com um dado papel/*role* numa corporação, trespasse informação verbalmente a outro colega com um papel diferente, que de forma racional pelos administradores, não lhe conferiram tal direito, quer seja por razões de política interna, ou outra. Relativamente à divulgação intencional, não existe solução de resolução ao nível do sistema ou do grupo que a implementa. Ainda quanto à divulgação acidental, torna-se necessário um constante alerta (ao nível do *software*, ou pessoalmente) aos utilizadores, e constantes auditorias.[70]

- **Modificações Não Autorizadas**

  Alguns modelos de controlo de acessos mais simplistas, principalmente ao nível de acessos físicos, a dificuldade de prover o conhecimento sobre os utilizadores de que dado objeto associado ao acesso não deve ter o seu estado modificado, é complicado. Deve-se portanto, auditar constantemente o registo de acessos e estados dos objetos, tal como prover pelos meios necessários, os utilizadores, das pretensões da companhia/instituição/corporação, do estado do objeto, ou sobre que formas os utilizadores podem agir sobre ele.[70]

- **Acessos Não Autorizados**

  Este pode ser feito sobre diferentes formas, algumas delas referidas adiante. Este risco é referenciado de uma forma muito generalista, pretendendo neste ponto alertar para os atos pós primeiro acesso não autorizado, para continuação destes de

forma oculta. A alocação de *malware* nos sistemas, furto de serviços e formas de atuar dos sistemas para posterior *hack*, são alguns dos risco associados a uma primeira forma de acesso não autorizado.

- ***Password Sniffing***

  Forma de *hack* que transforma o modo visual encriptado de texto (típico quando inserimos uma *password* em qualquer *software*), em modo deste simples.[70]

- ***Password Cracking***

  Senhas de acessos/*Passwords* que não seguem regras de complexidade comuns, sendo consequentemente fáceis de *hackear* recorrendo ao uso de informação básica do utilizador.[70]

- ***Hosts* Vulneráveis**

  Em sistemas de controlos de acessos, com topologias de rede, o risco é crescente com o número de *host* PCs na rede, bastando um destes apresentar vulnerabilidades ao nível de segurança, para a totalidade do sistema ficar comprometida a diversos níveis.

- **Engenharia Social/*Social Engineering***

  Este conceito está relacionado com a importância de formação dos utilizadores relativamente ao funcionamento do sistema de controlo de acessos. Quando estes não devidamente esclarecidos, as suas credenciais podem ser facilmente subtraídas fraudulentamente, por exemplo, recorrendo ao uso de formulários falsos que requisitam as credenciais dos utilizadores (esquema fortemente aplicável recorrendo a *e-mails*).[70]

- **Acesso de Terceiros**

  É importantíssimo prover os sistemas de segurança de mecanismos que invalidem o acesso de indivíduos terceiros a estes. Embora os principais modelos impliquem fiáveis mecanismos de identificação e autenticação, existe sempre um risco associado, quanto mais não seja, o simples exemplo, de acesso a um computador já previamente autenticado.[70]

- ***Tailgating***

  É uma das formas mais simples e comuns de aceder a um acesso sem autorização. Consiste em seguir um utilizador legítimo quando este entra num acesso, com ou sem cooperação deste. O risco é minimizado com a devida formação dos utilizadores, e também recorrendo a outras soluções que não simples portas, como torniquetes; e/ou utilizando operadores/seguranças/porteiros que impeçam este comportamento.

- ***Levering***

  Consiste em utilizar um objeto, normalmente de dimensões ínfimas, por exemplo, um parafuso, entre a porta e a armação exterior desta, para que a primeira não se feche. A maioria dos sistemas são providos de mecanismos de alarme caso, alguns segundos depois ao acesso ter sido provido, o trinco da porta ainda não

esteja fechado. Estes mecanismos rapidamente notificam os administradores ou seguranças da implantação do sucedido. Câmaras de filmar e outros dispositivos extra são passíveis de prover a identificação destes métodos ilícitos, mas nenhum deles, 100% infalível.

- ***Lock Spoofing***

  Bastante mais elegante e subtil do que o método anterior, baseia-se no uso de um íman forte o suficiente para atuar sobre a bobina de fechaduras elétricas ativadas por recurso a linguete ou a motores (*Direct Current* (DC)) específicos.

- ***Lock/Wall Bumping***

  Algumas das soluções para fechaduras elétricas são frágeis o suficiente para que o recurso a força, seja o bastante para fazer abrir o acesso. O mesmo se passa com paredes divisórias presentes em algumas das implantações onde estes sistemas são aplicados, e que da mesma forma são facilmente ultrapassáveis.

- ***Hack* de Cartões de Acesso**

  Algumas soluções *smart cards* ou *tags* RFID são alvo de sofisticados ataques, através da utilização de leitores que conseguem captar os dados transmissíveis por RF, ou eles próprios interagirem com estes, de forma a obterem dados, como o número de identificação (*Identity* (ID)) dos cartões, ou outros.

## 3.6 Protocolos de Comunicação de Suporte

Esta secção pretende dar a conhecer ao leitor algumas soluções ao nível de protocolos de comunicação contemplados na maioria dos sistemas de controlo de acessos conhecidos, ou implementáveis pelas suas características. Especificam-se as principais normas aplicáveis, sendo que, a variedade destes protocolos é de número relevante, e na perspetiva desta dissertação não tem valor acrescentado, referir a sua totalidade. É ainda feito referência a uma solução sem fios, não tão fortemente aplicada, mas na perspetiva do autor, uma das pouco soluções *wireless* capaz de inovar e acrescentar valor a sistemas deste tipo - *ZigBee*.

### 3.6.1 Protocolos de Comunicação Industrial

Neste ponto faz-se referência aos principais protocolos aplicados entre dispositivos industriais. Embora o seu uso se tenha vindo a tornar cada vez mais obsoleto, continuam a coexistir na indústria, com os equipamentos fortemente suportados por estes, continuando também os mesmos, a apresentar uma robustez suficiente ao nível da sua aplicabilidade em novos produtos. Os três primeiros referidos, especificam em pormenor um conjunto de regras e metodologias focadas no meio físico de comunicação, sinais elétricos, fichas aplicáveis, formato genérico da "palavra série", mecanismos previstos de controlo de fluxo (de dados), etc. O último especificado nesta secção, apresenta uma proposta protocolar focada na estrutura de mensagem de dados, e não na topologia física do meio de comunicação, nem nenhum aspeto relativo ao mesmo.

#### 3.6.1.1 RS232-422

Este é um dos protocolos mais implementados em equipamentos industriais, embora tenha vindo a sofrer um séria diminuição ao nível da sua aplicabilidade, associada à crescente utilização da tecnologia USB e *Fire Wire*.[71]

Trata-se de uma comunicação assíncrona, pois não recorre à utilização de um relógio que defina a sua frequência de amostragem, como por exemplo a comunicação I2C, pelo que o sincronismo entre dispositivos interligados segundo este protocolo deve estar devidamente acertado. As taxas de transferência de dados, denominada *baudrate*, toma diferentes valores, entre o valor mínimo de 9600*bits per second* (bps) e o máximo, 115200bps. Limita a interligação entre dispositivos, até dois (comunicação *node-to-node*, especificada em *Electronics Industry Association (EIA) RS-232*), embora possibilite a transmissão de dados simultaneamente entre estes (comunicação *full duplex*). Para o normal funcionamento da comunicação basta efetuar a ligação entre 3 pinos, ou seja, três condutores (um para a transmissão de dados - *TX*; outro para a receção de dados - *RX*; e o *ground*). O conetor *DB-9*(ver imagem 3.10) é o mais utilizado para assegurar este tipo de comunicação, e é provido obviamente de mais pinos, e consequentemente mais funções associadas a estes, tal como controlo de fluxo por *hardware*. A tabela 3.1 contém a descrição dos pinos de um conector DB-9.

A interligação deve ser feita de forma cruzada nos condutores de dados, para que o pino de envio de um, esteja ligado ao pino de receção do outro, e vice-versa. É uma comunicação unipolar, pelo que tende a ser ligeiramente afetada pelo ruído elétrico, e consequentemente o comprimento da cablagem de ligação, tem como limite um valor aproximado aos 15 metros, muito embora, este valor seja afetado por alguns fatores, tais como, o *baudrate* utilizado, e outros. Por esta razão, e por ser uma comunicação do tipo *node-to-node*, o RS-232 não é solução presente nas topologias atrás apresentadas, ou seja, não serve como interface de comunicação entre os diversos pontos de acesso e os painéis de controlo, ou qualquer outro modulo principal, numa topologia de rede. Isto não invalida que seja aplicado como protocolo de comunicação entre elementos constituintes de partes principais do sistema global (e.g. interface de comunicação entre um microcontrolador e um *chip* NFC, num leitor de identificação/autenticação).[71; 79; 73]

Algumas evoluções da norma *EIA-232* pressupõem novas especificações, onde é por exemplo, designado como novo modo de comunicação, o modo síncrono (em *EIA-232D*). Foram especificadas mais características na perspetiva de flexibilizar a tecnologia, ao longo da revisão do protocolo, designando por exemplo, novas fichas, como a *DB-25* e a *RJ-45*.[73]

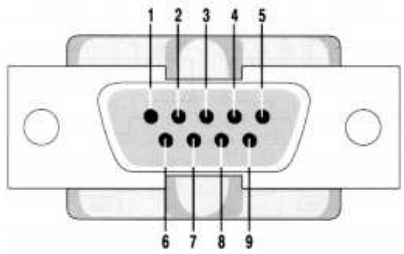



Figura 3.10: Conector DB-9 [74]

Tabela 3.1: *Pin-out* do Conector DB-9 [71]

| Pino | Descrição |
|---|---|
| 1 | Deteção de dados a enviar (CD) |
| 2 | Receção de dados (RX) |
| 3 | Transmissão de dados (TX) |
| 4 | Terminal de dados pronto (DTR) |
| 5 | Massa/Terra/Comum (GND) |
| 6 | Dados prontos a enviar (DSR) |
| 7 | Pedido de Transmissão (RTS) |
| 8 | Resposta ao pedido de transmissão (CTS) |
| 9 | Indicador de telefone (RI) |

O protocolo RS-422 (*Telecommunications Industry Association* (TIA)/EIA-422) apresenta menores níveis de ruído, por ser um modo de comunicação diferencial, o que permite ligar o dispositivo *master* a diversos dispositivos *slave* (limitado a 10) , e pela primeira razão, aumentar o comprimento da cablagem de ligação entre estes, até aproximadamente 1200 metros. Outra característica relevante, é a capacidade deste protocolo permitir taxas de transferência de dados até 10 *Megabits*/segundo (Mbit/s), embora em sistemas de controlo de acessos físicos este aspeto não seja essencial. Posto isto, a aplicabilidade deste passa pela possibilidade de o implementar para fins de interligação de dispositivos quer seja por barramento, ou outra topologia de rede alternativa.[79; 71; 75]

#### 3.6.1.2 RS-485

*Nota: O conteúdo desta secção tem como fonte quase integral a referência em [76]. Todo o conteúdo que não lhe diz respeito, é normalmente referenciado.*

Este protocolo define as características físicas de uma ligação entre dispositivos (previsto na camada 1 do modelo OSI). Este protocolo permite ainda o envio de palavras série entre os equipamentos, com uma estrutura similar ao protocolo RS-232, com um *Start bit*, vários *bits* de dados (7,6,8), um *bit* de paridade e *stop bits*(1,1.5,2). Dependendo da resistência interna dos dispositivos/equipamentos ligados em rede, o protocolo previa a interligação de até 32 destes com 12 kΩ de resistência interna, e atualmente 256 com uma resistência interna de 96 kΩ. Tal como o protocolo RS-422, este apresenta uma grande imunidade ao ruído eletromagnético (utilização do modo de comunicação diferencial), e por isso conectar dispositivos distanciados até 1200 metros. Um valor médio, apontado para a taxa de transferência de dados é 10 Mbit/s, embora para menores distâncias de ligação seja possível transmitir até aos 50 Mbit/s.[75; 76]

- **Meio de Comunicação**

  O meio físico de comunicação entre equipamentos não é especificado pelo protocolo, embora geralmente sejam aplicados condutores de cobre, entrançados, como o cabo 24-*American Wire Gauge* (AWG). É neste aspeto onde reside a principal diferença, relativamente ao protocolo RS-232. Enquanto neste último é apenas utilizado um condutor para envio, e outro para receção de dados, este preconiza, a aplicação de um par condutor para enviar dados e outro par para a receção. Existe uma clara vantagem associada a este método que reside no fato do equipamento recetor medir o diferencial de tensão do sinal recebido, entre dois condutores do equipamento de

envio (tensão diferencial), ao invés de medir o diferencial de tensão entre a sua terra e o condutor que liga ao emissor. Pode ainda ser implementado um 5º condutor a ligar a terra entre os equipamentos interligados. Na Figura 3.11 uma pequena representação da ligação física, destes pares entrançados, numa topologia *node-to-node*, com amplificadores operacionais.

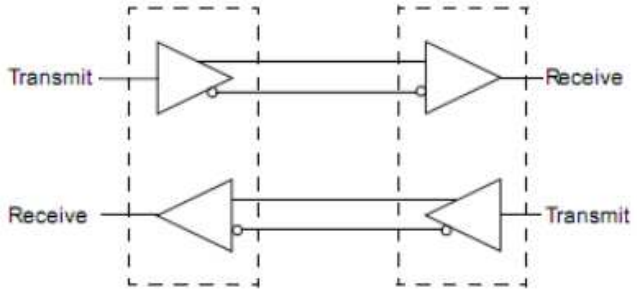



Figura 3.11: Amplificador operacional - Transmissor, Recetor RS-485 [76]

- **Níveis de Tensão**

  Este protocolo especifica que os equipamentos devem induzir uma tensão negativa entre os condutores de envio de dados, para o reconhecimento de um *bit* a "1" pelos dispositivos recetores, e uma tensão positiva nas mesmas circunstâncias para o reconhecimento de um *bit* a "0", pelos mesmos. A resolução deste diferencial deve estar contida num intervalo entre +/- 1,5 *Volt* (V) e +/- 6V, para que respetivamente, sendo ambos positivos ou negativos, sejam interpretados como *bits* a "0" ou a "1".

  Ainda relacionado com este aspeto, deve-se evidenciar que este protocolo, por permitir a ligação de um número de equipamentos limitado, em rede, apresenta três estados de funcionamento (*Tri-state*), especificamente ao nível dos amplificadores diferenciais, ou seja, quando diferentes dispositivos interligados pelo mesmo par de condutores entrançados, os seus amplificadores operacionais de saída não podem aplicar em simultâneo tensões neste, e consequentemente, quando um dos amplificadores aplicar tensões positivas ou negativas, todos os outros devem apresentar um estado de alta impedância (atuando como se não estivessem eletricamente ligados a esse par condutor).

  Posto isto, os três estados são, o já referido estado de alta impedância, o estado de tensão diferencial positiva, e o estado de tensão diferencial negativa.

- **Topologia**

  Relativamente às topologias, a especificação aconselha o tipo *bus* (barramento), e recomenda a não aplicação, do tipo estrela, árvore ou mistas, embora possam funcionar.

  Das topologias baseadas em barramento, destacam-se dois modelos típicos:

  – **Barramento com um par de condutores**

Barramentos apenas com um par de condutores, consistem em equipamentos conectados, em que as linhas de dados para envio e receção são comuns. Isto implica que todos os dados enviados por um equipamento emissor são recebidos por todos os outros ligados ao barramento, e por si mesmo, o que consequentemente requer, que quando um dos dispositivos necessita de enviar dados, todos os outros devem estar à "escuta", pois caso contrário, diversos dispositivos aplicando tensões em simultâneo nos condutores, induziriam a um estado de sinais corrompidos e não interpretáveis por estes. Por esta razão, barramentos com um par de condutores - RS-485, designam-se sistemas de comunicação - *half-duplex*. Na Figura 3.12 um esquema de ligações representativo desta topologia.

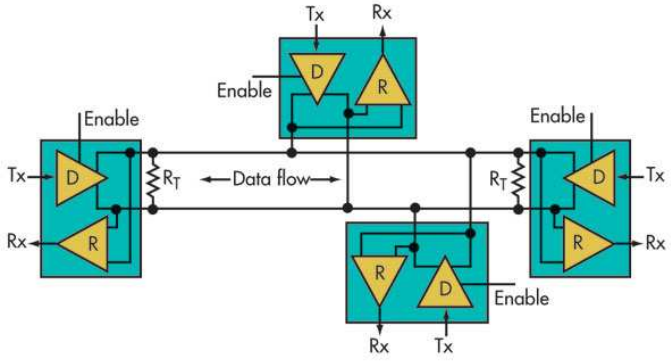



Figura 3.12: Barramento com um par de condutores - RS-485 [77]

– **Barramento com dois pares de condutores**
Nesta topologia já são aplicados dois pares de condutores, um para a receção de dados e outro para o envio, permitindo que um determinado equipamento consiga ser simultaneamente emissor e recetor, ou seja, funcionar em modo de comunicação *full-duplex*. Este equipamento é o designado *master* da comunicação, pois apenas ele pode enviar dados para todos os equipamentos ligados ao barramento, enquanto os outros, só conseguem enviar dados para o equipamento *master*, quando este consentir. Isto deve-se à necessidade de evitar a aplicação de várias tensões, por equipamentos *slave* distintos no condutor de receção de dados, que resultaria em sinais corrompidos. Na Figura 3.13 um esquema de ligações representativo desta topologia.

- **Controlo de Acesso ao Meio de Transmissão**

Quando vários equipamentos ligados por barramento, que partilham o mesmo meio de transmissão de dados, transmitem dados em simultâneo, como já evidenciado, os sinais são automaticamente corrompidos, e por isso, não interpretáveis. Posto isto, a necessidade de definir especificações para o controlo de acesso ao meio físico de transmissão, era expectável, mas não está previsto no protocolo RS-485. A falta deste mecanismo é colmatada por protocolos, como o "*Modbus*", que em conjunto com o RS-485, não só permite controlar o acesso ao meio de comunicação, como endereçar os vários equipamentos, e operar sobre as suas saídas analógicas e digitais (com mensagens de controlo para o efeito).

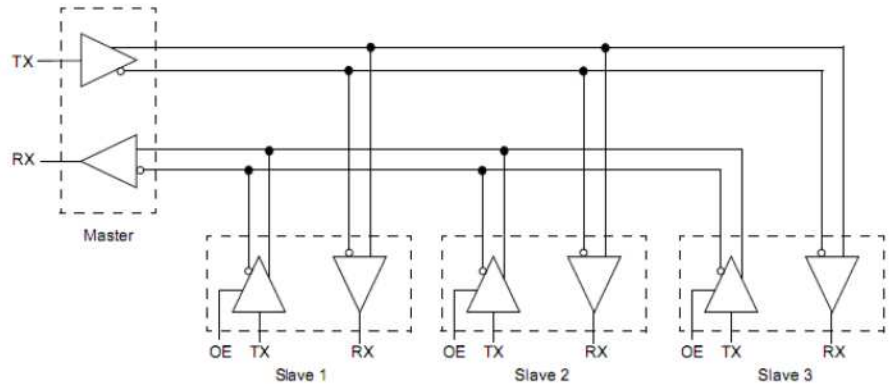



Figura 3.13: Barramento com dois pares de condutores - RS-485 [76]

#### 3.6.1.3 *Modbus*

*Nota: O conteúdo desta secção tem como fonte quase integral a referência em [78]. Todo o conteúdo que não lhe diz respeito, é normalmente referenciado.*

Como já referido, este protocolo, desenvolvido pela empresa Modicon®, baseia-se na definição da palavra série/trama trocada entre equipamentos, e foi pensado na perspetiva de definir uma linguagem global que permitisse a comunicação entre os seus autómatos. Mais tarde, todos os fabricantes puderam aplicar este conjunto de especificações livremente. A sequência de *bytes* definida por este protocolo não procura apenas normalizar uma estrutura de mensagem bem defina, mas além disso, através de campos específicos das mensagens, monitorizar e controlar, saídas e entradas dos equipamentos remotos. Portanto, especificações associadas ao tipo de ligações físicas entre equipamentos, sinais elétricos e outras normativas normalmente focadas na tecnologia e na sua forma de funcionamento ao nível de *hardware*, não são por este definidas. Diz- se por isto, que o *Modbus* é um protocolo implementado por *software* (quando se programa os equipamentos), e por *firmware* quando se refere o fato dos equipamentos serem capazes de interpretá-lo, ou seja, por virem programados de fábrica para tal.

Sendo um protocolo definido com o intuito de definir a mensagem trocada entre equipamentos, onde estas deverão ser interpretáveis por estes, o único requisito é que os fabricantes preparem os mesmos para tal. Por isso, redes compostas por equipamentos que implementem o RS-232/422/485, Ethernet, ou outro protocolo de comunicação deste tipo, poderão simultaneamente implementar o *Modbus* como robusto suporte, pois além deste definir um conjunto de *bytes* de instruções bastante úteis para o desenvolvimento e implementação da comunicação entre os equipamentos, ele ainda define, por exemplo, que dispositivo pode enviar dados e em que altura, um modo de endereçamento, entre outras funcionalidades.

- **Tipo de Diálogo/Partilha do Meio de Transmissão**

  O protocolo *Modbus* é normalmente referenciado na literatura como um modo de comunicação *Master-Slave*, no entanto, é possível que o modelo seja do tipo Cliente-Servidor, no caso do meio físico se tratar do protocolo *Ethernet*, denominando-se nestes casos de *Modbus TCP*. No caso das comunicações série comuns RS-232/485,

topologias de rede mais aplicadas, denominam-se como já referido, como modo *Master-Slave*. Por o *Modbus TCP* se tratar duma solução atípica serão apenas descritos os dois modos de transmissão de mensagens mais comuns: *Modbus ASCII* e *Modbus RTU*.[71]

O modo *Master-Slave*, ao contrário de outros protocolos que permitem a cada equipamento enviar os seus dados para o meio de comunicação sempre que desejarem, podendo ocorrer colisões de dados no processo (caso sejam enviados dados em simultâneo por dois ou mais equipamentos), prevê mecanismos para o evitar.

O *master* pode enviar mensagens no modo *unicast*, ou no modo *broadcast*, ou seja, respetivamente, enviar uma mensagem endereçada apenas a um equipamento, ou a todos conectados ao barramento. Algumas destas mensagens pressupõem resposta do *slave*, tipicamente mensagens de "leitura", onde os dispositivos *slave* deverão nestas circunstâncias processar os pedidos do *master* e devolver a informação requisitada. Por outro lado, se a mensagem for do tipo "escrita", estas não necessitam de resposta, devendo apenas o recetor processar o comando, tipicamente uma atualização de parâmetros ou atuação sobre um saída digital ou analógica.

- **Estrutura de Mensagem**

  A estrutura de mensagem base, para qualquer um dos tipos mais à frente apresentados, é a apresentada na Tabela 3.2. A sequência dos *bytes* na mensagem equivale à definida na tabela referida. Na Tabela 3.3 é possível consultar alguns códigos das funções aplicáveis pelo protocolo, e interpretáveis pelos equipamentos recetores.

Tabela 3.2: Elementos da estrutura de mensagem *Modbus*

| Posição | **Nome** | **Tamanho de Dados** | **Descrição** |
|---|---|---|---|
| 1º Campo | Endereço | 1 *byte* | Endereço do equipamento de destino codificado em 8 *bits*. Se designado o valor "0" a mensagem é do tipo *broadcast*. |
| 2º Campo | Função | 1 *byte* | Existem 4 tipos de classes de funções: Leitura de entradas digitais; Controlo de Saídas Digitais; Leitura de Posições de Memória só de Leitura; Leitura ou Escrita de Posições de Memória. |
| 3º Campo | Dados | 0 a 252 *bytes* | Posições da palavra série destinas a dados necessários à mensagem, como por exemplo, o valor a escrever numa posição de memória. |
| 4º Campo | *Cycling Redundancy Check* (CRC)/*Longitudinal Redundancy Check* (LRC) | 2 *bytes* | Valores gerados algoriticamente implementáveis para validação do conteúdo da mensagem pelo recetor. |

  - **Tipo RTU**

    As mensagens *Modbus* podem ser de dois tipos: RTU ou ASCII. No primeiro, cada *byte* da mensagem (o *byte* de endereço, função, dados e *bytes* de confirmação) são codificados em 8 *bits*, e são normalmente transmitidos numa

Tabela 3.3: Alguns códigos de funções *Modbus*

| **Código da Função** | | | |
|---|---|---|---|
| **Decimal** | **Hexadecimal** | **Binário** | |
| 1 | 1 | 00000001 | Leitura do estado das saídas digitais do equipamento remoto (*on/off*) |
| 2 | 2 | 00000010 | Leitura de entradas digitais do equipamento remoto (*on/off*) |
| 3 | 3 | 00000011 | Leitura de posições de memória do equipamento remoto 2 *bytes* |
| ... | ... | ... | ... |
| 15 | 0F | 00001111 | Ativa/Desativa um conjunto de saídas digitais consecutivas |
| 16 | 10 | 00010000 | Escreve em várias posições de memória |
| ... | ... | ... | ... |

palavra série RS-232/485. Para cada *byte* enviado o protocolo pressupõe, também o envio de 3 *bits* adicionais: *start bit* (primeiro a ser enviado), *bit* de paridade (a seguir ao valor enviado que procede o *start bit*), e um *stop bit* no final. No contexto de mensagens *Modbus RTU* os dois bytes codificados para confirmação da fiabilidade da mensagem, são calculados através do algoritmo CRC16. Como referido atrás, a confirmação é feita quando o recetor recebe a palavra série, isola os 16 *bits* gerados pelo algoritmo, recalcula o valor deste com base nos bytes recebidos, e finalmente verifica o *match* entre os 2 *bytes* previamente isolados, e os re-calculados por ele. Na Tabela 3.2, e na Tabela 3.3 pode-se consultar respetivamente, a estrutura da mensagem *Modbus RTU*, e a posição dos *bits* auxiliares enviados com cada *byte* da mensagem, previstos no protocolo (a leitura da tabela deve ser feita da esquerda para a direita).

Tabela 3.4: Estrutura da mensagem *Modbus RTU*

| **Endereço (1*byte*)** | **Função (1*byte*)** | **Dados de Comprimento Variável (0 a 252*bytes*)** | **Algoritmo Confirmação (2*bytes*)** |
|---|---|---|---|
| 0x12 | 0x15 | Dados | CRC |

Tabela 3.5: Posição de *bits* adicionais, associados a cada byte da mensagem *Modbus RTU*

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Start bit | 01001000 (0x12) | Parity Bit | Stop Bit | | Start bit | 10101000 (0x15) | Parity Bit | Stop Bit | ... |

– **Tipo ASCII**

Como verificado no modo anterior, este contém um número, por exemplo o endereço de destino 12, ou o código da função com o valor 15. Como tal, cada um destes tem, ou pode ter, um valor inteiro capaz de ser codificado num *byte*. Posto isto, é mais fácil definir o *Modbus* ASCII, comparado-os com os pressupostos anterior. Para a mesma mensagem anterior, transformando-a neste tipo, os passos seriam:

∗ **1º Passo**
Dividir o número contido em cada *byte*, pelos algarismos, e convertê-los para os caracteres respetivos da tabela ASCII, codificando-os cada um em

7 *bits*. Em específico, para o exemplo dado, o dígito "1" corresponderia ao binário 0110001, o "2" a 0110010, e o "5" a 0110101. Além disso as mensagens *Modbus* ASCII iniciam-se sempre com o caracter ":", e terminam com o caracteres "CR" (*Carriage Return*) e "LF" (Line Feed). A Figura 3.14 pretende clarificar a estrutura adotada para a transmissão de dados neste tipo.

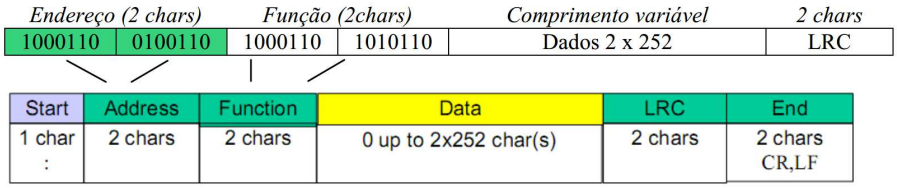



Figura 3.14: Representação da estrutura de mensagem *Modbus ASCII* [76]

* **2º Passo**
  Da mesma forma que no modo *Modbus* RTU existe a necessidade de se agregar os 3 *bits* complementares, por cada *byte* pertencente à trama da mensagem ASCII o mesmo é necessário(tratam-se dos mesmos já referidos para o caso anterior). A diferença prende-se ao fato que por cada *byte* auxiliar da mensagem ASCII, os caracteres de inicio e fim de mensagem, deverão também ser contemplados com os *bits* auxiliares. A Tabela 3.6 pretende representar esta estrutura, e também a sequência de envio, desde o *bit* menos significativo (*start bit*), com os que dados que o procedem, respetivamente, da esquerda para a direita de acordo com a tabela. O algoritmo de verificação aplicado nesta estrutura de mensagem é o LRC, que calcula os *bytes* de confirmação com uma metodologia distinta do CRC16, embora o objetivo seja o mesmo, tal como o processo de validação da mensagem pelo recetor.

Tabela 3.6: Posição de *bits* adicionais, associados a cada byte da mensagem *Modbus RTU*

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Start bit | 0101110 *Char*(:) | Parity Bit | Stop Bit | Start bit | 1000110 *Char*(1) | Parity Bit | Stop Bit | ... |

### 3.6.2 *Ethernet*

*Nota: O conteúdo desta sub-secção tem como fonte integral a referência em [79].*

A *Ethernet* é uma arquitetura de interconexão para redes locais (LAN), definidas pela IEEE *802.3*. Esta norma pressupõem dois modos de operação: *full-duplex* e *half-duplex*. No segundo, os dados são transmitidos utilizando o popular *Carrier-Sense Multiple Access* (CSMA)/*Collision Detection* (CD), que baseio o seu mecanismo, na gestão da rede de partilha, de forma a evitar/detetar colisões de dados, ou seja, o mecanismo verifica o estado da rede, verificando se esta está a ser utilizada, evitando transferência de dados em simultâneo, na mesma rede *Ethernet*. As suas principais desvantagens devem-se à fraca eficácia do modo de operação, e a limitação da distância entre equipamentos da

rede. Estas desvantagens relacionam-se com o *minimum frame size* da camada *Medium Access and Control* (MAC), induzindo por isso também, a ineficiência da comunicação em altas taxas de transferência de dados.

A norma prevê quatro especificações diferentes, distinguidas pelas taxas de transferência aplicadas, através de cabos de fibra ótica ou de cobre (de pares entrançados):

- *10 Mbit/s - 10Base-T Ethernet* (IEEE *802.3*)
- *100 Mbit/s - Fast Ethernet (IEEE 802.3u)*
- *1000 Mbit/s - Gigabit Ethernet (IEEE 802.3z)*
- *10-Gigabit - 10 Gigabits/segundo (Gbit/s) Ethernet (IEEE 802.3ae)*

Existem três elementos base que compõem um sistema *Ethernet*, sendo estes, o meio físico utilizado para transportar sinais *Ethernet* entre os diferentes dispositivos; um conjunto de regras padrão de controlo de acesso ao meio (embutidas en cada *interface Ethernet*, que permite vários equipamentos de forma ordenada, arbitrar o acesso ao canal compartilhado); e uma mensagem tipo (*frame*/trama) que permite transportar dados, e assim, estabelecer uma comunicação lógica entre os elementos ativos da rede. Como qualquer outro protocolo IEEE *802*, a camada de enlace de dados ISO (*Data Link Layer*) é dividida em duas sub-camadas IEEE *802*: A camada MAC e a sub-camada MAC-cliente. A especificação correspondente à camada física (IEEE *802.3*), corresponde à respetiva da ISO.

A sub-camada MAC tem como principio, tarefas como o encapsulamento de dados, incluindo a construção da *frame* antes da sua transmissão, e a gestão da deteção de erros durante e depois da receção, e ainda, inclui mecanismos de iniciação do envio da palavra série (e recuperação destas em caso de falha de transmissão). A sub-camada MAC-cliente implementa o mecanismo de controlo de ligação lógica (*Logic Link Control* (LLC)), que providencia o interface entre o MAC da *Ethernet* e as camadas superiores da pilha protocolar. O LLC é definido pela IEEE-*802.2*. Ainda prevê propriedades de *bridging*, que consiste numa interface entre LANs que usam o mesmo protocolo (e.g. *Ethernet* para *Ethernet*), ou mesmo, entre distintos protocolos (e.g. *Ethernet* para *Token Ring*). Este mecanismo está especificado em IEEE *802.1*.

Cada computador interligado numa rede *Ethernet* opera independentemente de todas as outras estações conectadas à mesma, ou seja, não existe um *master* da comunicação (controlador central). Todos os equipamentos ligados a uma rede deste tipo estão ligados a um sistema de sinalização, denominado meio (*medium*). A atividade sobre o meio físico consiste num mecanismo inicial de "escuta do canal" (antes do envio de qualquer dado), e quando este estiver inativo, os dados são enviados sob a forma de *frames* ou pacotes. Esta processada, o princípio mantém-se, recorrendo como tal ao referido mecanismo de controlo de acesso ao meio (da camada MAC) - CSMA/CD.

Como cada *frame Ethernet* é enviada para o meio compartilhado, todas as interfaces *Ethernet* verificam o endereço de destino na mensagem e processam-na, caso exista um *match* com o seu valor identificativo.

A estrutura de mensagem comum, para redes *Ethernet* 10/100 Mbit/s (*Basic IEEE Ethernet MAC Data Frame*) é descrita abaixo na Tabela 3.7. A sequência de envio corresponde à ordem sequenciada da linha mais acima para a mais abaixo, da tabela referida.

Tabela 3.7: Elementos e descrição da mensagem *Ethernet*

| Posição | Nome | Tamanho de Dados | Descrição |
|---|---|---|---|
| 1º Campo | Preâmbulo | 7 *bytes* | Padrão alternado de zeros e uns que sinalizam o inicio de uma *frame* nos recetores. |
| 2º Campo | *Start-of-frame delimiter* (SFD) | 1 *byte* | Padrão de sequência de *bits* que sinalizam a chegada dos *bytes* relativos ao endereço de destino. |
| 3º Campo | Endereço de Destino | 6 *bytes* | Seis *bytes* identificativos do endereço no qual deve ser processada a mensagem. |
| 4º Campo | Endereço de Origem | 6 *bytes* | Seis *bytes* identificativos do endereço do equipamento do qual a mensagem é proveniente. |
| 5º Campo | Comprimento/Tipo | 2 *bytes* | Indica o número de *bytes* de dados MAC-cliente que estão contidos no campo de dados da *frame*, ou o ID de tipo de *frame* utilizada (existem outras estruturas de mensagens especificadas menos utilizadas). |
| 6º Campo | Dados | 46-1500 *bytes* | Campo disponível para *bytes* de dados. |
| 7º Campo | *Frame check sequence* (FCS) | 4 *bytes* | Tipicamente aplicado o algoritmo CRC (já referido). |

### 3.6.3 IP

*Nota: O conteúdo desta secção tem como fonte integral a referência em [80].*

O protocolo IP foi desenvolvido pelo departamento de defesa dos E.U.A, com o intuito de possibilitar a trocar de blocos de dados (*datagram*) entre computadores. Cada equipamento tem um endereço definido pelo próprio protocolo, possibilitando o encaminhamento de dados entre estações, até ao seu destino. Além disso, o IP permite a fragmentação dos dados a enviar, em mensagens mais curtas, que possam ser transmitidas por redes locais como a *Ethernet*. Os equipamentos que implementarem este protocolo podem reagrupar os fragmentos, construindo a mensagem original novamente.

O protocolo *internet* permite o envio de dados de forma independente às redes físicas que os conectam (Telefónica, *Ethernet*, *X.25*, *Token bus*, etc.), sendo que, para tal, este cria uma rede virtual (rede *internet*) baseado nos endereços *Internet*. Este protocolo fornece à camada de transporte um serviço de transferência de informação não confirmado, sem estabelecimento de ligação (*Connectionless*). Desta forma a troca fiável de mensagens entre as camadas de transporte não é garantido. O percurso das mensagens não é constante, podendo estas, por isso, chegarem fora de ordem ao destino.

- **Mensagem Internet**

  A unidade de transferência de dados deste protocolo denomina-se mensagem IP. Esta tem uma grande variedade de campos, e é apresentada abaixo na Tabela 3.8, pressupondo a mesma sequência de leitura, das tabelas do mesmo tipo apresentadas atrás. O comprimento máximo da mensagem não está definida no protocolo, no entanto, estas mensagens são transmitidas dentro de mensagens de "camada inferior", por exemplo do protocolo *Ethernet*, até ao equipamento de destino.

Tabela 3.8: Elementos e descrição da mensagem *IP*

| **Posição** | **Nome** | **Tamanho de Dados** | **Descrição** |
|---|---|---|---|
| 1º Campo | Versão | 4 *bits* | Versão do protocolo IP usado pelo equipamento. |
| 2º Campo | Comprimento Cabeçalho | 32 *bits* | - |
| 3º Campo | Tipo de Serviço | 8 *bits* | Cada mensagem tem uma prioridade que pode variar de 0 a 7. Pode ser pedido à rede que entregue a mensagem com *delay*, ou pelo contrário, no caso de existirem vários caminhos à escolha, que seja o mais rápido (maior largura de banda). |
| 4º Campo | Comprimento Total | 16 *bits* | - |
| 5º Campo | Identificador | 16 *bits* | Permite ao recetor identificar e reagrupar os vários fragmentos da mesma mensagem original. |
| 6º Campo | *Flags* | 3 *bits* | *Flags* que sinalizam aspetos relativos à fragmentação da mensagem. |
| 7º Campo | *Fragment Offset* | 3 *bits* | Especifica a posição do fragmento na mensagem principal ( pois os dados podem não chegar ao destino sequencialmente). |
| 8º Campo | Tempo | 12 *bits* | Usado para as mensagens IP não circularem indefinidamente na rede. A cada passagem num *gateway* este valor é decrementado. |
| 9º Campo | Protocolo | 8 *bits* | Campo utilizado por protocolos de mais alto nível, tipicamente TCP ou *User Datagram Protocol* (UDP), para indicar qual deles está a suportar-se na mensagem IP. |
| 10º Campo | *Checksum* do Cabeçalho | 16 *bits* | Verificação da integridade dos bits do cabeçalho, por um mecanismo simples de soma e verificação, entre o emissor e o recetor. |
| 11º Campo | Endereço de Origem | 32 *bits* | Endereço do equipamento de origem do qual a mensagem é enviada. |
| 12º Campo | Endereço de Destino | 32 *bits* | Endereço do equipamento de destino no qual a mensagem é recebida. |
| 13º Campo | Opções | Variável | Este campo não é usado em todas as mensagens IP, apenas é usado nas mensagens de controlo e teste da rede. |
| 14º Campo | *Padding* | 8 *bits* | Este campo é o último do cabeçalho e não contém nenhuma informação útil, apenas existe para garantir que o número de bits do cabeçalho é múltiplo de 32. |
| 15º Campo | Dados | Variável | Neste campo circulam os cabeçalhos e dados das camadas superiores. O comprimento deste campo é variável e depende do tamanho das tramas da camada lógica (ou MAC-*frames*) onde as mensagens IP , viajam através da rede. |

- **Endereço IP**

  Como verificado, o endereço IP, designado a cada equipamento que implementar o protocolo, é a chave que permite a este, encaminhar as mensagens através dos vários tipos de redes como se o equipamento emissor estivesse na mesma rede do equipamento de destino. O endereço IP foi criado para facilitar as decisões de encaminhamento. A Tabela 3.9 contêm as três classes do endereço IP (cada um deles com 32 *bits*).

Tabela 3.9: Elementos e descrição da mensagem *IP*

| **Classe** | **3 *bits* iniciais** | **Número de *bits* para identificar a rede** | **Número de *bits* para identificador o equipamento** | **Máscara de Rede** |
|---|---|---|---|---|
| A | 0XX | 7 | 24 | FF000000 |
| B | 10X | 14 | 16 | FFFF0000 |
| C | 110 | 21 | 8 | FFFFFF00 |

É sob esta forma que os endereços permitem identificar o equipamento de destino, tal como a rede onde este se encontra. Os *routers* analisam os *bits* do endereço relativos à rede de destino, e tomam com base nesses processos de verificação, decisões de encaminhamento. Como este endereço é definido com base na rede onde está inserido, o seu valor é dinâmico caso o equipamento não seja estático.

- **Routing**

  Como já referido, a *Internet* é formado por muitas redes ligadas entre si, através de *gateways* ou *routers*. São estes que permitem encaminhar as mensagens IP, ao longo dos equipamentos intermédios, sendo isto feito, de forma transparente para o equipamento emissor. Existem dois tipos de encaminhamento, o directo e o indirecto, tal que, o equipamento destino está na mesma rede física que o equipamento emissor, ou respetivamente, o equipamento destino está noutra rede e os pacotes IP têm de passar através de outros *routers* ou *gateways* para alcançarem o equipamento. Na Figura 3.15 pode-se observar um pequeno esquema entre ligações de várias redes por meio de *routers*, que criam uma rede virtual que a todos os contempla.

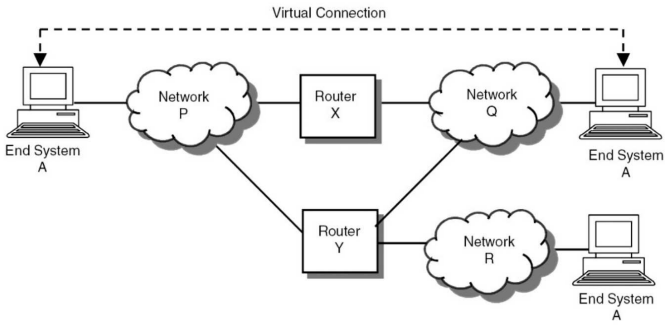



Figura 3.15: Esquema de *routing* [80]

Os mecanismos de *routing* passam inicialmente, por o equipamento emissor verificar o endereço de destino do recetor, e analisar se ele faz parte da sua rede, ou seja, decidir se precisa de enviar a mensagem para o destinatário, através de uma mensagem-IP que tem de ser enviada para um *router* (para encaminhamento). Até a mensagem chegar ao destinatário, o procedimento é continuado, ou caso contrário, a mensagem é prontamente enviada para o equipamento da mesma rede do emissor, sem recorrer ao *routing*. Os *routers* são dotados de uma tabela, denominada *Tabela de IP-Routing* onde constam informações que permitem a estes decidir se precisam de re-encaminhar a mensagem para outro (para o mesmo procedimento), ou enviá-la diretamente para o equipamento de destino (na sua rede).

- ***Internet Control Message Protocol* (ICMP)**

  O protocolo IP, como referido, não estabelece mecanismos de confirmação de entrega de mensagens, pois trata-se de um serviço sem estabelecimento de ligação (modo Pacote). Caso o processo de *routing* não seja bem sucedido, é conveniente que as camadas superiores de funcionamento sejam notificadas para que sejam tomadas as devidas ações corretivas, tipicamente o re-envio.

  O protocolo ICMP pode ser implementado pelos dispositivos de reencaminhamento para enviarem mensagens de erro ou controlo. As mensagens protagonizadas por este protocolo são transferidas dentro da mensagem IP e são trocadas entre entidades ICMP transparentemente ao utilizador.

- ***Address Resolution Protocol* (ARP)**

  O ARP consiste num protocolo de resolução, associado à problemática de o endereço Internet ser atribuído independentemente do endereço físico, sendo sempre necessário obter este último, exceto nas mensagens *broadcast*, para envio destas(mensagens direcionadas apenas a um equipamento) até ao destino. O problema assenta no fato de que normalmente o endereço físico não é encapsulável no endereço Internet (exceto em algumas exceções, como na *Pronet*), e por isso, este tem de ser validado dinamicamente por recurso ao ARP. O mecanismo consiste, quando um dado equipamento pretende saber o endereço físico de outro, envia um pacote ARP (endereço físico *broadcast*) com o endereço Internet do equipamento pretendido. O equipamento que verificar o *match* deste com o seu próprio, responde com o seu endereço físico.

- ***Reverse Address Resolution Protocol* (RARP)**

  Este protocolo faz o processo inverso do anterior, sendo que, com base no endereço físico, determina qual o seu endereço IP.

### 3.6.4 *ZigBee*

*Nota: O conteúdo desta secção tem como fonte quase integral a referência em [81]. Todo o conteúdo distinto é normalmente referenciado.*

Esta secção pretende focar dentro dos protocolos sem fios, o *Zigbee*, que pelas suas características, apresenta ser a solução mais robusta, pela sua versatilidade nos sistemas em estudo, e pela forte aplicabilidade em sistemas tipicamente pouco lineares no que

toca à topologia de rede. Na perspetiva em que se pode ter apenas um nó de acesso controlado (e.g. habitações comuns), ou uma rede composta por dezenas (ou mesmo centenas de pontos de acesso), em que para os diferentes casos, este apresenta robustez suficiente para cumprir ambos os requisitos, ao nível da complexidade da implantação, sem se tornar inviável financeiramente (com topologias mais ou menos exigentes). O fato de ter sido arquitetado para baixos consumos energéticos, permitindo grandes níveis de autonomia, e por ser uma ferramenta flexível nas mais variadas áreas de interesse, torna a necessidade do seu foco relativamente a outro soluções, ainda mais imprescindível.

As áreas de aplicação do *ZigBee* são imensas, podendo-se apontar como as principais, a aplicação em sistemas automatizados de edifícios (segurança, sitemas de *heating, ventilation, and air conditioning* (HVAC), domótica, etc.), sistema de controlo de energia e sua gestão, e nos mais distintos sistemas industriais, quer ao nível de controlo e monitorização de sistemas de produção, quer ao nível de sistemas de informação puramente alheios ao acionamento de sistemas. A Figura 3.16 apresenta mais algumas áreas de aplicação desta tecnologia.


Figura 3.16: Áreas de aplicação do *ZigBee* [82]

De forma geral, a grande potencialidade desta tecnologia, assenta na sua grande capacidade de poupança de energia, do fato da dimensão dos módulos instalados ser claramente reduzida face a outras soluções, e pela simplicidade de prototipagem de sistemas. Por outro lado, a velocidade de transferência de dados é baixa (relativamente a outras soluções como *Wi-Fi*), e o nível de complexidade de parametrização dos módulos de uma uma rede de média/grande dimensão, aumenta.

#### 3.6.4.1 Norma 802.15.4

A norma *802.15.4* especifica as duas camadas de funcionamento mais baixas da tecnologia *Zigbee* (MAC e *Physical Layer* (PHY)), enquanto a *ZigBee Alliance* desenvolveu as duas camadas superiores, respetivamente, "Rede (*Network Layer Overview* (NWK)/Segurança(*Security Support Provider* (SSP)))" e "Suporte e Aplicação".

- **Camada Física**

  A camada física (PHY) do *ZigBee* é responsável por permitir a transmissão de PDUs (unidades de dados), através de ondas rádio. Esta utiliza a modulação *Di-*

*rect Sequence Spread Spectrum* (DSSS) que incorpora em cada bit um padrão de redundância, e os difunde pela largura de banda utilizada. Essa redundância permite não só que os dados sejam identificados como pertencentes a um determinado nó, como facilita a deteção de erros, e sua correção.

As gamas de frequência utilizadas, são a 2.4*gigahertz* (GHz) (global), 925MHz (América), e 868MHz (Europa). Cada um destes valores de funcionamento pressupõem diferentes taxas de transferência, número de canais, e claro está, espectros de funcionamento diferentes. Esta camada é ainda responsável por monitorizar a potência dos canais, indicar a qualidade da conexão, e de fazer o *report* dos canais disponíveis (*Clear Channel Assesment* (CCA)).

- **Camada MAC**

  A camada MAC, como já referida no contexto de outras tecnologias, é responsável pelo processo de encapsulamento dos dados provenientes de camadas superiores, para de seguida os transmitir. Existem dois modos de operação aplicáveis por este protocolo, que caracterizam o modo de acesso ao meio. São este o *Modo Beaconing* e *Modo Non-Beaconing*. O primeiro consiste em fazer com que os nós com função de roteamento transmitam periodicamente *beacon frames*, sinais sinalizadores para confirmar a sua presença na rede. Utilizando-se de boa sincronia, os nós da rede (exceto o coordenador) podem permanecer inativos entre os *timings* de poupança de energia e os *beacon frames*. O modo *non-beaconing* é caracterizado por os *routers ZigBee* normalmente terem os seus recetores continuamente ativos, necessitando por isso, de uma fonte de energia mais robusta e arquitetada. No entanto, este permite redes heterogéneas, em que alguns dispositivos recebem dados constantemente, enquanto outros apenas transmitem quando detetam um estímulo externo.

#### 3.6.4.2 Dispositivos

- **Tipos**

  As especificações IEEE definem para as redes *ZigBee* dois tipos de dispositivos: os de função reduzida (*Reduced Function Device* (RFD)), e os de função total ( *Full Function Device* (FFD)). Estes últimos são capazes de funcionar em qualquer modo de operação padrão, tais como, coordenador, *router*, ou dispositivo final, sendo capazes de comunicar com outros de qualquer um dos tipos. Os RFD, por sua vez, só podem comunicar com outros do mesmo tipo, tal que, só poderão atuar apenas como *end-pointings*. São dispositivos simples e de mais baixo custo, visando um consumo de energia ainda mais baixo.

- **Funções Lógicas**

  Dependendo das funções dos nós da rede, estes podem ser classificados como pontos coordenadores, *routers*, ou dispositivos finais (*end-points*).

  – **Coordenador**

    O coordenador é o nó inicial da rede. Um dispositivo ao ser ligado pela primeira vez como coordenador iniciará a sua rede selecionando um identificador

*Personal area network* (PAN) único no seu raio de influência. Na inicialização, todos os canais da frequência de operação são verificados até esse PAN ID único ser encontrado. O coordenador opera em estado ativo para efetuar o controlo da rede e costuma ser alimentado diretamente, reduzindo o risco de falha no nó centralizador da rede.

- ***Router***
  Os dispositivos *routers* são usados em topologias em malha (*mesh*) e *cluster*, para dar maior robustez à rede. Eles possuem tabelas de roteamento e, por serem FFD, permitem encontrar o menor caminho para se chegar ao destino. Caso o *router* não possua o endereço de destino requisitado, este fará o *broadcast* de uma requisição de rota (*route request*) e receberá do destino a rota mais eficaz atualizando sua tabela. Este mecanismo dá à rede a característica de auto-regeneração caso ocorra a queda das funcionalidades de outros nós com funções de roteamento na rede.
- **Dispositivo Final**
  São os nós terminais das topologias estrela, *cluster*, e *node-to-node*. Por serem dispositivos RFD, não recorrem a mecanismos de roteamento, nem coordenam a rede. Eles comunicam-se diretamente com o *router* "pai" e podem ser implementados com microcontroladores ainda menores (em termos de memória e potência) passando quase todo o tempo em estado inativo. Um dispositivo RFD é a comum localização de sensores, atuadores e sistemas de controle.

A Figura 3.17 demonstra de forma simplista um rede que contempla todos os três tipos de dispositivos funcionais que podem integrar um sistema *ZigBee*. A Tabela 3.10 contempla algumas das funções na camada de rede, respetiva a cada um dos tipos, sendo que, a utilização da letra "x" corresponde à existência de tal funcionalidade.

Tabela 3.10: Funções dos dispositivos na camada de rede *ZigBee*

| **Coordenador *ZigBee* (ZC)** | ***Router ZigBee* (ZR)** | **Dispositivo Final *ZigBee* (ZED)** | **Função na Camada de Rede** |
|---|---|---|---|
| x | - | - | Estabelecer uma nova rede *ZigBee* |
| x | x | - | Conceder endereço lógico de rede |
| x | x | - | Permitir que dispositivos entrem ou saiam da rede |
| x | x | - | Manter lista de vizinhos e rotas |
| x | x | - | Roteamento de pacotes da camada de rede |
| x | x | x | Transferir pacotes da camada de rede |

#### 3.6.4.3 Topologias

Este protocolo possibilita diferentes topologias de rede, ou seja, diferentes formas de dispor os diferentes dispositivos com base na suas funcionalidades, sendo que, cada distinta opção pressupõem vantagens e desvantagens dependendo da aplicação, sejam estas ao nível da robustez, economia energética, ou níveis de centralização/distribuição da rede. Existem três topologias principais, sendo estas do tipo estrela, malha, ou árvore.

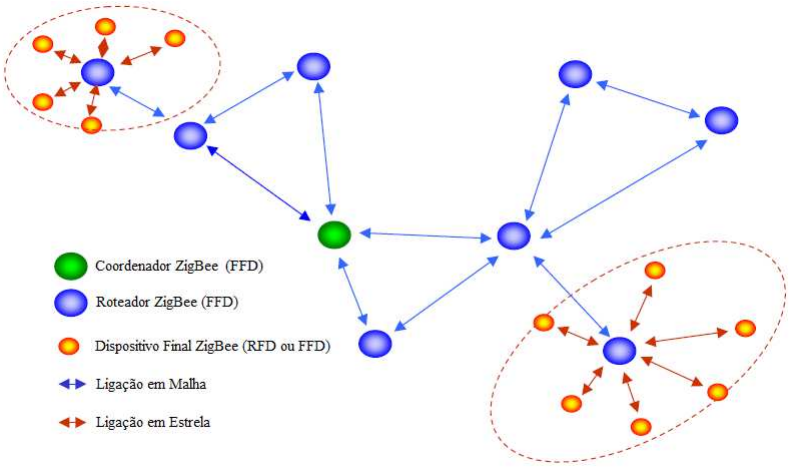



Figura 3.17: Modelo de rede *Zigbee* [81]

- **Estrela**

  Na topologia estrela a conexão é realizada entre os dispositivos, e um único coordenador central, que é chamado de coordenador PAN. Quando um FFD for ativado pela primeira vez, ele pode estabelecer sua própria rede e tornar-se o coordenador PAN. Cada rede vai funcionar com um identificador PAN, diferente dos usados por outras redes que estejam dentro da região de influência das ondas de rádio, permitindo que cada uma das redes opere individualmente.

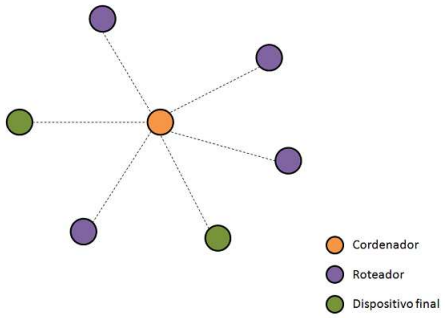



Figura 3.18: Representação de uma rede em estrela [81]

- **Malha**

  A topologia em malha, também conhecida como *mesh*, tem apenas um coordenador PAN. Nessa topologia todos os dispositivos podem comunicar entre si, desde que estejam dentro dos alcances dos dois. Essa topologia pode ser considerada uma rede *ad-hoc*, com capacidade de se auto-organizar e de se auto-estruturar (*self-organizing e self-healing*). Essa configuração permite também múltiplos percursos de dados, ligando um dispositivo aos outros da rede, de forma a permitir uma maior robustez nesta.

- **Árvore**

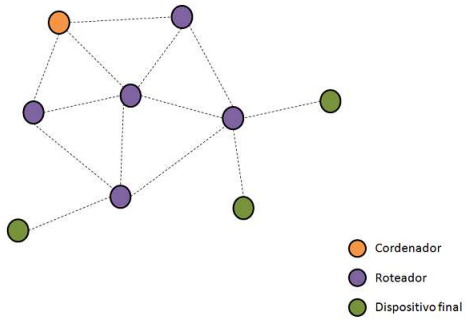



Figura 3.19: Representação de uma rede em malha [81]

Esta topologia pode ser exemplificada como um aglomerado de redes com topologia malha, ligados por um coordenador PAN, que ficará responsável pela rede. O coordenador PAN formará o primeiro *cluster* estabelecendo-se como um coordenador do aglomerado (*Cluster Head* (CLH)), estipulando um identificador para esse *cluster* (*Cluster Identifier* (CID)), através da escolha de um identificador PAN ocupado. O dispositivo fará o *broadcast* do *beacon frame*, anunciando a existência da rede. Qualquer dispositivo que o tenha recebido, pode requisitar a sua entrada na rede (no CLH em questão). Se o coordenador PAN permitir a entrada do novo dispositivo ele será adicionado como um novo dispositivo "filho" na sua listagem da vizinhança. Os dispositivos recém adicionados irão estabelecer-se, e assim como os seus "pais", enviarão *beacon frames* procurando novos candidatos a juntarem-se à rede. O coordenador PAN pode instruir um dispositivo a se tornar o CLH de um novo aglomerado adjacente ao primeiro. A principal vantagem desta estrutura em árvore é aumentar a área de cobertura, com a consequência de aumento do *delay* da mensagem.

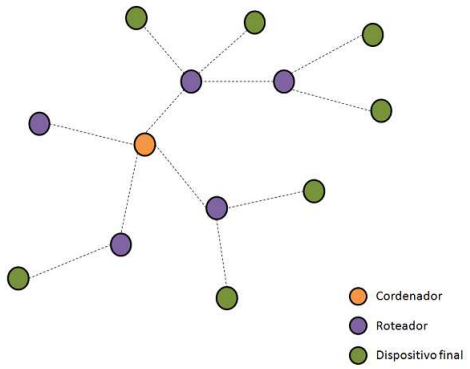



Figura 3.20: Representação de uma rede em árvore [81]

# Capítulo 4

# Sistemas de Controlo de Acessos Físicos: Especificação

Neste capítulo pretende-se que o leitor tome conhecimento geral da solução proposta e das razões que levaram à sua definição, explicando-se sustentadamente, numa fase inicial, a tecnologia de identificação/autenticação proposta (através de uma tabela de apoio à decisão). Numa segunda fase, o capítulo pretende apresentar uma série de pontos, analisando aspetos como a posição do mercado relativamente à tecnologia selecionada, e claras vantagens no desenvolvimento de novas soluções baseadas nesta.

## 4.1 Tabela de Apoio à Decisão: Tecnologia de Identificação/Autenticação

Com o objetivo de suportar a decisão na escolha da tecnologia de identificação/autenticação, foi utilizada uma tabela de apoio à decisão (Tabela 4.1). Para a construção desta, o autor selecionou o conjunto de tecnologias que apresentam maiores níveis de utilização no contexto de controlo de acessos físicos, e outras que tecnologicamente apresentam recursos para tal (um total de seis). Foram também definidas seis características de análise: segurança, flexibilidade, grau de inovação, tendência de mercado, complexidade de desenvolvimento de soluções, e custo da tecnologia. Pontoou-se as tecnologias num intervalo de 1 a 6, sendo que, a repetibilidade destes valores no mesmo parâmetro não deverá existir, de tal forma, que a cada tecnologia fica associado um, e só um valor, para o mesmo parâmetro. Estes definidos, é feita uma média aritmética dos resultados designados a cada uma das tecnologias, e gerada uma pontuação. Por esta razão todos os parâmetros de avaliação contêm um peso na decisão final equivalente. É importante referir que este tipo de recurso está limitado ao conhecimento e opinião do autor, mesmo que, tenha sido aplicado o máximo de imparcialidade.

Nos tópicos abaixo, será para cada um dos parâmetros de avaliação, feita uma breve explicação dos valores apontados, com o intuito de os justificar:

- *Segurança*

  As tecnologias biométricas, pelo seu teor de análise de características uni-pessoais e utilização de modelos matemáticos altamente fiáveis, foi considerada o grupo de

tecnologias de reconhecimento mais segura. Por outro lado o cartão magnético pela facilidade de reprodução, e ausência de sistema integrado de encriptação (módulo processador) é designado como o menos seguro. A chave metálica, solução mais adotada no mercado para prover o acesso a um dado espaço físico, continua, nas suas versões *state-of-the-art*, a ser uma das mais seguras formas de restringir o acesso a um espaço. A designação do valor associado à tecnologia *smart card* é feita, pelo fato de se tratar de uma tecnologia de contacto, muito embora, os leitores tenham de ser implantados em posições que viabilizam o *hack* destes. O RFID é apontado como o segundo menos seguro, devido a ser uma tecnologia que baseia o seu funcionamento na transmissão de dados por rádio-frequência, onde existe a possibilidade de interceção de dados com dispositivos próprios para o efeito, que posteriormente permitem a reprodução da mensagem intercetada. O NFC pelas restrições de distância de comunicação (máx. 10cm), e pelas especificações de comunicação em alguns dos seus tipos (por exemplo, P2P), inviabilizam, quando devidamente estruturada um sistema nele baseado, a descodificação ou reprodução das mensagens (ou troca destas) que influem na validação de um acesso.

- *Flexibilidade*

  Este é um dos fatores industrialmente mais "pesados" aquando a análise de uma tecnologia para desenvolvimento de produto ou serviço. Deve-se essencialmente ao fato de hoje em dia o mercado exigir um nível de prestação de funcionalidades centralizadas nos mais distintos dispositivos, bastante alto. Por se ter definido que a designação de valores tinha que ser distribuída por cada uma das tecnologias propostas sem repetibilidade, neste ponto fará menos sentido argumentar os valores propostos, já que, algumas delas não são minimamente integráveis noutros dispositivos. O NFC é claramente a tecnologia com maior nível de interoperabilidade e flexibilidade entre distintas áreas de aplicação (principalmente ao nível de serviços). O RFID apesar da sua aplicação em massa nas mais distintas operações industriais e de serviços, ao nível da integrabilidade apresenta menores níveis de implementação em dispositivos "contentores de pequena dimensão" (embora seja igualmente flexível). Ambos, pela diminuta dimensão do *hardware*, e por implementarem modos de comunicação *wireless* são os mais bem cotados. As tecnologias biométricas têm a melhor pontuação seguinte, por alguns dos seus tipos se basearem em *templates* recolhidos por simples câmaras (e.g. reconhecimento facial), ou sensores de muito pequena dimensão (e.g. impressão digital). Os *smart cards* de contacto, pela sua pequena dimensão também apresentam boas características de integração, embora a flexibilidade na construção das aplicações esteja algo condicionada. As chaves e bandas magnéticas, a este nível apresentam ser soluções obsoletas.

- *Grau de Inovação*

  O grau de inovação é outro dos aspetos considerados bastante relevantes nesta análise. Entenda-se este numa perspetiva de mercado, em que a classificação é feita com base no nível expectável de satisfação durante a experiência dos utilizadores e o fator "novidade" associado, ou seja, avaliação da capacidade de resposta ao mercado sustentada na inovação ou melhoria do produto. Por as bases de desenvolvimento do NFC terem sido exatamente este aspeto, e a questão da capacidade de incorporação noutros dispositivos de funcionalismos principais distintos, foi-lhe garantida

a classificação máxima. As tecnologias biométricas, associadas ao claro desenvolvimento computacional que as suportam (na obtenção dos *templates* e tempo de verificação em processo de autenticação), aliado ao aumento de resolução dos sensores e câmaras, garantem-lhe o segundo lugar. As restantes, excetuando o RFID ao nível dos sistemas anexos de processamento e gestão de dados, são obsoletas a este nível.

- *Tendência do mercado*

  Este parâmetro pretende classificar a aposta da indústria na aplicação e desenvolvimento destas tecnologias, onde é inversamente proporcional o nível de estagnação destas. Como é percetível este fator é fortemente dependente dos anteriores. Como referido anteriormente, na tentativa de acompanhar os requisitos de mercado, as necessidades passam principalmente, por centralizar os recursos e serviços num único dispositivo (sendo os *smartphones* os dispositivos de maior foco pelas suas propriedades e dependência dos utilizadores). Outras vertentes do mercado têm foco distinto, pelas necessidades inquiridas ao produto ou serviço em sistemas de controlo de acessos físicos que prestam, tais como, implantações tremendamente exigentes ao nível de segurança (e.g. espaços militares, e *data center's* de informação altamente confidencial), ou implantações em que a rapidez de autenticação é fulcral (e.g. grandes corporações na hora de início de serviço), onde respetivamente, no primeiro caso a segurança é foco de melhoramento (centrando-se principalmente nas tecnologias biométricas), e no outro a facilidade de uso (e.g. RFID/NFC). Pela primeira razão apontada, o NFC é a tecnologia com maior aposta, seguindo-se o RFID pelo baixo custo e flexibilidade num conjunto alargado de aplicações. As tecnologias biométricas pelos aspetos apontados no tópico anterior em 3º, seguindo-se os *smartcards* de contacto pelas possibilidades associadas às suas características de *hardware*. Finalmente, a chave metálica e os cartões magnéticos.

- *Complexidade*

  A complexidade no desenvolvimento de novas soluções, ou de implementação de raiz de soluções distintas assentes na mesma tecnologia, são proporcionais ao nível de complexidade do *hardware* de implementação dos sistemas, e estão também, diretamente relacionados com a complexidade da arquitetura física destes, da complexidade dos modelos de análise dos "templates" ou dados de credenciação, e dos recursos anexos que necessitam para o seu normal funcionamento. Por todo o conjunto de aspetos referidos nos outros parâmetros, pela quantidade de projetos desenvolvidos bem documentos *open-source*, e pela tecnologia em si, a pontuação foi definida de acordo com a tabela seguinte.

- *Preço*

  Pelas razões indicadas no início do tópico anterior, os sistemas por biometria são claramente os mais dispendiosos. Por ser uma tecnologia de contacto de pequenas dimensões; com módulo controlador; normalmente embutida; e na generalidade pouco aplicada (concorrência de mercado menor), considerou-se a tecnologia *smartcard* a segunda mais dispendiosa. A chave metálica pela sua forma de fabrico (altamente complexa e precisa para versões *state-of-the-art*), e numa perspetiva de

gestão destas numa grande implantação, foi pontuada como o 3º pior caso. O cartão magnético pela sua simplicidade/baixa complexidade foi considerado mais caro que o RFID e NFC pela posição que detém no mercado como recurso funcional, seguro e versátil, ao contrário destes dois, que pela tecnologia que implementam e pela dinâmica industrial que produzem à volta das suas aplicações e novas soluções, os embaratece.

Feita esta análise, aponta-se o NFC pelo seu carácter inovador, versatilidade, e capacidade de incorporação noutros dispositivos, como a tecnologia de suporte a implementar e validar nesta dissertação.

## 4.2 Aspetos de Mercado

Esta secção pretende apresentar ao leitor de uma forma breve, aspetos importantes de mercado relacionados com a tecnologia selecionada (NFC), recorrendo a dados estatísticos sob a forma de diagramas ou gráficos, com a final pretensão de dar a conhecer o atual nível de maturidade da tecnologia, o seu nível de integração, e a conjuntura desta para o futuro.

### 4.2.1 Maturidade e Evolução

Com vista a explicar a emergência desta nova tecnologia, ou seja, a sua evolução, e como esta progride até um nível de aceitação global, serão apresentados os *Hype Cycles for emerging technologies*, lançados anualmente pela Gartner's (companhia de análise de mercados e tecnologias, e de consultadoria para os mais diversos ramos). Os *Hype Cycles* têm cinco fases (*Technology Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment, e Plateau of Productivity*), que contemplam os estados que atravessa uma tecnologia até ao seu estabelecimento completo. Para além disso uma tecnologia tem um nível de visibilidade(expectabilidade) em cada um dos cinco estágios (posição desta numa curva imutável), sendo estes últimos, sequenciados no tempo. A análise destes diagramas entre dois, ou três anos consecutivos, permite a parametrização da evolução da tecnologia. As Figuras 4.1, 4.2, e 4.3 consistem nos *Hype Cycles for emerging technologies*, respetivamente, do ano 2011,2012 e 2013.

Pela análise do *Hype Cycles* de 2011, verifica-se que o "NFC *Payment*", que dita na generalidade a potencialidade da tecnologia, posicionou-se no pico das "expetativas exageradas", revelando curiosidade do mercado na sua aplicação, com um prazo previsto, até ao seu estabelecimento robusto, de 5 a 10 anos. No ano seguinte, com o mesmo prazo de maturação previsto, a tecnologia foi posicionada na zona do "vale da desilusão" (zona típica de início de desenvolvimento de aplicações, re-estruturação da normalização, e adição de especificações). Este ano, a *Gartner's* deixou de especificar a tecnologia sob a forma de serviço para pagamentos, mas como lhe é devido, como apenas a tecnologia "NFC", diminuindo num ano para um prazo de maturação expectável de 2 a 5 anos. Posto isto, a consolidação está para breve, tanto ao nível de sistemas de pagamento móveis integrados, como da tecnologia em si para outros efeitos.

Por outro lado, o fato de grandes companhias (*Apple, Google, Microsoft*) serem pioneiras na exploração desta tecnologia, e tendo em conta a influência dos seus produtos

Tabela 4.1: Tabela de apoio à decisão da tecnologia de identificação/autenticação

| | Segurança | Flexiblidade/Embeddedness Capacity | Grau de Inovação | Tendência do Mercado/Nível de Estagnação Tecnológico | Complexidade no Desenvolvimento de Soluções | Preço | Pontuação |
|---|---|---|---|---|---|---|---|
| **Chave Metálica** | 5 | 1 | 2 | 2 | 6 | 3 | 3,3 |
| **Cartão Magnético** | 1 | 2 | 1 | 1 | 5 | 4 | 2,5 |
| ***Smart Card* (de contato)** | 3 | 3 | 3 | 3 | 2 | 2 | 2,7 |
| **Tecnologias Biométricas** | 6 | 4 | 5 | 4 | 1 | 1 | 3,5 |
| ***RFID*** | 2 | 5 | 4 | 5 | 4 | 6 | 4,3 |
| ***NFC*** | 4 | 6 | 6 | 6 | 3 | 5 | 5,0 |

e da sua posição do mercado, no mesmo, é bastante expectável que a adoção do NFC possa acontecer mais rapidamente.[83].

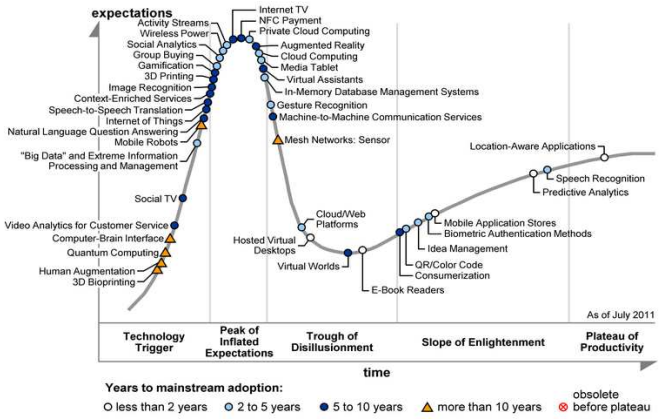



Figura 4.1: *Hype Cycles for emerging technologies*, 2011 [84]

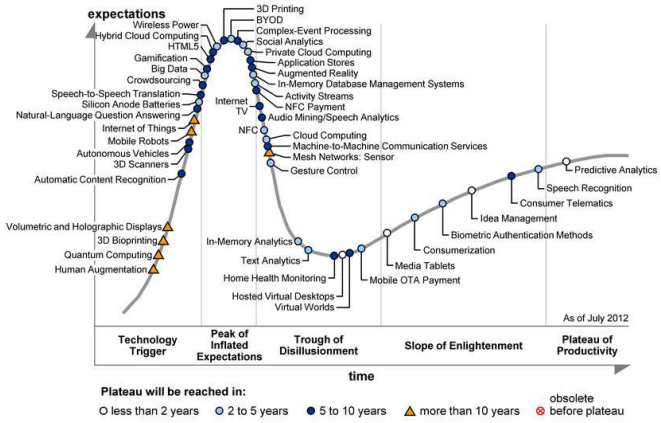



Figura 4.2: *Hype Cycles for emerging technologies*, 2012 [84]

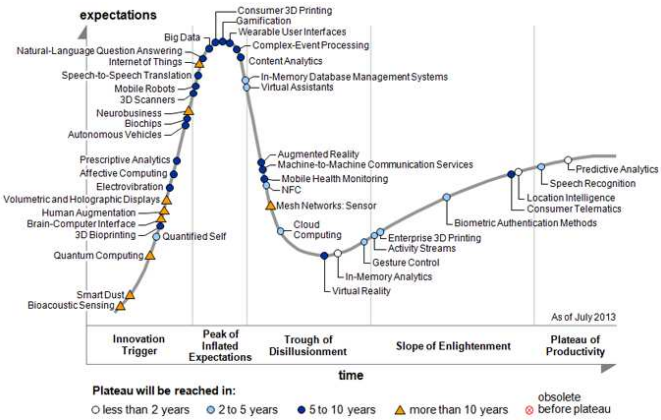



Figura 4.3: *Hype Cycles for emerging technologies*, 2013 [84]

A Novembro de 2012 foram também lançados dados interessantes pela ABI Research®, onde apresentaram sob forma de um gráfico (4.4) a evolução da taxa de fornecimento de dispositivos móveis habilitados com a tecnologia NFC para o mercado. No artigo que o referencia, é referido que a ‘*‘ABI Research has announced that it is expected that NFC will come out of the trial phase next year, as a result the tech is expected to see growth in the number of devices and functionality”*. É destacado também, que a tecnologia atingiu um nível de interoperabildiade tal, que o foco deixa de ser unicamente para os pagamentos através de *smartphones*, mas também para outras aplicações, tais como, retalho, funções de leitura, autenticação, e aplicações comerciais gerais.[85]

Pela análise da Figura 4.4, verifica-se o claro crescimento de *smartphones* dotados de tecnologia NFC entre 2008 e 2012, não só em quantidade, como em valor percentual. O fato deste crescimento se dar num período em que a tecnologia ainda é referida como estando em estágio “trial”, serve de indicador de que a mesma, é alvo de aposta pelos principais fabricantes para aplicações de futuro.

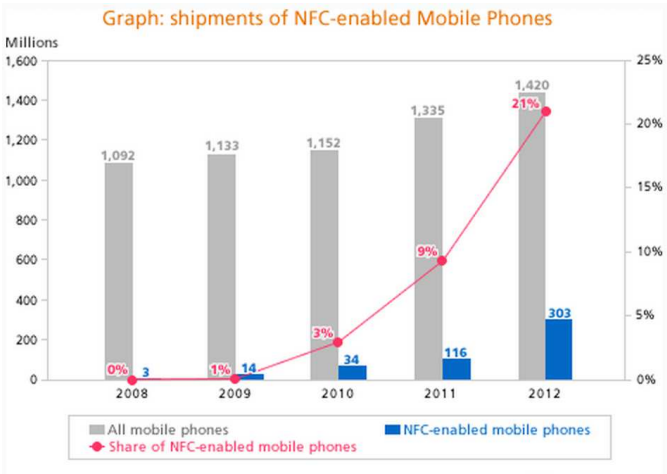



Figura 4.4: Evolução da taxa de fornecimento de dispositivos móveis habilitados com a tecnologia NFC para o mercado [2008-2012] [85]

### 4.2.2 Previsões

Nesta fase, é interessante verificar algumas previsões relacionadas com a tecnologia NFC, que aliadas ao seu comportamento no mercado(analisado atrás), permite compreender não só o seu percurso até à data, como a mais provável conjuntura num futuro próximo. Algumas curiosidades a este nível são feitas nos seguintes tópicos, estando estes associados, igualmente a dois distintos artigos.

- *ABI® - NFC Mobile Payment Transaction Spend to Hit the $100 billion Mark in 2016 [86]*

  A 18 de Outubro de 2012 a ABI® *Research* publicou um artigo, onde afirma que o valor das transações por tecnologia NFC ía subir dos registados 4 biliões de dólares em 2012, para 191 em 2017, ultrapassando a marca dos 100 em 2016. Porém o destaque é focado no fato de se considerar que mais importante do que efetuar pagamentos desta forma, é a convergência dos vários tipos de pagamentos

já existentes (por proximidade, P2P, e online), num único dispositivo NFC. Apesar destes dados, outros analistas apontam valores completamente díspares dos aqui referidos (mais dados em [87]). Além disso, o artigo refere que a convergência do mercado não está completamente pronto para a implementação comercial em massa, mas que o valor potencial de acrescentar o NFC foi identificado, e que, os fornecedores de *smart cards*, dispositivos de *Original Equipment Manufacturer*s (OEMs), e *Mobile Network Operator*s (MNOs), em parceria com prestadores de serviços de redes e pagamentos, estão prontificados a beneficiar desta convergência induzida pelo NFC.

- *IHS® - US Wireless Carriers Partner with Big Credit Card Companies, Boosting Cell Phone NFC Market [88]*

  A 12 de Maio de 2011 a iSuppli®, por Jagdish Rebello, publicou um artigo onde entre muitos aspetos, refere o caráter impulsionador que as grandes operadoras móveis em parceria com as grandes empresas de cartões de crédito norte americanas, tiveram sobre o desenvolvimento da tecnologia NFC. É também referida a grande contribuição da Google®, muito associado ao desenvolvimento da plataforma *Wallet*, que numa fase inicial dependia da tecnologia NFC para o seu uso.

  Analisando a Figura 4.5, fica-se com uma ideia clara da aposta do mercado móvel na tecnologia NFC nos últimos anos, e para o futuro, perspetivando um crescente proporcional número de aplicações e serviços apoiados nesta tecnologia.

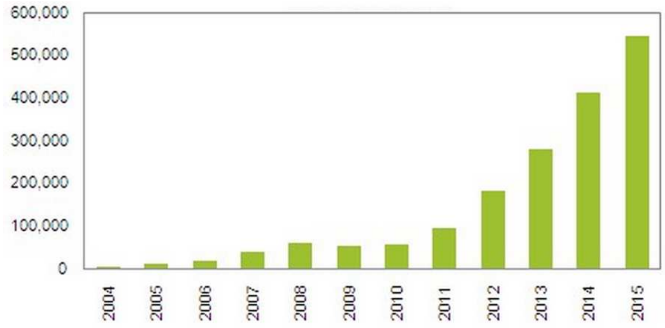



Figura 4.5: Previsão mundial do número de dispositivos com tecnologia NFC de 2010 a 2015, e evolução verificada de 2004 a 2010 (em milhares de unidades) [88]

## 4.3 Definição do Problema

Como deverá ser percetível, nesta fase em que a tecnologia base de funcionamento proposta para a implementação (NFC), foi definida e caracterizada (ao nível do mercado e funcionamento), alguns aspetos propiciam à sua implementação. Na perspetiva de uma dissertação é conveniente que estes sejam problemas, que influam numa solução que permita tirar conclusões sobre os mesmos, e no limite validar algo que os diminua.

Como indagado até então, nas diversas referências ao NFC, a sua necessidade passa por convergir mais rapidamente para um estado de verdadeira definição e aceitação no mercado. Portanto, o fato de esta ser uma tecnologia emergente, confere-lhe algumas desvantagens, tais como, grau de desconfiança, e consequentemente, considerável baixo

nível de implementação; carência de definição no mercado; necessidade de demonstrar ser solução alternativa nas mais diversas aplicações (face a tecnologias já devidamente estabelecidas); entre outros aspetos.

Ao nível do mercado de sistemas de controlo de acessos físicos, destaca-se de forma clara o problema base. Este baseia-se no fato de existir uma convergência óbvia para o desenvolvimento de soluções, que visam grandes implantações, onde tipicamente, estão associadas corporações com alto nível de exigência em controlo de acessos ( modelos e sistemas suficientemente robustos para cumprir os seus requisitos). Desta forma, o mercado influi num estado de baixo fornecimento de soluções alternativas para as comuns habitações domésticas.

## 4.4 Objetivos da Implementação

Definidos os principais problemas, ou pontos de interesse, os objetivos da implementação desta dissertação, passam simultaneamente por dois pontos principais:

1. Desenvolver um protótipo funcional de um sistema de controlo de acessos físicos, para aplicação doméstica, onde por um lado, procurará fornecer as principais funcionalidades dum sistema deste tipo, como tentará simplificar o produto, tanto ao nível da arquitetura do *hardware*, como em termos de interação com o utilizador.

2. Validar o NFC como alternativa tecnológica para aplicações de autenticação em sistemas de controlo de acessos físicos, procurando também, oferecer um contributo na evolução e aceitação da tecnologia.

## 4.5 Solução Proposta para a Implementação

A presente secção pretende dar a conhecer ao leitor a proposta de implementação, que inclui a descrição geral da arquitetura do sistema, a interação geral pretendida entre os diferentes subsistemas, tal como a definição base do funcionamento, e potencialidades que se pretendem implementar nos diferentes módulos do sistema. Esta solução visou atingir um estado de prototipagem funcional, na perspetiva de determinar pelo seu uso, características e aspetos positivos, em determinação do trabalho futuro, relativamente à viabilidade e visão geral, de um produto final.

### 4.5.1 Arquitetura Geral

A presente solução proposta prende-se com a prototipagem de um sistema que contemple apenas um nó de acesso, focado em aplicação doméstica, gerido por um sistema remoto ao *Physical Access Point (PAP)*, e com dispositivo móvel como meio de identificação/autenticação. Este está dividido em três subconjuntos distintos, que devem interagir entre si. Um primeiro módulo (módulo central), constituído por um computador e um módulo de comunicação wireless, sendo o primeiro, dotado de um software de interação com os utilizadores do sistema, tendo este acesso a uma base de dados local, com intuito de guardar e gerir a informação do sistema. Este deve comunicar via *wireless* com o sistema remoto, que fica localizado no PAP, e que é constituído por um elemento

controlador; um módulo de comunicação compatível com tecnologia de dispositivos móveis NFC; um módulo de comunicação *wireless* que permita a troca de dados com o módulo central, e uma fechadura elétrica. O "ator" final do sistema, utilizador dotado de um dispositivo móvel com tecnologia NFC (com a aplicação desenvolvida) que deverá interagir diretamente com o nó de acesso para efeitos de identificação/autenticação, sob a forma de aproximação deste após a inserção de uma password. A Figura 4.6 apresenta um esquemático simples dos elementos base referidos.

### 4.5.2 Módulo Central

O módulo central, como referido, contempla um conjunto de elementos, que no limite se destinam a fornecer ao administrador e utilizadores um subsistema, que de forma geral, permita gerir o PAP, interagir com este, tal como, contemplar um *software* dotado de interface gráfica que possibilite fazer as operações básicas comuns, dum gestor de controlo de acessos físicos. Como tal, pretende-se utilizar recursos que potencializem o bom funcionamento geral deste módulo, como um dispositivo de comunicação *wireless* que deverá comunicar segundo o protocolo *Zigbee*, e uma base de dados local, utilizando um gestor adequado como ferramenta de desenvolvimento e *debug*, e a linguagem *Structured Query Language* (SQL) como meio de comunicação entre este último e o programa desenvolvido.

#### 4.5.2.1 *Software*

Como qualquer sistema de controlo de acessos físicos contêm um *software* de gestão de dados, e modos intuitivos de interação com os utilizadores do sistema, propôs-se a construção de um semelhante, que seja provido das funcionalidades básicas destes, sendo que, de forma a não perder o foco do objetivo principal (avaliação da tecnologia NFC em sistemas de controlo de acessos físicos), evitou-se a implementação de recursos de complexa aplicação, tal como, a execução rígida em forma de código, de qualquer um dos modelos de controlo de acessos previamente apresentados, que garantem obviamente, uma flexibilidade e robustez aos sistemas deste tipo. Nesta perspetiva, revela-se trabalho bastante árduo e pouco conclusivo na linha dos objetivos definidos, perfeitamente evitável.

A este nível, propõem-se a utilização de um *Integrated Development Environment* (IDE) desenvolvido pela *Microsoft*, Visual Basic®, que apresenta comparativamente a outras soluções, algumas vantagens, tais como, uma estrutura de programação simples e intuitiva, um ambiente interativo e de rápido desenvolvimento de interface gráfica, boa documentação *online*, e as mais variadas classes de funções para implementação direta. Como desvantagens, pode-se apontar o fato de os programas não serem funcionais noutros sistemas operativos (distintos do *Windows*®), e por exemplo, comparativamente à linguagem C, é impossível deter como recurso de programação, mecanismos como *array's* de estruturas e outros.

A Figura 4.7 contêm um esboço do posicionamento relativo aos objetos com o qual os utilizadores poderão interagir, da *interface* proposta. A *form* inicial de autenticação deverá surgir no arranque do programa, e logo que validado o utilizador, é fechada. Por isso, pela sua simplicidade, será apresentada apenas no capítulo seguinte (Implementação).

Posto isto o programa deverá ter as seguintes características e funcionalidades:

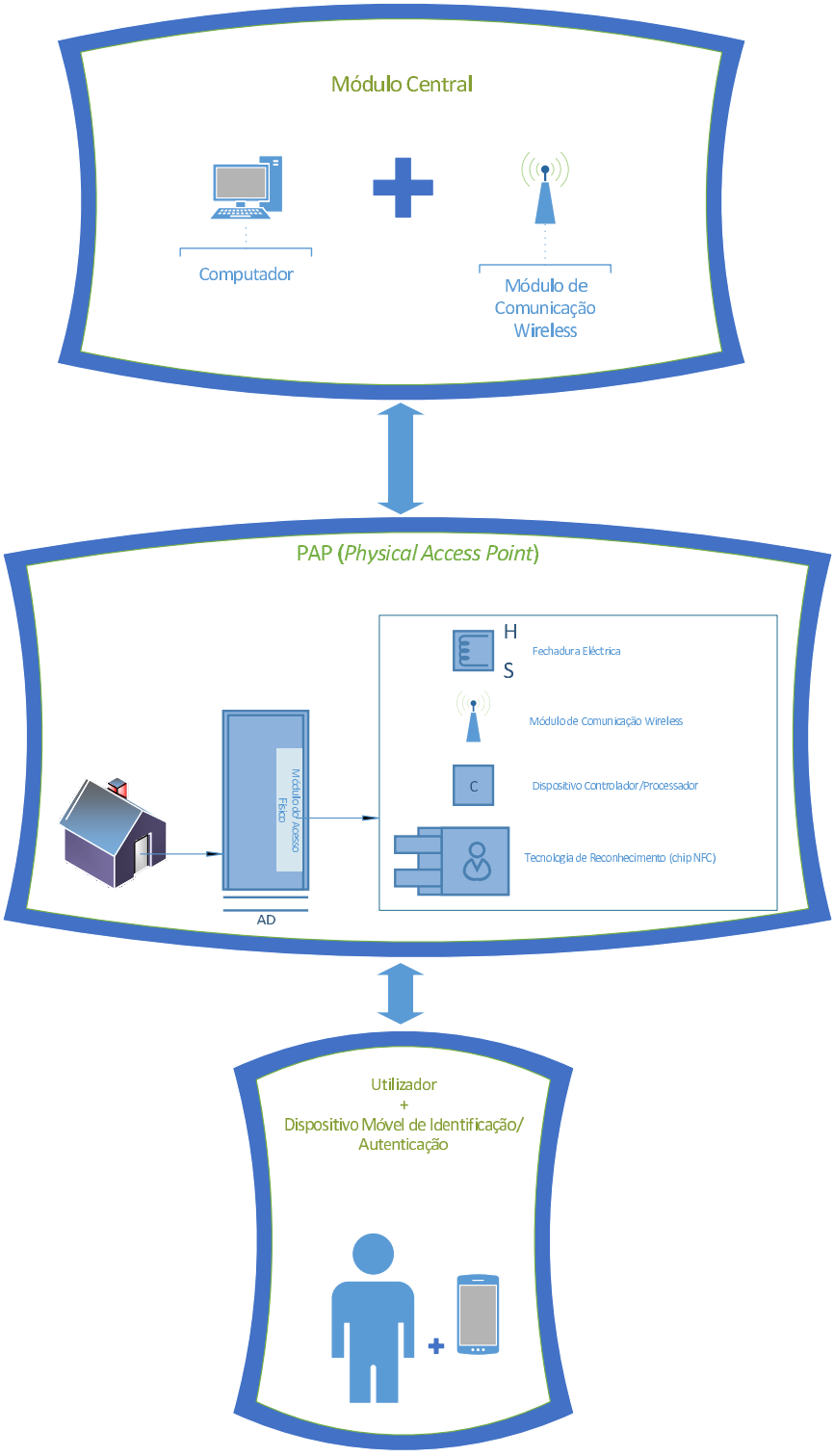



Figura 4.6: Esquema geral da solução proposta

- *Interface* inicial de autenticação, recorrendo ao *match* de um nome de utilizador e *password* correspondente, por consulta da Base de Dados (BD), onde também deve ser introduzida o valor da porta *Communication Port/Serial Port Interface* (COM), correspondente à ligação com o módulo de comunicação *wireless*;
- Dois tipos de autenticação: como administrador ou como utilizador comum;
- Comunicar através da porta série (RS-232) com o módulo de comunicação *wireless ZigBee*;
- Comunicar com a base de dados por SQL para efeitos de consulta e registo de dados;
- Receber e processar mensagens vindas do PAP;
- Atualização de um histórico de acessos na BD ,*on-time*, quando for efetuado um destes pelos utilizadores;
- Deter um modelo simplista de permissões, que gira funcionalidades, como adicionar utilizador ao sistema, remover um deste, condicionalismo na verificação de histórico de distintos utilizadores, e no limite possibilitar outros gerirem permissões dos distintos (fornecer permissões de administrador);
- Permitir a modificação de dados dos utilizadores autenticados;
- Proteções gerais ao nível da programação que evitem constrangimentos ao utilizador durante a interação com o programa;
- Aplicação de *threads* (principalmente rotinas automáticas de atualização de campos), com o objetivo de diminuir a dependência do programa, relativamente ao utilizador;
- Abrir remotamente o acesso através do programa.

#### 4.5.2.2 Módulo de Comunicação *Wireless*

Este elemento do módulo central, é um recurso de *hardware* que permite comunicar com o PAP via *wireless*, ou seja, sem cablagem. Como terá sido entendido nas secções apresentadas focadas nas topologias de sistemas de controlo de acessos físicos, a comunicação entre os controladores, ou elementos de processamento e/ou reencaminhamento de informação, é feita tipicamente com recurso a protocolos de comunicação que assentam em transmissão de dados por meio físico sólido (cabos - fios elétricos). Este aspeto não é descabido, pois as garantias de proteção contra interferências externas, provocados por sistemas vizinhos, é maior nestes casos, porém, por os meios de comunicação *wireless* apresentarem uma cada vez maior robustez a este nível, pela sua crescente utilização em virtude do decréscimo dos sistemas apoiados em meio de comunicação físicos, e por este protótipo não ter sido focado para ambiente industrial (altamente interferente), propõem-se a implementação de uma comunicação *ZigBee* P2P.

O programa deverá, por intermédio deste módulo de comunicação, enviar mensagens para o PAP, com pedidos de credenciação (ou modificação de credencias) de utilizadores, eliminação de credenciais destes, e abertura direta do acesso físico diretamente pelo programa (remotamente).


Figura 4.7: Esboço da proposta da *interface* gráfica

#### 4.5.2.3 Base de Dados

Considerando-se a base de dados, sob os seus diversos modelos de funcionamento, um dos recursos computacionais aplicados mais importantes, desde em pequenas aplicações, aos mais complexos sistemas de informação, propõem-se a sua utilização, na perspetiva de que é uma forma de garantia organizacional dos dados do sistema, e um mecanismo de proteção destes. Neste contexto a BD será local, no mesmo computador onde corre a aplicação que interage com o administrador/utilizadores, embora muito facilmente pudesse ser alocada num servidor externo, onde consequentemente a ligação á *WEB* seria uma necessidade, apresentado-se tal fato como uma desvantagem claro para um sistema de controlo de acessos físicos de nó único.

Pela simplicidade e baixa quantidade dos recursos necessários a guardar na base de dados, não foi necessário o recurso às propriedades relacionais dos gestor da BD. A solução proposta pressupõem três tabelas, uma para registo de administradores, outra para utilizadores comuns (embora estes possam deter permissões que os igualem aos primeiros, caso estes o permitam), e finalmente, uma para o histórico. Cada uma das duas tabelas inicialmente referidas, deverá ser constituída por 9 atributos característicos a cada utilizador (*Username*, *Login Password*, *PAP Password*, *First Name*, *Last Name* e quatro atributos com *flags* associados às suas permissões). A tabela de histórico deverá ser constituída pelos atributos: *Username, First Name, Last Name, Time, Date and "n"*. Este último deverá representar o número de acesso desde o início de implementação do sistema, sendo iterado automaticamente a cada acesso validado.

As operações de "leitura" e "escrita" na BD pelo programa *VB* deverá ser feita sob a forma de *query's* SQL, trocadas entre a aplicação e o servidor implementado.

### 4.5.3 PAP

Este módulo é o mais determinante e exigente relativamente ao funcionalismo necessário, para que o protótipo seja validado. Também, pelos inúmeros elementos em interação, o controlo e gestão deste módulo acrescenta complicações. Este deverá ser capaz de processar as ordens do módulo central, intercetar os pedidos de abertura do acesso físico, prover o utilizador de notificações áudio-visuais, abrir a fechadura elétrica (quando um acesso for confirmado). Deve ainda notificar o módulo central aquando um acesso validado (para atualização do histórico).

#### 4.5.3.1 Controlador

Um elemento controlador que consiga processar comandos com base em decisões lógicas, é de todo indispensável neste módulo. Este para além de ser capaz de efetuar processamento lógico e operações aritméticas, deve conter um conjunto de periféricos e características que o permitam, por exemplo, implementar os mais distintos protocolos de comunicação (UART, I2C e SPI), gerar sinais *Pulse-Width Modulation* (PWM), implementar *timer's*, etc.

Além deste aspeto, deve ser um elemento de pequenas dimensões. Posto isto, propõe-se a utilização de um microcontrolador ($\mu$c), pois ao contrário de um microprocessador não necessita de circuitos externos para funcionar e são aplicados em sistemas tipicamente mais compactos, contendo todos os periféricos necessários ao seu funcionamento. Por outro lado, são computacionalmente menos poderosos, mais lentos, e possuem um espaço de endereçamento menor.

Este microcontrolador deverá ser capaz de implementar as seguintes funcionalidades:

- Utilização de saídas digitais para ativação e desativação dos *led's*;
- Gerar um sinal PWM para ativação do *buzzer*;
- Comunicar via I2C com a placa de desenvolvimento NFC a adotar;
- Atuar sobre o transístor de ativação da fechadura elétrica;
- Comunicar via UART com o módulo de comunicação *wireless*;
- Conter funções de interrupção chamadas aquando a receção de dados vindos do módulo central;
- Configurar o *Watchdog Timer* (WDT) para re-ativação em caso de bloqueio numa dada instrução máquina;
- Rotinas de filtragem da mensagem recebida via *wireless* do módulo central, e processamento das ordens respetivas;
- Configurar, inicializar o chip NFC, e processar as mensagens vindas deste;
- Processar o CRC-16 nas mensagens de envio, e verificar o mesmo, nas mensagens de receção;
- Operar sobre a *Electrically-Erasable Programmable Read-Only Memory* (EEPROM) interna, com funções de registo e leitura;

#### 4.5.3.2 Placa de Desenvolvimento NFC

Este é o elemento crucial, e a base da tecnologia em estudo nesta dissertação. Por facilitismo e por em estado de prototipagem não fazer sentido a implementação direta do *chip* NFC (devido às suas dimensões reduzidas, provável danificação do seu estado durante a soldadura dos pinos, e pela necessidade de adição de *hardware* complementar), é proposta a utilização de uma placa de desenvolvimento com o *chip* NFC integrado.

O *chip* em questão deverá comunicar sob três formas possíveis: I2C, SPI, ou UART. Como o modo de comunicação entre o microcontrolador e o módulo *wireless* utiliza a porta série do $\mu$c, e apenas haver uma disponível, e aliado ao fato do protocolo I2C ser o modo pré-definido padrão (comummente), este último é o proposto. O *chip* deverá ser o dispositivo *slave* da comunicação, e por isso, toda a gestão da comunicação e interação com dispositivos móveis de aproximação é feita nas camadas superiores de funcionamento pelo *master* - $\mu$c. O tipo de comunicação proposto é o P2P, pela sua versatilidade e vantagens nesta aplicação, tal que, o dispositivo "alvo" será o *chip* NFC da placa adotada (do PAP), e o dispositivo "iniciador", é o de identificação/autenticação dos utilizadores, usados para validar o acesso.

#### 4.5.3.3 Elementos de Notificação Áudio-Visual

A proposta de elementos deste tipo, baseiam-se na necessidade do utilizador ter um *feedback* do funcionamento e estado do sistema. Propõem-se a utilização de um *led* vermelho (pisca quando há erro de processamento do leitor, ou credenciais não válidas), verde (pisca quando há credenciais válidas e acesso garantido) e amarelo (pisca durante o *beam* da mensagem), para notificação visual, e dois sinais sonoros distintos gerados pelo *buzzer*(um associado ao evento do *led* vermelho, e outro do verde).

#### 4.5.3.4 Fechadura Elétrica

Este é o elemento do sistema que constringe o acesso de indivíduos alheios ao sistema, e que assim, garante a proteção do espaço por impedimento de passagem, sendo este apenas possível aquando cumprido o algoritmo de identificação/autenticação. Propõem-se a aplicação de uma fechadura elétrica do tipo relé (bobine excitada, por tensão aplicada nos seus terminais, que pelo campo magnético induzido, atrai o linguete de bloqueio da mesma).

#### 4.5.3.5 Módulo de Comunicação *Wireless*

Este módulo é a segunda *Peer* de comunicação *wireless* do sistema, e como tal, permite o fluxo de dados entre o PAP e o módulo central. É através deste par intercomunicador bi-direcional que são transferidas as mensagens entre os dois elementos essenciais do sistema global. Por implementarem um modo de comunicação *Zigbee* P2P, na implementação um dos dois será configurado como coordenador, e outro como "dispositivo final", muito embora, este aspeto seja irrelevante no caso P2P, onde não à necessidades de operações de *routing*, nem constrangimentos associados à posição que assim lhes serão definidas. Este módulo serve unicamente para receber as ordens do sistema global (já referidas), e de notificação (em tempo real) a este, dos acessos que o PAP conferir.

### 4.5.4 Dispositivo Móvel

Ao nível do dispositivo móvel, será necessário, para completar a arquitetura funcional do sistema, a construção de uma aplicação de identificação/autenticação baseada na tecnologia NFC, sendo lógico que para isso, o dispositivo seja dotado de tal. Propõem-se para tal o desenvolvimento de uma aplicação protótipo funcional, para sistema operativo Android®com as seguintes características:

- *Interface* simplista e de rápida interação;
- *Text Box* limitada a 4 caracteres onde deverá ser inserida a *password* de acesso;
- Texto simples, breve, e discreto, a descrever o procedimento de autenticação;
- Relativamente a aspetos de programação mais específicos:
  - Encapsular a *password* num *MIME record*;
  - Codificar e encapsular o registo gerado numa mensagem no formato NDEF;
  - Instanciar *handler's* para verificações gerais, tal como, a existência de tecnologia NFC no dispositivo;

# Capítulo 5

# Implementação

Neste capítulo pretende-se que o leitor fique com o conhecimento total da implementação realizada. Serão abordados aspetos funcionais, tal como os algoritmos de processamento de dados no programa do módulo central, e do controlador do PAP; esquemas elétricos(endereçados para os apêndices); componentes usados; mensagens de interação entre diferentes subsistemas; entre outros aspetos.

## 5.1 Módulo do PAP

Nesta secção é abordada toda a implementação relacionado com o PAP[1], módulo localizado junto à posição de autenticação na implantação, abordando-se aspetos relacionados com a sua arquitetura física, e dinâmica entre os seus distintos elementos. É feita também uma breve justificação da escolha dos principais elementos, seu funcionamento e configurações.

### 5.1.1 Arquitetura Física

Numa primeira fase é importante evidenciar de forma genérica, de que forma é que foi arquitetado este subsistema, para que o conteúdo abordado nos seguintes tópicos seja mais facilmente compreendido, e para isso é apresentado na Figura 5.1 um esquema geral das partes ativas, e de que forma elas interagem com o microcontrolador.

#### 5.1.1.1 Seleção dos principais elementos

No seguimento da solução proposta, onde foi subtilmente indiciado o tipo de componentes que se pretendiam aplicar, é importante referir nesta fase que *hardware* foi realmente utilizado, fundamentando-o.

- *Microcontrolador*

  O elemento controlador selecionado, de todo o módulo PAP, foi a *PIC 18F4620*. A escolha deste microcontrolador sustenta-se no fato deste apresentar uma enorme potencialidade ao nível dos recursos que detem, fiabilidade, e suporte da

[1]Designação típica do módulo, de um sistema de controlo de acessos físicos, que é posicionado junto dos pontos de acesso, onde estes devem ser validados ou revogados

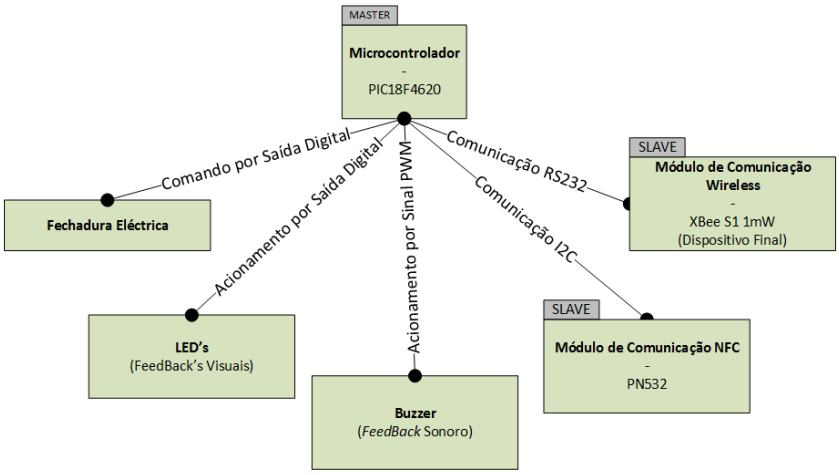



Figura 5.1: Esquema da interação entre os vários intervenientes no módulo PAP, e de que como estes interagem com o microcontrolador

Microchip®(seu fabricante), tanto ao nível do IDE de desenvolvimento gratuitamente fornecido, como da documentação facilmente interpretável para uma rápida implementação das funcionalidades pretendidas. Inicialmente foi utilizada um *PIC 16F877*, verificando-se numa fase avançada, que detinha pouca quantidade de memória *flash* programável. Selecionou-se então a *PIC 18F4620*, pelo baixo custo relativo que apresentava, por utilizar um compilador bastante semelhante (mesmo produto - *HI-TECH C*), mas para a "Family18", por ser dotado de EEPROM, e integrável na placa de desenvolvimento utilizada - *PIC DEM 2 PLUS* (fabricada pela Microchip). O esquema elétrico desta placa de suporte pode ser consultado no Apêndice A(Figura A.3).

A grande desvantagem associada ao uso deste microcontrolador, passa pela inexistência de uma biblioteca de funções aplicáveis para estabelecimento de uma comunicação com qualquer uma das alternativas de placas de desenvolvimento de sistemas, com recurso NFC. Assim, durante a realização da implementação definiu-se como objetivo secundário (embora obrigatório pelo seu caráter decisivo no funcionamento final), a criação de uma biblioteca de funções de interface entre a a placa de desenvolvimento NFC aplicada, e os PIC's de arquitetura semelhante ao utilizado.

Posto isto, apresenta-se na Figura 5.2 e Tabela 5.1, respetivamente, a representação do microcontrolador, e a listagem das suas características.

- *Placa de Desenvolvimento NFC*

  A placa NFC escolhida é fornecida pela Adafruit®, com o *chip* PN532 integrado, fabricado pela *NXP*®. A escolha assenta no fato, de à data ser das poucas soluções que apresentava um mínimo de suporte para a sua implementação, e de igual forma, o PN532, ser um dos mais utilizados e melhor documentados. Esta placa foi construída para funcionar com um Arduino®UNO, pretendendo ser uma "shield" de desenvolvimento de acoplagem direta na "board" micro-controlada, e também com largo suporte de funções para rápido desenvolvimento de soluções. Nesta linha

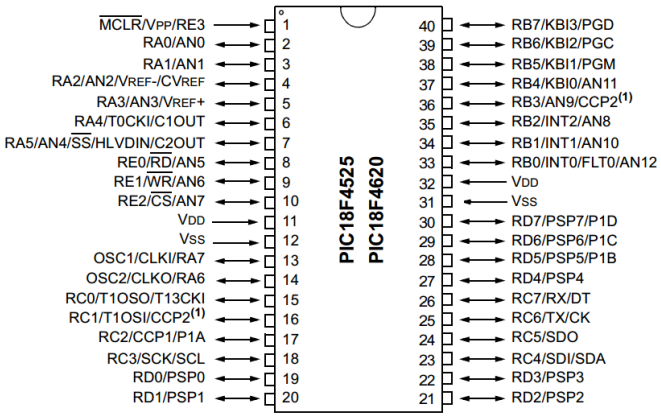



Figura 5.2: Esquemático do PIC18F4620 com referência às portas em cada pino (Versão 40 pinos) [90]

Tabela 5.1: Características de *hardware* da PIC18F4620 [89]

| **Parameter Name** | **Value** |
|---|---|
| *Program Memory Type* | Flash |
| *Program Memory* (KB) | 64 |
| *CPU Speed* (MIPS) | 10 |
| *RAM bytes* | 3,968 |
| *Data EEPROM* (bytes) | 1024 |
| *Digital Communication Peripherals* | 1-UART, 1-A/E/USART, 1-SPI, 1-I2C1-MSSP(SPI/I2C) |
| *Capture/Compare/PWM Peripherals* | 1 CCP, 1 ECCP |
| *Timers* | 1 x 8-bit, 3 x 16-bit |
| *ADC* | 13 ch, 10-bit |
| *Comparators* | 2 |
| *Temperature Range* (C) | -40 to 125 |
| *Operating Voltage Range* (V) | 2 to 5.5 |
| *Pin Count* | 40 |

o autor considera que a utilização de um dispositivo altamente suportado e orientado à placa em questão tinha sido a melhor solução (implementação de Arduino em prol das soluções da Microchip) em termos de rapidez de implementação. No entanto, expectou-se problemas de flexibilidade em outras operações necessárias, e mais importante, a contribuição de um conjunto de funções funcionais para microcontroladores PIC deixaria de ser implementada. No Apêndice A, Figura A.1, pode ser consultado o esquema elétrico da placa utilizada. A Figura 5.3 contêm a representação do seu estado de fornecimento.

- *Módulo de Comunicação Wireless (ZigBee)*

  Embora já tenha sido indicada a pretensão de utilizar dois módulos de comunicação *wireless ZigBee* para estabelecer a comunicação P2P, entre o módulo central

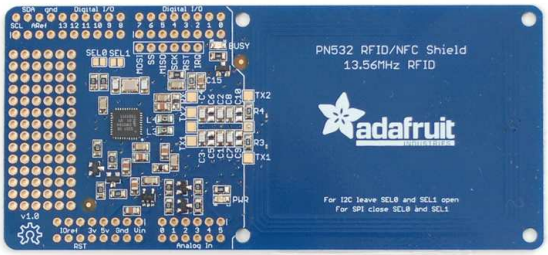



Figura 5.3: *Adafruit PN532 NFC/RFID Controller Shield* no seu estado de fornecimento [93]

e o módulo do PAP, ainda não foi referida a solução de *hardware* proposta. Foram selecionados dois módulos XBee®da Série 1 (desenvolvidos pela Digi®), quase exclusivamente pela sua simplicidade de implementação. Estes módulos vêm suportados de fábrica com *firmware* que providencia a implementação do protocolo *ZigBee*. Permite nomeadamente, a configuração dos módulos de uma forma bastante interativa e simples, recorrendo ao *X-CTU* (*software* disponibilizado pela Digi para o efeito). Além deste aspeto os módulos disponibilizados pela *Digi*, nas suas diversas configurações, contém de forma genérica funcionalidades extra, que lhe garante vantagens claras pela flexibilidade que induzem aos produtos. No Apêndice A, Figura A.2, pode ser consultado uma tabela com breves especificações de toda a linha de produtos deste tipo. A Figura 5.4 consiste no módulo aplicado, quer ao nível do PAP, quer do módulo central (embora distintamente configurados).


Figura 5.4: Módulo XBee S1 1mW [92]

#### 5.1.1.2 Esquema de Ligação

Descritos os elementos principais do sistema PAP, é agora importante descrever, de forma suportada com recurso ao esquema elétrico implementado, e a imagens da implementação, as ligações efetuadas entre as diversas partes ativas. Esta descrição tem como foco principal dar a conhecer ao leitor o meio físico por que se dão as diversas ordens de comando, acionamento, e de implementação de protocolos de comunicação, para o normal funcionamento do módulo. A Figura 5.5, corresponde à implementação do módulo PAP, e a Tabela 5.2 define os diferentes elementos enumerados na mesma. O esquema elétrico

presente no Apêndice B, Figura B.1 deve ser consultado para melhor entendimento.

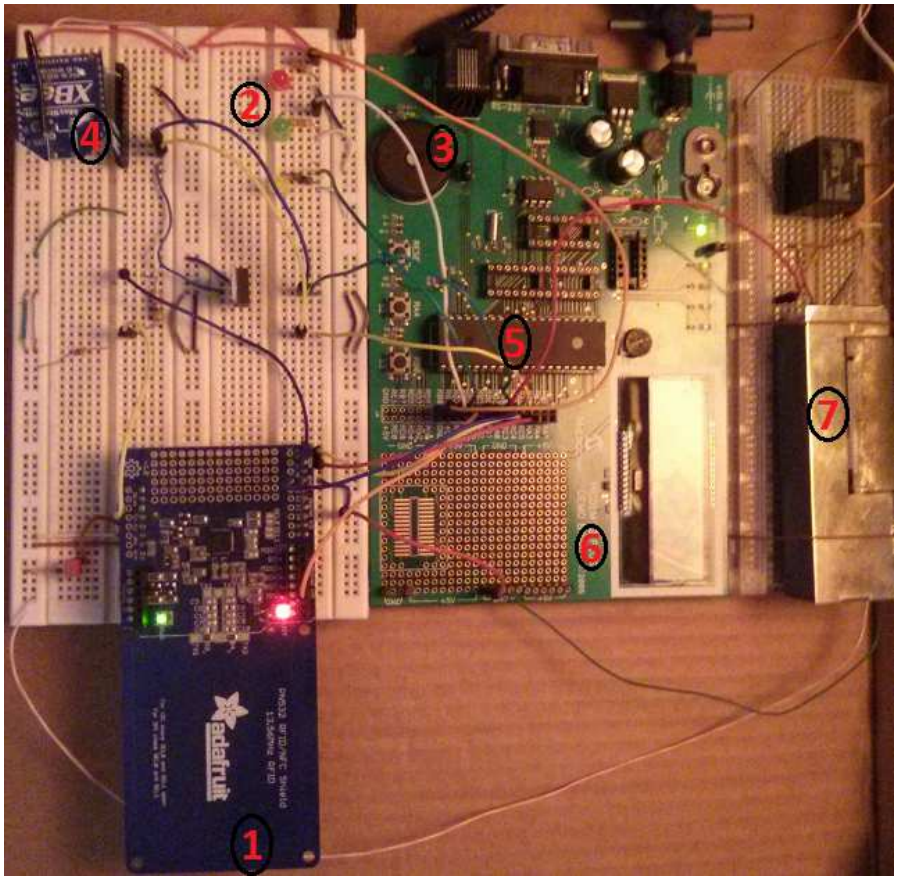



Figura 5.5: Implementação do módulo PAP

Tabela 5.2: Descrição dos elementos identificados na imagem de implementação do PAP 5.5

| **Referência Numérica** | **Elemento** |
|---|---|
| 1 | *Adafruit PN532 NFC/RFID Controller Shield* |
| 2 | LED's de sinalização |
| 3 | Buzzer |
| 4 | Xbee S1 1mW |
| 5 | PIC18F4620 |
| 6 | PIC DEM 2 Plus |
| 7 | Fechadura Elétrica |

Como evidenciado, na Figura 5.5 e Tabela 5.2, estão presentes todos os elementos até agora referenciados como indispensáveis ao funcionamento do sistema proposto. Excluindo a referência aos componentes eletrónicos pouco relevantes no contexto da dissertação, como reguladores de tensão, divisores resistivos (por meio de resistências), e outros, será feita uma descrição das ligações e o que com elas se pretende. Para uma boa compreensão, aconselha-se à consulta constante do esquema elétrico situado no Apêndice B, Figura B.1. Sobre a forma de enumeração são caracterizadas as diversas ligações

efetuadas, e elementos importantes até agora não referenciados.

1. A PIC18F4620 acciona e conecta-se ao *buzzer* através da porta RC2. Esta deve ser configurada para criar um sinal PWM, tal como, parametrizados os seus valores. O *buzzer* é também ligado ao *ground*.

2. A PIC18F4620 implementa a comunicação I2C com a placa NFC, ligando-se a esta, através da porta RC3 (configurada como linha de *clock*), e pela porta RC4 (configurada como linha de dados). Além disso conecta-se a esta através de uma entrada digital RB3 (que deve ser configurada como tal) no pino IRQ (linha de notificação utilizada para notificar o master por *hardware*, que uma resposta a um dado comando está pronta para ser encaminhada para o mesmo), e a uma saída digital RB4 que actua sobre o pino RSTPDN (utilizado para efeitos de *reset* e ativação da placa, por *hardware*). Todos os parâmetros relativos à comunicação I2C devem ser definidos em registos da memória do microcontrolador para o efeito. A placa de desenvolvimento NFC deve ser ainda ligada aos 5V do barramento de alimentação.

3. Para a atuação sobre os LED's de notificação, o microcontrolador utiliza três saídas digitais: RB0, RB1, e RB2. Estas devem também ser configuradas como tal.

4. Para comunicar com o módulo XBee são utilizadas as portas RC6 e RC7, que devem ser devidamente configuradas para implementar uma comunicação série. O RC6 corresponde ao pino de envio ("Tx"), e o RC7 ao pino de receção("Rx"), conectando-se estes, respetivamente, à porta de receção de dados do módulo XBee ("Data In" - *Din*), e à de envio ("Data Out" - *Dout*). Este ainda é ligado à linha de alimentação de 3.3V e ao *ground*.

5. A ativação da fechadura é feita por meio de um transístor e de um relé. O transístor BC547 quando em saturação pela atuação do saída digital RB7 do microcontrolar, permite o fluxo de eletrões entre os terminais da bobine do relé T73S5D15-5V, fechando este o circuito, que incorre no mesmo mecanismo da bobine da fechadura elétrica (12 V). Finalmente, o campo induzido por esta atrai o linguete e a fechadura abre-se.

6. De forma a fornecer um sinal de *clock* externo ao microcontrolador, foi utilizado um cristal de 8MHz. Este é ligado nas portas RA6 e RA7. Respetivamente, cada um deles, deve ser configurado através dos bits de configuração, como "OSC2" e "OSC1", para que o microcontrolador implemente o sinal gerado.

7. É ainda representada a ficha de programação, denominada *In Circuit Serial Programming* (ICSP), onde automaticamente gerido pelo *hardware* de programação (neste implementação foi usada a Pick It 3 - Microchip), as portas RB7/**PGD** e RB6/**PGC** são automaticamente configuradas para o efeito.

### 5.1.2 Funcionamento e Configurações

Nesta secção serão abordados todos os aspetos funcionais do sistema PAP, tal como as configurações necessárias para o seu normal funcionamento. Estes aspetos estão diretamente relacionados com o microcontrolador, por este ser a unidade processadora e de comando do subsistema.

Recorrendo ao apoio de diagramas de casos de uso, atividade, e sequência (previstos no UML 2.0), serão explicados os diversos algoritmos funcionais desta unidade. Estes diagramas não estão completamente normalizados segundo o UML 2.0, pois alguns deles não prevêem elementos de apoio adicionados pelo autor, na tentativa de facilitar a compreensão do leitor.

A estrutura deste tópico, será baseada na sequência de atividades prevista nos diagramas apresentados deste tipo. Os diagramas de caso de uso pelo seu carácter de "rascunho inicial" de desenvolvimento de aplicações, foram remetido para o Apêndice C, muito embora a sua consulta prévia seja de suma importância para uma melhor compreensão, do a seguir abordado. A Figura C.1 no mesmo apêndice, contêm o diagrama de casos de uso do sistema PAP.

#### 5.1.2.1 Iniciação do Módulo do PAP

Como referido, nesta fase é apresentado o diagrama de atividade de iniciação do módulo do PAP, sob forma da rotina de iniciação do microcontrolador - configurações internas e verificação de comunicação com o chip NFC. Na Figura 5.6 é apresentado o diagrama de atividade respetivo. Para cada bloco associado a uma atividade será explicado o procedimento tomado para a sua implementação.

- **Inicialização e Configuração de Saídas e Entradas Digitais**

  A primeira configuração no programa do microcontrolador, é a definição e configuração das portas deste, para saídas e entradas digitais. Anteriormente já foi referido a finalidade destas, e portas utilizadas, nomeadamente, actuação sobre os *LED's* de notificação (RB0, RB1, e RB2), actuação sobre o sistema "transístor-relé" para abertura da fechadura (RB7), e os dois restantes, para operações de notificação e controlo por *hardware*, com o *chip* NFC - portas RB3 e RB4.

- **Implementação do *WatchDogTimer***

  O WDT utiliza um *timer* interno não configurável, com frequência imutável, no qual se pode implementar um *prescaler* para definição do tempo de ciclo deste. Este fator foi definido com valor tal, que o WDT atua de 4 em 4 segundos. O objetivo da sua implementação passa pela necessidade de fiabilizar o sistema, pretendendo-se com o seu uso, que de forma autónoma, este reinicie em caso de bloqueio numa dada instrução. A sua configuração é feita de forma interativa, através do IDE de desenvolvimento mais recente (MPLAB X®), na definição dos *bits* de configuração. A sua ativação e desativação pode ser feita ao longo do programa, embora neste caso essa funcionalidade não tenha sido necessária, já que o processo de autenticação é bastante mais rápido, e por isso, não é interrompido.

- **Parametrização e Configuração do Sinal PWM**

  Como enunciado, este sinal é o meio de atuação no *buzzer*, aquando a necessidade de gerar ruídos de sinalização sonora. Os parâmetros de modulação da onda, consistem na definição do *duty cycle* de 50% a uma frequência de 4*quilohertz* (kHz). Esta última é definida com recurso a um *prescaler* do sinal de relógio interno *"Timer2"*. A configuração destes dois parâmetros é feita por meio da atuação sobre os registos de memória para o efeito, denominados *Special Function Register*s (SFRs).

- **Parametrização e Configuração da Porta Série**

  A configuração da comunicação série RS-232, feita do mesmo modo do que qualquer outra configuração (atuação sobre os SFRs para o efeito), consiste na configuração dos pinos RC6 e RC7, como meio de transmissão e receção de dados, definição do modo assíncrono, e definição da taxa de transferência de dados a 9600 bits/s. Além destes recursos, indispensáveis à implementação deste modo de comunicação, a PIC é configurada para associar uma função de interrupção cada vez que é recebido um *byte* no pino *Rx*. Esta função permite interromper qualquer rotina que esteja a ser processada, para processar comandos vindos do módulo central, retornando no fim destes processados, à instrução interrompida.

- **Parametrização e Configuração dos Parâmetros da Comunicação I2C**

  Neste estágio, o microcontrolador configura os pinos RC3 e RC4 como meio de comunicação I2C, entre a *PIC* e o chip NFC, sendo respetivamente, um para implementar o sinal de relógio, e outro o meio físico de transmissão e receção de dados segundo este protocolo. É definida a frequência aplicada do sinal de relógio (400 kHz), e configurado o microcontrolador como dispositivo *master* da comunicação. O endereçamento necessário para operações de "leitura" (0x48) e "escrita" (0x49) é definido nas funções para o efeito.

- **Inicialização do *Chip PN532***

  Efetuadas todas as configuração necessárias ao normal funcionamento do microcontrolador, é inicializado o *chip PN532*. Esta inicialização é feita por recurso *hardware*, atuando sobre o pino RSTPDN, com um sinal digital a 1, passando por um sinal digital a 0 por 400 ms, retornando a 1, com um *delay* posterior de 100 ms.

- **Verificação da Comunicação com o *PN532***

  Com o intuito de verificar se a inicialização do *PN532* teve efeito, é enviada um comando que pressupõem resposta do microcontrolador, e assim, a confirmação do seu estado. O comando utilizado é o *GetFirmwareVersion*, especificado em [95]. Caso não seja recebida qualquer resposta, é feito uma nova tentativa de inicialização do *chip*, e novamente verificado o seu estado. Mais detalhes na página 73 da fonte acima referida.

- **Configuração do *Security Access Module* (SAM) do *PN532***

  A configuração do SAM do *PN532* é necessária, neste caso para notificar o *chip* de que a sua utilização é prescindível e não vai ser implementada. Para efeitos de utilização, é necessária a parametrização do fluxo de dados pretendido, pela configuração interna do *switch* de dados série. É também neste comando que é definida a pretensão de se utilizar o pino *IRQ*. Mais detalhes na página 89 da referência em [95].

- **Configuração de Parâmetros Internos do *PN532***

  Esta configuração, tem como objetivo definir parâmetros gerais de configurações, do seu comportamento nos mais distintos casos(geração automática, ou não, de comandos de baixo nível implementados pelo *chip*; utilização, ou não, de certos

campos na estrutura de mensagem entre o *master* e o *slave*; etc.). As configurações são feitas num único *byte*, em que cada bit constituinte corresponde a uma *flag* para o estado pretendido de cada recurso. Mais detalhes na página 85 da referência em [95].

#### 5.1.2.2 *Loop* Funcional do PAP

Validado todo o algoritmo anterior, o microcontrolador entra no designado "*Loop* Funcional do PAP", que corresponde à rotina de espera de aproximação de um dispositivo móvel de autenticação, comunicação com este, processo de verificação, e autenticação. O diagrama de atividade correspondente a este algoritmo, é apresentado na Figura 5.8. A descrição das atividades e aspetos com estas relacionados, são abordados de seguida.

- **Configuração do *PN532* como Dispositivo "Target" - Efeitos de Deteção**

  A implementação desta atividade é de suma importância, relativamente ao mecanismo de espera do dispositivo móvel de aproximação. O comando utilizado foi o *TgInitAsTarget* , que tem por objetivo configurar através do dispositivo *master* (PIC), o PN532 como *target* (e todas as características de comunicação associadas), na comunicação P2P (por NFC), sendo por isso, o dispositivo de aproximação o "initiator". Mais detalhes na página 151 da referência em [95].

  Embora esta função tenha uma aplicação muito própria, neste contexto, foi utilizada como ferramenta, ou mecanismo, de espera de dispositivo. Implementou-se desta forma, pois o PN532 só responde ao comando em questão, no fim de interagir com o dispositivo de aproximação. Isto possibilita interromper a rotina do microcontrolador na instrução de leitura da resposta, do barramento I2C, até que esta seja entregue pelo mesmo.

- **Espera por Dispositivo de Aproximação**

  Esta atividade consiste na espera de resposta do comando anterior, que é equivalente, como referido, à espera da dinâmica inicial entre o chip "leitor", e o chip de "identificação".

- **Configuração do *PN532* como Dispositivo "Target" - Efeitos de Comunicação**

  Detetado o posicionamento de um dispositivo externo, em fronteira de comunicação com o PN532 do PAP, o comando atrás mencionado é novamente utilizado, para configurar o PN532 como dispositivo "target", desta vez, com a devida parametrização para efeitos de comunicação. Este é sem dúvida o comando de campos de parametrização mais complexo de definir, pois implica um conhecimento razoável dos vários estágios de inicialização entre os dois dispositivos, tais como, operações de configuração para devida sincronização dos parâmetros de comunicação, PDUs para ativação do protocolo, seleção de parâmetros genéricos, *Data Exchange Protocol* (DEP), e desativação da comunicação. A definição destes campos só pode ser feita por consulta da especificação referenciada em [96]. Os estágios com necessidade de configuração, estão de forma global, presentes no diagrama da página 11 do mesmo documento.

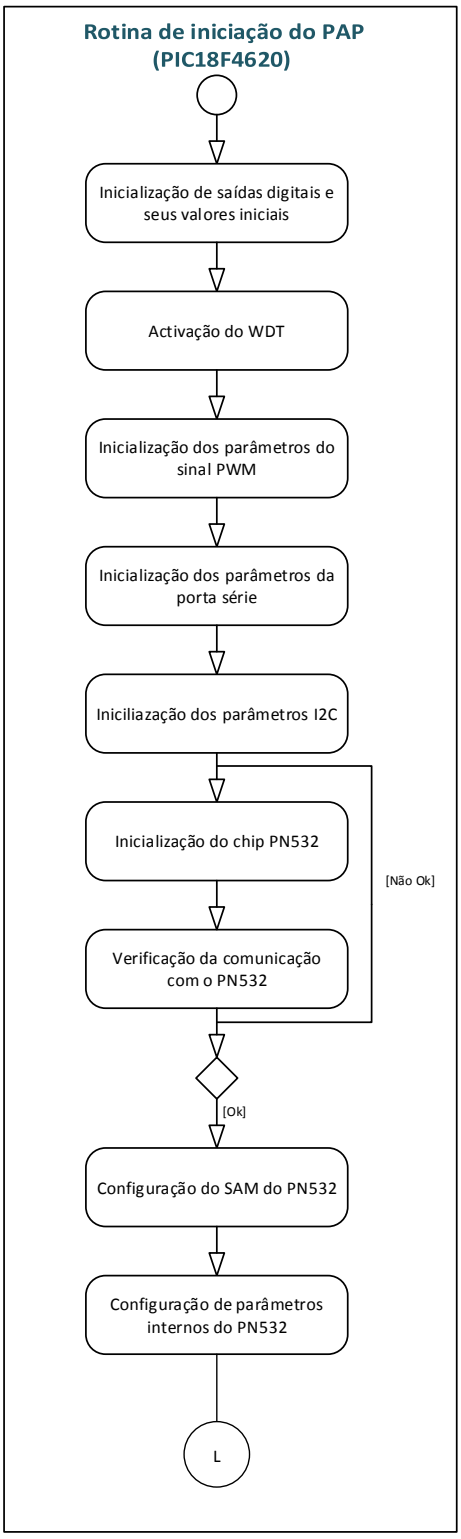



Figura 5.6: Diagrama de atividade representativo da inicialização do módulo PAP (rotina de configurações do microcontrolador)

- **Parâmetros de configuração adicionais**

  Ainda no mesmo contexto da operação anterior, é utilizado o comando *TgSetGeneralBytes*. Este é normalmente utilizado em combinação com o anterior, para fornecer dados ao *PN532* de qual informação deverá conter o comando *ATR-RES* (*Attrbute Response*). Esta mensagem é a resposta a um *Attribute Request* do dispositivo *initiator* que tem como objetivo constatar se deverá proceder a uma rotina de re-configuração de parâmetros internos de comunicação, para efeitos de compatibilidade posterior, com o dispositivo *target*. A troca de mensagens a este nível é gerida autonomamente entre os dispositivos de interação, embora o seu conteúdo tenha de ser especificado. Para melhor compreensão, aconselha-se à consulta do diagrama de atividade da página 21 da fonte referenciada em [96], e da página 158 da fonte referenciada em [95].

- **Troca de PDUs entre o "Leitor" e o Dispositivo Móvel**

  Neste estágio são trocados PDUs entre os *chip's* NFC de ambos os dispositivos, especificados no LLCP. Este protocolo já foi especificado no capítulo de NFC do estado da arte, mas de forma genérica, providencia os procedimentos de troca de dados entre dois dispositivos NFC.

  Para a implementação desta interação de comunicação, é simultaneamente necessária a consulta do manual de utilização do PN532 (páginas 160-165), e da especificação do LLCP. A documentação deste último está referenciada em [62].

  Como é entendido nesta fase, o controlo das operações do PN532 é feito através do microcontrolador, de tal forma, que é este é que gere e define as mensagens, e quando estas são enviadas. Este controlo é gerido no microcontrolador, com o *feedback* dos comandos enviados para o chip PN532. Para o pedido de reencaminhamento de PDUs para o dispositivo de aproximação, é utilizado o comando *TgSetData* (página 164 em [95]). É no campo "Data Out" desta mensagem que é inserida a PDU que se pretende reencaminhar. Por outro lado, para requisitar ao PN532, as PDUs por si recebidas do dispositivo iniciador, é utilizado o comando *TgGetData*.

  A Figura 5.7 apresenta sob a forma de diagrama de sequência, as interações necessárias (sob a forma de troca de PDUs), que o subsistema do PAP ($\mu$c + PN532) faz com o chip NFC do dispositivo móvel de aproximação. É importante referir que a interpretação do diagrama de sequência, prevê o entendimento do leitor, de que os comandos "*GetData*" e "*SetData*" são enviados do microcontrolador para o PN532 do PAP, e posteriormente por este geridos e comandados, e não, como a figura pode subentender - envio destes comandos diretamente de um *chip* para o outro. Da mesma forma, deve-se subentender de que todos os PDUs recebidos do lado do dispositivo NFC do PAP, são encapsulados numa mensagem I2C, e reencaminhados para o microcontrolador, para este prosseguir com o controlo e gestão da comunicação entre os dois dispositivos NFC. Caso a dinâmica entre os dispositivos NFC não seja a expectável, o algoritmo é direcionado para uma rotina de erro, e o algoritmo "Loop Funcional do PAP" é recomeçado.

  A comunicação segue a seguinte interação lógica:

1. Comando "getData()" que deve verificar o PDU de simetria (SYMM). Este PDU implementa simetria na comunicação sempre que não está disponível outro comando;
2. Comando "setData(SYMM)" para verificar o mesmo efeito, ciclicamente, até o microcontrolador receber do PN532 a notificação da receção da PDU CC (*Connection Request*).
3. Comando "setData(CC)" que corresponde à ordem de encaminhamento do $\mu$c para o PN532, para este último enviar a PDU CC (*Connection Complete*) - *acknowledge* ao CR (*Connection Request*).
4. Novamente deve ser implementado o ciclo de simetria entre os dispositivos, até à receção de uma PDU do tipo I (*Information*) vinda do dispositivo móvel de autenticação, que corresponde ao instante de tempo de envio da mensagem portadora da *password* de acesso (*beam* do utilizador). Este é o único tipo de PDU capaz de encapsular dados induzidos pelas aplicações e utilizadores, sendo todas as outras utilizadas para operações de controlo da comunicação.
5. Comando "setData(RR)" para pedido de reencaminhamento da PDU RR (*Receive Ready*) para o dispositivo NFC externo - *acknowledge* necessário, após receção de uma PDU do tipo *I*.
6. Ainda do lado do microcontrolador, é imediatamente enviado um pedido de reenvio da PDU recebida no PN532 (do PAP), pretendendo-se verificar uma PDU de simetria, que constata a confirmação da receção do lado do dispositivo móvel do PDU *RR*.
7. Finalmente, o microcontrolador comanda o *PN532* para requisitar o pedido de desconexão, através da PDU DISC (*Disconnect*).

- **Filtragem da *Password* do PDU de dados**

  Validada a comunicação, o microcontrolador filtra o campo de dados da resposta ao comando "getData(I)"; associa a *password* de acesso a um *array* de caracteres; e verifica a existência da mesma na EEPROM.

- **Sinalização Sonora de Erro/Validação**

  Em simultâneo com as três atividades abaixo descritas, é executada uma função, que ativa a porta e o sinal PWM pré-configurado, e o aplica sobre o *buzzer*. Caso seja, respetivamente, uma notificação de validação, ou não validação, o sinal apresenta duas cadências de ruído distintas.

- **Sinalização Visual de Erro/Validação**

  Na mesma circunstância da "atividade" acima, podem ser executados dois tipos de sinalização.

  1. *LED* verde pisca em caso de validação;
  2. *LED* vermelho pisca em caso de não validação.

- **Ativação da Fechadura**

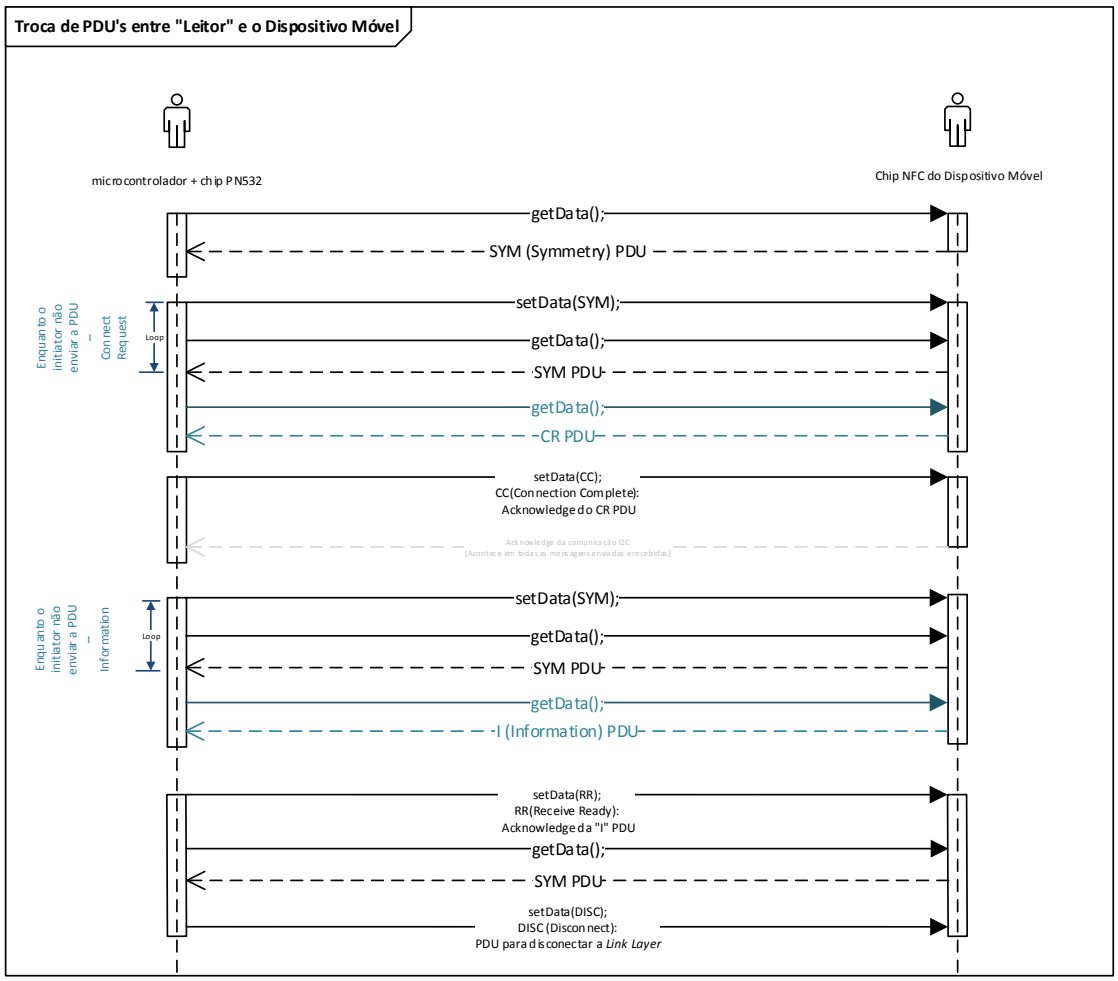



Figura 5.7: Diagrama de sequência dos PDUs trocados entre os dispositivos NFC

Caso o acesso tenha sido autenticado após a verificação da *password* de acesso, a fechadura é ativada por atuação do subsistema "transístor-relé", consequência, da ativação da saída digital do microcontrolador (já referida).

- **Envio de Dados de Acesso para o Computador Remoto**

  Se a *password* for validada, a fechadura é ativada, e é imediatamente enviado para o módulo central, para registo no histórico da base de dados, a *password* de acesso. Todos os dados registados adicionais são definidos pelo programa do módulo central.

O ponto de ligação "3" do diagrama de atividade da Figura 5.8 é meramente representativo, pelo que, a atividade por este representado não vai ser apresentado, pretendendo apenas demonstrar a continuação do processamento dos dados enviados do PAP no módulo central.

### 5.1.3 Módulo *XBee* - Dispositivo Final

Os módulos *XBee* vêm configurados de fábrica para operar no seu modo mais simples, enviando e recebendo dados pela porta série, bastando efetuar ligações em quatro pinos

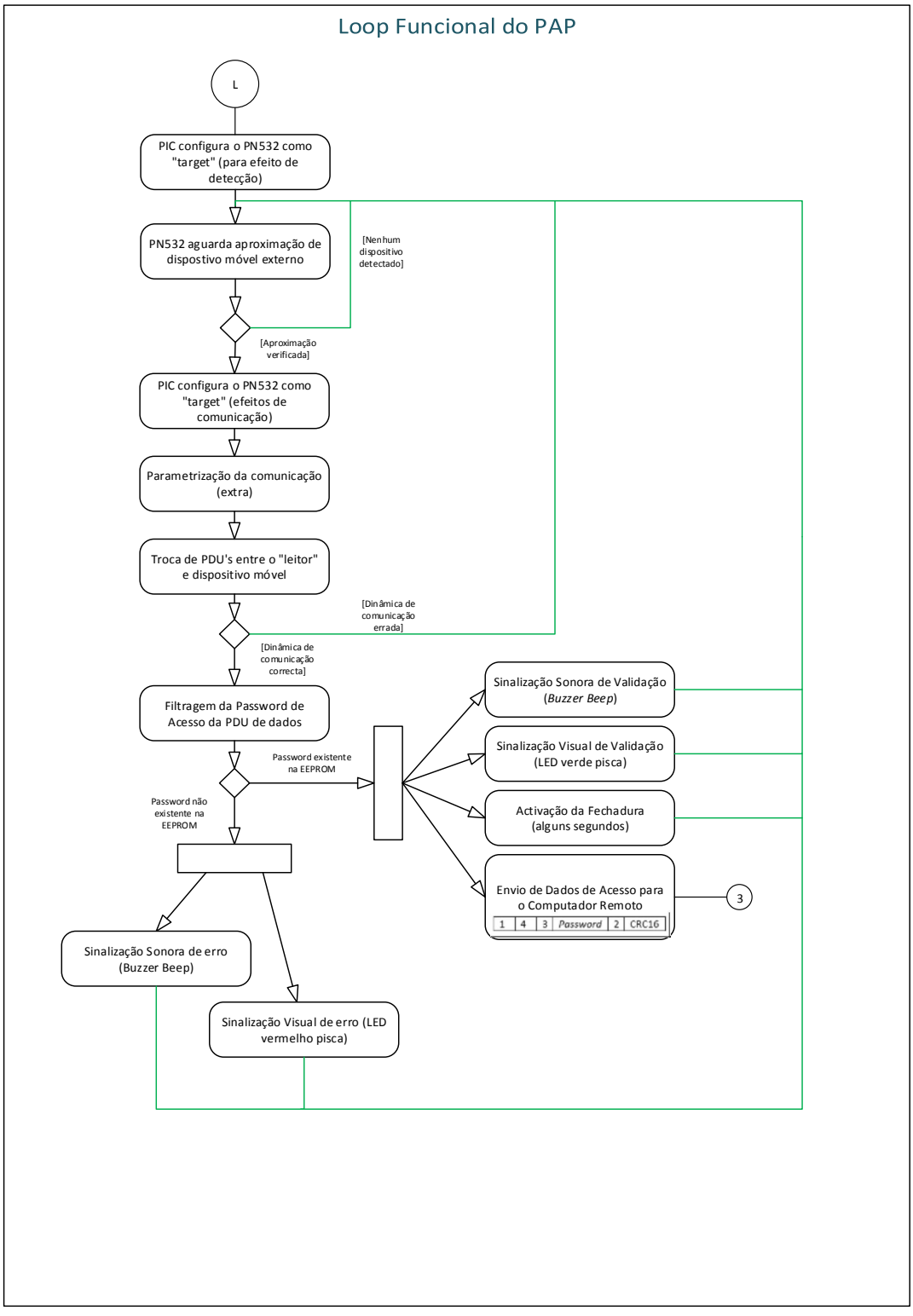



Figura 5.8: Diagrama de atividade do "Loop Funcional do PAP"

(*Ground (reference voltage)* (GND), *Power Supply* (Vcc), *Receive Line* (RX), *Transmission Line* (TX)). Para a implementação efetuada, é o suficiente em termos dos recursos que o módulo pode prover.

Para a configuração dos módulos, como referido anteriormente, foi utilizado o *software* de interface gráfica, disponibilizado pela Digi®- *X-CTU*. Este permite uma interação e facilidade enorme no processo de configuração dos módulos, sendo apenas necessário, conectá-los diretamente à porta série do computador, ou caso esta não exista, utilizar um adaptador de RS-232 para USB. Outra possibilidade de configuração é através da utilização de comandos *Hayes Command Set* (AT).

Todas as configurações efetuadas, e explicações abaixo efetuadas, têm como fonte a referência em [98].

Na Tabela 5.3, e enumeração abaixo representadas, estão descritos os principais parâmetros a configurar. Para uma consulta mais exaustiva dos comandos AT e respetiva descrição técnica associada aos módulos *XBee*, consultar a fonte referenciada em [99]

Tabela 5.3: Comandos necessários para configurar um módulo *XBee* [98]

| **Comando** | **Tipo** | **Descrição** |
|---|---|---|
| CH | R/W | Canal a utilizar |
| ID | R/W | Endereço de Rede |
| DH/DL | R/W | Endereço de destino (High/Low) |
| MY | R/W | Endereço do Módulo |
| NI | R/W | Nome do módulo na rede |
| BD | R/W | *Baud Rate* |
| NB | R/W | Paridade |
| D6 | R/W | Controlo de Fluxo (RTS) |
| D7 | R/W | Controlo de Fluxo (CTS) |
| DB | R/W | Força do sinal recebido |
| ND | R/W | Descobrir módulos ligados na rede |
| CN | W | Sair do modo de comando |
| RE | W | Repor as definições de fábrica |
| WR | W | Guardar as alterações feitas no módulo |

- **Definições de Rede**
  - ***Broadcast Hops* (BH)**
    O padrão *ZigBee* oferece a possibilidade de operar em vários canais. Para que dois ou mais módulos possam comunicar entre si estes devem operar no mesmo canal.
  - **ID**
    Este parâmetro define o PAN ID. Para que dois ou mais módulos comuniquem entre si na mesma rede sem interferir com redes vizinhas, este devem ter o mesmo PAN ID (deve ser diferente das outras redes).
  - ***Destination Address Low* (DL)/*Destination Address High* (DH)**
    Para que um módulo envie mensagens exclusivamente para outro módulo é necessário definir o endereço de destino da mensagem. O DH e o DL podem ser configurados de modo a que um módulo envie mensagens para um

único endereço. Caso se pretenda que um módulo envie mensagens para todos os módulos que partilham o mesmo PAN ID deve-se definir o DH=0 e o DL=0xFFFF.

- ***Unique Source Address* (MY)**

  Para que outros módulos possam enviar mensagens exclusivamente para um módulo é necessário que este tenha um endereço. O parâmetro MY permite definir o endereço do módulo. Caso se pretenda que o módulo receba mensagens de todos os módulos que partilham o mesmo PAN ID deve definir-se MY=0xFFFF.

- ***Node Identifier* (NI)**

  O parâmetro NI permite atribuir um nome ao módulo para que seja facilmente identificado na rede. O tamanho máximo está limitado a 20 caracteres.

- ***Node Discover* (ND)**

  Este parâmetro permite identificar todos os módulos que estão ligados em rede.

- **Definições da Comunicação RS-232**

  - **BD**

    Este parâmetro permite definir a taxa de transmissão de dados na comunicação.

  - ***Serial Parity* (NB)**

    Este parâmetro permite definir o tipo de paridade, ou simplesmente desativar a função.

  - ***DIO6 Configuration* (D6)**

    Ativar ou desativar o controlo de fluxo - *Request To Send* (RTS).

  - ***DIO7 Configuration* (D7)**

    Ativar ou desativar o controlo de fluxo - *Clear to Send* (CTS).

- **Definições de Configuração**

  - ***Restore Defaults* (RE)**

    Para repor as definições de fábrica sem ter que alterar todos os parâmetros, basta enviar este comando.

  - ***Write* (WR)**

    Para gravar no módulo as alterações efetuadas.

  - ***Exit Command Mode* (CN)**

    Para terminar o modo de comunicação AT.

Para o módulo presente no PAP definiram-se as seguintes configurações (Tabela 5.4):

Tabela 5.4: Configurações do módulo *XBee* do PAP

| Parâmetro | Valor |
|---|---|
| CH | C |
| ID | 1111 |
| MY | 1 |
| DH | 0 |
| DL | 0 |
| NI | ABC |
| BD | 3 (9600 bit/s) |
| NB | 0 (sem paridade) |
| D6 | 0 (sem controlo de fluxo) |
| D7 | 0 (sem controlo de fluxo) |

## 5.2 Módulo Central

Nesta secção é abordada a implementação do módulo central, explicando todos os aspetos funcionais do *software* criado, para interação com o utilizador. É especificado também, recorrendo a uma discrição maioritariamente por tópicos, o funcionamento interno do programa, incluindo a comunicação com a base de dados e o módulo de comunicação *wireless* XBee. A Figura 5.9 contém o esquema geral da conexão dos intervenientes deste módulo.

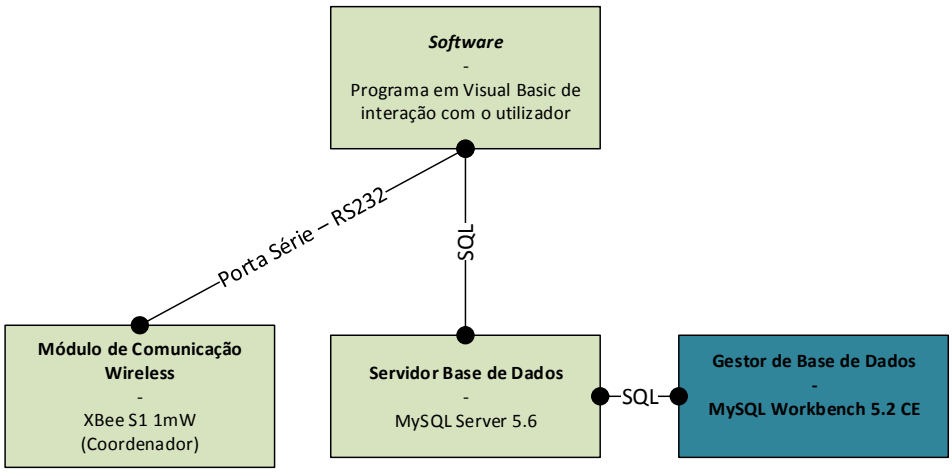



Figura 5.9: Esquema geral da conexão dos elementos do módulo central

### 5.2.1 Software

Esta sub-secção é inteiramente dedicada ao programa criado para interagir com o utilizador. Serão abordadas todas as suas principais rotinas internas, tipicamente associadas a eventos gerados pelo utilizador em interação com a interface gráfica. A forma como este interage com o módulo de comunicação *wireless*, e com o PAP, será também tratada. Nesta fase, aconselha-se à consulta do diagrama de sequência presente no Apêndice D, Figura D.1. Este prevê de forma simplificada, de como são processadas todos as ações que o utilizador pode praticar sobre o sistema.

#### 5.2.1.1 *Interface Gráfica*

Nesta secção, são apresentadas as janelas da interface de interação com o utilizador. São apontados as diversas funcionalidades e aspetos de cada uma, na seguinte enumeração:

1. **Janela de *Login* - Figura 5.10**

   Esta primeira janela da interface gráfica é constituída por um título de identificação do sistema, uma imagem representativa do modo de autenticação dos utilizadores, e quatro campos que devem ser devidamente preenchidos para os utilizadores terem acesso aos recursos do programa. Dois destes, consistem em campos de texto que devem ser preenchidos com o "Nome de Utilizador" e "Chave de Acesso", sendo nos restantes necessário, entre as possibilidades de duas lista de seleção, definir a porta COM de comunicação com o módulo de comunicação *wireless*, e caracterizar o tipo de utilizador como o mesmo foi registado no sistema (administrador, ou utilizador comum).


Figura 5.10: "*Form1*" VB, de autenticação

2. **Janela Geral de Interação com o Utilizador - Figura 5.11**

   Este ponto pretende apresentar os objetos imutáveis da interface, em qualquer uma das operações, ou *menus* selecionados, ou seja, elementos sempre visíveis independentemente da aba selecionada. No canto superior esquerdo foi adicionado o típico *menu* ficheiro, que possibilita sair do programa, ou fazer *Log Off* para a janela de interface de autenticação do programa. Abaixo, aparece o *container* "*Login Data*", que pretende providenciar de forma intuitiva, a consulta do utilizador, dos seus dados de acesso. Ainda, abaixo deste, outro *container*, denominado "*My Permissions*", que permite apresentar ao utilizador de forma equivalente as suas permissões. Na parte superior foi inserido o símbolo da universidade, e departamento em que foi desenvolvida esta implementação. No canto superior direito da janela, um botão e uma barra de progressão logo abaixo, que permitem respetivamente, abrir o

acesso físico durante alguns segundos (remotamente sem recurso a dispositivo móvel), e representar sob forma gráfica o decréscimo de tempo, até este ser novamente fechado.

(a) **Aba de Consulta de Histórico - Figura 5.11**

A aba de consulta de histórico, consiste numa sub-janela composta por um calendário de seleção de dias (máximo 8), uma lista de seleção com os nomes de utilizadores, e uma caixa de texto onde deverão aparecer os registos. Os dados são apresentados na caixa de texto de forma tabular, em linha com as *labbel's* de identificação dos campos de identificação dos registos, que surgem após seleção do utilizador e dias de consulta. Caso o utilizador não tenha permissão para consultar o histórico de outros, a lista de seleção fica impossibilitada e não visível.

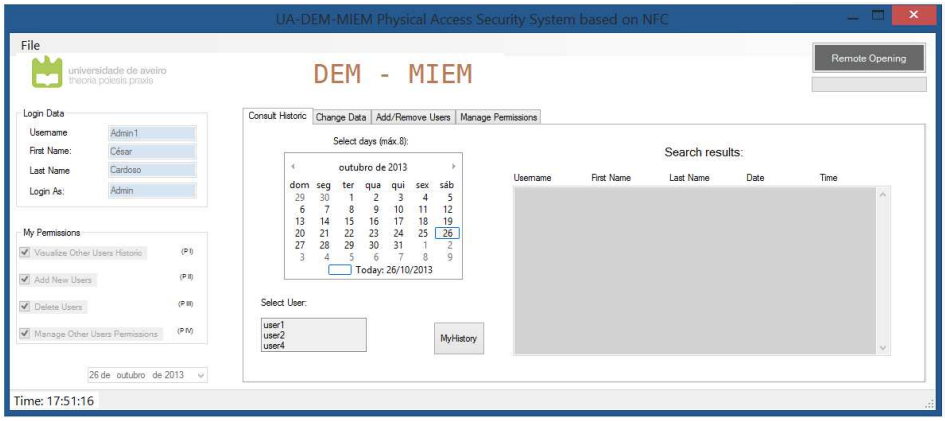



Figura 5.11: "*Form2*" VB, com a aba ativada, de consulta de histórico

(b) **Aba de Modificação de Dados de Utilizador - Figura 5.12**

A aba de mudança de dados de utilizador possibilita a alteração do "Nome de Utilizador", "*Password* de acesso no PAP", e "*Password* de autenticação no programa". Para cada registo de utilizador alterado é pressuposto a inserção do novo valor, e da bi-confirmação de um dos dados do utilizador autenticado.

(c) **Aba de Adicionar/Remover Utilizadores - Figura 5.13**

A aba que permite visualizar a interface de adição e remoção de utilizador está divida em dois *container's* independentes, respetivos a cada uma das operações. No *container* de adição de utilizadores é necessária a inserção dos seus dados identificativos - "*Username*/Nome de Utilizador", "*First Name*/Primeiro Nome", e "*Last Name*/Último Nome", em três caixas de texto para o efeito. Nas restantes quatro devem ser inseridas , com confirmação, as *Password's* respetivas ao acesso físico e ao programa. Finalmente, um botão para adicionar o registo à base de dados.

O *container* de remoção de utilizador é constituído por uma lista de seleção, onde deverá ser selecionado o utilizador a remover; duas caixas de texto que atualizam os seus valores com o nomes identificativos respetivos ao utilizador selecionado; e finalmente um botão para concluir a operação.

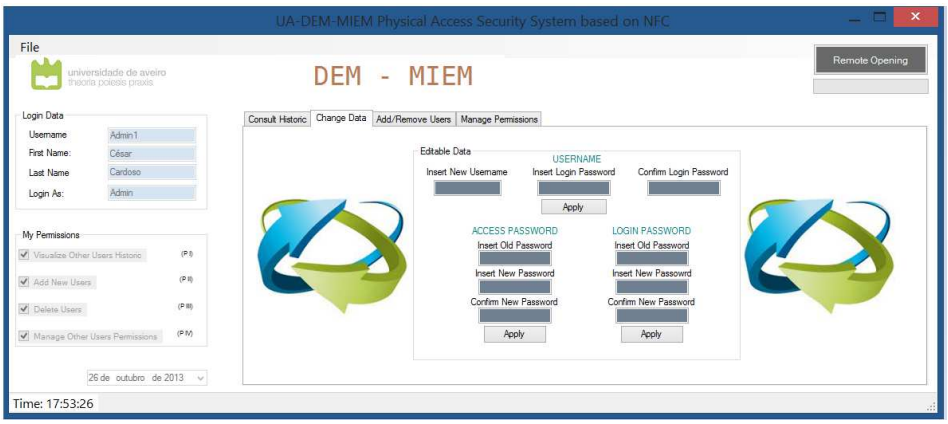



Figura 5.12: "*Form2*" VB, com a aba de modificação de dados do utilizador ativada

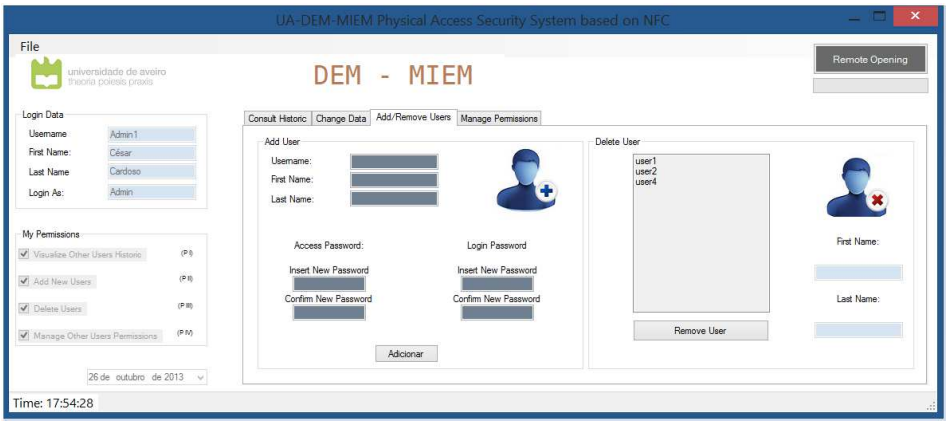



Figura 5.13: "*Form2*" VB de adicionar/remover utilizadores, com a aba ativada

(d) **Aba de Gerir Permissões - Figura 5.14**

Esta aba é constituída por três *container's* relacionados entre si. O primeiro contêm unicamente uma lista de seleção de utilizadores, ao qual se pretende alterar as permissões. O segundo, contêm duas caixas de texto, que automaticamente apresentam o nome de utilizador selecionado na lista anterior, e finalmente, um conjunto de quatro *check box's*, associadas às quatro permissões. O simples ato de validar ao não a *check box* de cada uma das permissões, após seleção do utilizador, atualiza automaticamente na base de dados o estado da permissão respetiva.

#### 5.2.1.2 Funcionamento

Nesta secção são explicados os algoritmos de funcionamento das principais rotinas do programa. Será feita uma breve explicação dos mesmos, de forma enumerada e sequencial equivalente ao funcionamento das rotinas.

- Autenticação no Programa

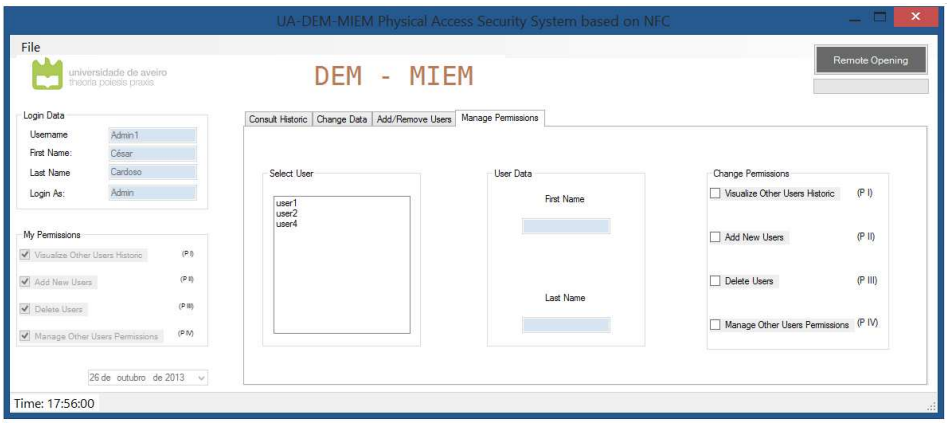



Figura 5.14: "*Form2*" VB de gerir permissões de utilizadores, com a aba ativada

1. O utilizador insere os campos necessários à sua autenticação e valida-os pressionando num botão para o efeito;
2. O programa verifica os campos de preenchimento, e caso alguns não estejam preenchidos gera uma mensagem de aviso;
3. O programa parametriza com os valores estáticos definidos, a porta COM, e abre-a. Caso o número da porta inserido pelo utilizador não seja o correto, é executada uma mensagem de aviso;
4. O programa inicia a conexão com o servidor base de dados, e verifica o *match* entre os dados de acesso do utilizador. Caso este não seja verificado, o utilizador é notificado através de uma mensagem de aviso. Se as credenciais estiverem corretas, o programa abre automaticamente a "*form*" de controlo e monitorização, com todos os recursos já apresentados.

- Abertura Remota do Acesso Físico

1. O utilizador pressiona o botão que executa os eventos para abertura de acesso físico;
2. O programa gera uma mensagem de verificação, que prevê a confirmação ou negação por parte do utilizador;
3. O programa encapsula a mensagem constituída pelos caracteres "1", "4", "4", "0", "0", "0", "0", "2", e envia-a pela porta série, para reencaminhamento da mensagem para o PAP;
4. O microcontrolador do PAP, recebe a mensagem, e processa-a numa função de interrupção, comandando de seguida a abertura da fechadura durante 4 segundos.

- Consultar Histórico

1. O utilizador seleciona o utilizador do qual pretende consultar o histórico;
2. O utilizador seleciona o dias, ou dias consecutivos (máximo 8), que pretende fazer leitura;

3. O programa regista em variáveis, o nome de utilizador e as datas de consulta pretendidas;
4. O programa abre a conexão ao servidor base de dados, e faz-lhe pedidos sobre a forma de *query's* SQL, associando as respostas em variáveis para o efeito;
5. O programa faz o *display* do *output* da base de dados na caixa de texto não editável.

- Alteração de Dados do Utilizador

1. Dependendo do dado de utilizador a modificar, o valor pretendido deve ser inserido, tal como a inserção de um elemento de garantia do utilizador (verificação se o utilizador autenticado é o mesmo que pretende praticar a alteração de dados), e confirmação desta. No caso da modificação das próprias chaves de acesso, deve ser inserida a antiga, a nova pretendida, e a confirmação desta última;
2. O programa verifica o preenchimento de todos os campos (mensagem de notificação em caso de inconformidade);
3. O programa verifica a igualdade entre os campos supostamente repetitivos (mensagem de notificação em caso de inconformidade);
4. O programa abre a conexão com o servidor de base de dados, e verifica a existência dos dados inseridos, e se estes se relacionam com o utilizador autenticado;
5. Caso validados os dados inseridos, o programa gera uma mensagem de confirmação da pretensão de alteração dos dados;
6. Caso validada a confirmação pelo utilizador, o programa inicia novamente a conexão à base de dados e procede com as alterações;
7. Caso o dado alterado seja a *password* de acesso ao PAP, o programa envia uma mensagem para o módulo *XBee*, através da porta série, para este proceder ao reencaminhamento da mensagem para o PAP. Esta recebida, o microcontrolador reescreve a *password* antiga, pela nova, na sua EEPROM.

- Adicionar Utilizador

1. O utilizador/administrador deve inserir todos os dados respetivos ao novo utilizador a inserir;
2. O programa verifica o preenchimento de todos os campos (mensagem de notificação em caso de inconformidade);
3. O programa verifica a igualdade entre os campos supostamente repetitivos (mensagem de notificação em caso de inconformidade);
4. Caso validados os dados inseridos, o programa gera uma mensagem de confirmação da pretensão de alteração dos dados;
5. Caso validada a confirmação pelo utilizador, o programa inicia novamente a conexão à base de dados e procede com a adição do novo utilizador;

6. O programa envia para a porta série uma mensagem para o módulo de comunicação *wireless* XBee, que este deve reencaminhar para o PAP, para adição das novas credenciais na sua EEPROM.

- Remover Utilizador

1. O utilizador deve escolher de uma lista de seleção, o utilizador a remover, e validar a operação carregando no botão para o efeito;
2. O programa gera uma mensagem de confirmação da pretensão de alteração dos dados;
3. Caso validada a confirmação pelo utilizador, o programa inicia novamente a conexão à base de dados e procede com a remoção do utilizador;
4. O programa envia uma mensagem para o PAP, por intermédio do módulo *XBee* coordenador, e este remove as credenciais deste utilizador.

- Gerir Permissões de Utilizadores

1. O utilizador deve escolher de uma lista de seleção, o utilizador a que pretende modificar o nível de permissões;
2. O programa atualiza as caixas de texto com o primeiro e segundo nome deste (melhor perceção dos utilizadores selecionados);
3. Sempre que o utilizador atuar sobre as *check box's*, é gerado um evento que atualiza os campos das permissões na base de dados do utilizador selecionado;

- *Thread's*

  São implementadas duas *thread's* distintas. Uma para atualização de listas de seleção, e outra para atualização dos dados de *login* do utilizador e suas permissões. O seu funcionamento é semelhante. Em *loop*, é constantemente feita uma verificação dos registos das bases de dados, e caso algum destes se altere, todos os campos são imediatamente atualizados.

### 5.2.2 Base de Dados

Como referido na solução proposta para a implementação, utilizou-se o serviço *MySQL*® para desenvolvimento da base de dados. Este utiliza a comum linguagem de base de dados, SQL. A linguagem SQL é dividida em subconjuntos de acordo com as operações que queremos efetuar sobre uma base de dados.

- **DML - Linguagem de Manipulação de Dados**

  *Data Manipulation Language* (DML) é um subconjunto da linguagem SQL que é utilizado para realizar inclusões, consultas, alterações e exclusões de dados presentes em registos. Estas tarefas podem ser executadas em vários registos de diversas tabelas ao mesmo tempo. Os comandos que realizam respetivamente as funções acima referidas são *Insert, Select, Update e Delete*.

- **DDL - Linguagem de Definição de Dados**

  O segundo grupo é a *Data Definition Language* (DDL). A DDL permite ao utilizador definir tabelas novas e elementos associados. A maioria das bases de dados de SQL comerciais tem extensões proprietárias no DDL. Os comandos principais são o *Create, Drop, e Alter*.

- **DCL - Linguagem de Controlo de Dados**

  O terceiro grupo é o *Data Control Language* (DCL). O DCL controla os aspetos de autorização de dados e licenças de utilizadores para controlar quem tem acesso para ver ou manipular dados dentro da base de dados. Os comandos principais são o *Grant, e Revoke*.

- **DTL - Linguagem de Transação de Dados**

  A *Data Transaction Language* (DTL) implementa a funcionalidade de transações. Estas permitem aprovar todas as modificações ou voltar ao estado inicial após as mesmas terem sido efetuadas, de forma facilitada. Isto garante a integridade da base de dados relativamente a falhas (não relacionais), pois quando dentro de uma operação complexa ou mesmo de apenas dois comandos, se houver alguma falha pode-se anular toda a operação, e voltar ao estado anterior com o comando *Rollback*, ou então se a operação ocorreu como pretendido, pode-se confirmar a operação com o comando *Commit*.

Destes quatro subconjuntos claramente o mais aplicado do lado do software foi o DML. Isto dever-se-á ao fato, de todo o processo de criação do esquema, tabelas, atributos, e outros, tenham sido efetuados por recurso ao gestor de interface gráfica MySQL Workbench®.

As operações efetuadas pelo *software* no que toca à comunicação com a base de dados, consistiram maioritariamente em:

- Definição dos objetos VB necessários à implementação da comunicação com a base de dados;

- Instanciação das conexões com a base de dados. Podia ter sido apenas utilizada uma, mas de forma a estruturar devidamente o código, definiram-se diferentes conexões para distintas operações, que necessitavam a atuação sobre o servidor SQL. Estas conexões foram criadas através do gestor "*Workbench*" e abertas e fechadas durante o processamento das operações para os quais foram definidas no programa VB, respetivamente, no ínicio e fim de cada uma destas;

- Aplicação de "queries" de consulta para apresentação do histórico de entradas com base nos *inputs* do utilizador;

- Aplicação de rotinas que implementam "queries" de consulta para atualização em tempo real dos dados de utilizador na aba lateral esquerda;

- Aplicação de "queries" de consulta para validação dos dados de *login* dos utilizadores/administradores;

- Aplicação de *queries* de atualização, remoção, ou inserção de registos nas operações de edição de dados de utilizador (*username*, *accessPassword*, ou *loginPassword*);
- Aplicação de *queries* de remoção, ou inserção de registos nas operações de adição ou remoção de utilizador;
- Aplicação de *queries* de atualização dos registos associados aos atributos das permissões dos utilizadores;
- Aplicação de *queries* nos campos de texto não editáveis, para atualização automática destes (nomeadamente atualização de *list box's* e os dados apresentados nos evento *onclick* na seleção de um dos seus elementos).

Nas Figuras 5.15, 5.16, 5.17 apresentam-se as tabelas aplicadas para a implementação da base de dados, onde podem ser consultados os atributos e alguns registos aplicados na fase de testes do protótipo. Estas tabelas são todas pertencentes a um único esquema.

| | Username | Pass_login | Pass_access | FirstName | LastName | P1 | P2 | P3 | P4 |
|---|---|---|---|---|---|---|---|---|---|
| ▶ | Admin1 | 1111 | 5555 | César | Cardoso | 1 | 1 | 1 | 1 |
| * | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL |

Figura 5.15: Tabela de administradores na base de dados, acedida pelo MySQL Workbench 5.2 CE

| | Username | Pass_Login | Pass_Access | FirstName | LastName | P1 | P2 | P3 | P4 |
|---|---|---|---|---|---|---|---|---|---|
| ▶ | user1 | 1111 | 1111 | A | A | 1 | 1 | 1 | 1 |
| | user2 | 2222 | 2222 | B | B | 0 | 0 | 0 | 0 |
| | user4 | 4444 | 4444 | D | D | 1 | 1 | 1 | 1 |
| * | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL | NULL |

Figura 5.16: Tabela de utilizadores na base de dados, acedida pelo MySQL Workbench 5.2 CE

| | Username | Data | Hora | n | FirstName | LastName |
|---|---|---|---|---|---|---|
| ▶ | user2 | 2013-07-09 | 16:45:38 | 107 | Rui | Bártolo |
| | user2 | 2013-07-09 | 16:46:18 | 108 | Rui | Bártolo |
| | cesar | 2013-07-18 | 21:51:00 | 109 | César | Cardoso |
| | cesar | 2013-07-18 | 21:51:37 | 110 | César | Cardoso |
| | cesar1 | 2013-07-18 | 21:52:40 | 111 | César | Cardoso |
| | user1 | 2013-07-18 | 21:55:48 | 112 | Tiago | Godinho |

Figura 5.17: Tabela de histórico na base de dados, acedida pelo MySQl Workbench 5.2 CE

### 5.2.3 Módulo *XBee* - Coordenador

No seguimento das explicações dadas na secção do módulo paralelo a este, definem-se apenas os parâmetros associados a este módulo (Tabela 5.5).

Tabela 5.5: Configurações do módulo *XBee* do módulo central

| **Parâmetro** | **Valor** |
|---|---|
| CH | C |
| ID | 1111 |
| MY | 0 |
| DH | 0 |
| DL | 1 |
| NI | CBA |
| BD | 3 (9600 bit/s) |
| NB | 0 (sem paridade) |
| D6 | 0 (sem controlo de fluxo) |
| D7 | 0 (sem controlo de fluxo) |

## 5.3 Dispositivo Móvel

Esta secção pretende explicar toda a implementação efetuada ao nível do dispositivo móvel, sendo especificado todo o funcionamento do programa e como este foi construído. No Anexo D, Figura C.3, é apresentado o diagrama de casos de uso, preparado com o intuito de elaborar os objetivos e funcionamento pretendido do programa.

### 5.3.1 Dispositivo de Desenvolvimento

O dispositivo móvel utilizado para a validação da aplicação foi o *Nexus* 4. Este é um produto da *Google*®, fabricado pela *LG*®. É um dispositivo com o SO Android®, com a versão 4.2 (*Jelly Bean*) disponibilizado no ato de compra, embora seja gratuitamente atualizável, até ao momento, com a versão 4.3. O *smarthphone* vem equipado com um *chip* NFC fabricado pela Broadcom®, deixando de adotar os anteriores *chip's* da *NXP*®que vinham a ser implementados (o mesmo que os dispositivos da *Samsung*®, e da placa utilizada nesta implementação). Esta particularidade foi também interessante, na perspetiva de validar os protocolos de comunicação em modo P2P, especificados pelo NFC Forum, entre *chips* diferentes (o que se veio a verificar).

### 5.3.2 Aplicação

Para o desenvolvimento da aplicação foi utilizado o *Eclipse IDE for Java Developers*, versão *Juno Service Release 2*. A escolha da sua utilização baseou-se no fato desta ser uma ferramenta altamente dotada para efeitos de *debug*, e simulação (*Android Virtual Device Manager*), para além, de permitir a consulta de documentação de uma forma bastante intuitiva. O fato, das atualizações das APIs ser feita de forma bastante empírica, é outro ponto bastante influente na decisão.

Esta aplicação implementa o uso de comunicação P2P, através do protocolo SNEP, especificado pelo NFC Forum. O intuito da sua especificação passou pela necessidade de uma definição concreta na forma de trocar mensagens NDEF, fazendo uso do protocolo

LLCP. É principalmente devido a esta normalização, que a implementação ao nível do subsistema "Dispositivo Móvel", foi validada em ambos os dispositivos testados, *Nexus 4* e *Samsung Galaxy SIII*.

#### 5.3.2.1 Interface Gráfica

Para o desenvolvimento da interface gráfica o *Android* disponibiliza duas formas distintas:

1. **Declarar os elementos de interface em *eXtensible Markup Language* (XML)**

   O Android possibilita um implementação de código XML de aplicação direta e simples, facilmente associável aos objetos das classes de elementos de visualização, como os *widget's* e *view's*.

2. **Instanciar os elementos do *layout* em tempo real (*runtime*)**

   A aplicação pode definir e instanciar as diferentes *activity's* e *view's*, e manipular as suas propriedades, com recurso a rotinas no programa.

O método utilizado para o desenvolvimento da interface gráfica foi a primeira opção, pela sua simplicidade de posicionar as diferentes *view's* num *layout* gráfico disponibilizado pelo *Eclipse*. A Figura 5.18 corresponde a uma captura de ecrã do dispositivo móvel utilizado, durante a utilização da aplicação em causa.

Para o desenvolvimento da interface foi apenas utilizada uma atividade, ou seja, uma janela única de objetos imutáveis. Esta contêm as seguintes *view's*[2]:

- ***ImageView***

  Imagem no canto superior esquerdo com o símbolo da Universidade de Aveiro.

- ***TextView's***

  - Texto identificativo do curso e departamento sobre o qual esta dissertação faz parte - "DEM - MIEM".
  - Texto identificativo posicionado junto à imagem da Universidade de Aveiro - "Universidade de Aveiro".
  - Texto de explicação, em tom discreto (cinza), com uma breve explicação de como deve ser utilizada a aplicação.
  - Texto identificativo do funcionamento do sistema global - "Access Control System Based on NFC".
  - Caixa de texto sem conteúdo, que é alterada, caso se verifique a inexistência de tecnologia NFC no dispositivo móvel Android - "NFC is not available on this device".

- ***EditText***

  Caixa de texto onde deverão ser inseridos todos os quatro caracteres de autenticação, associados à *password* no acesso físico.

[2]designação do *Android* aos objetos de interacção com os utilizadores, tais como, butões, caixas de texto, etc.

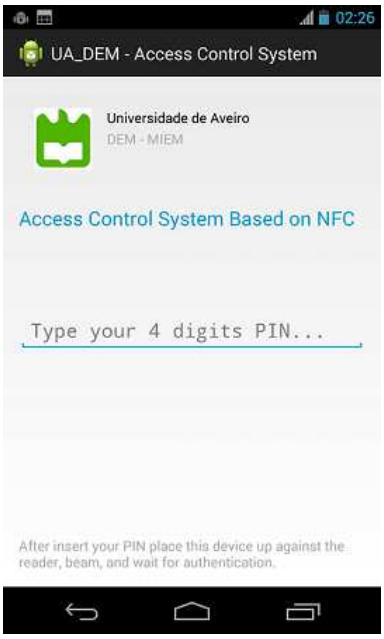



Figura 5.18: Janela de interface da aplicação Android desenvolvida

#### 5.3.2.2 Funcionamento

Para melhor compreensão aconselha-se à análise prévia do diagrama da Figura A.4, Apêndice A. Este representa os diferentes estados de uma atividade, tal como, através dos retângulos e balões ovais, respetivamente, as funções de chamada (*callback methods*) que são um recurso para efetuar operações entre diferentes estados da atividade, e os estados principais.

De seguida é explicada de forma breve e sequencial a estrutura do programa, embora o *script* seja maioritariamente constituído por funções de resposta a eventos, não apresentando a construção típica de um programa não orientado a objetos (programação estruturada).

- Declaração da classe principal *main*, onde são implementadas duas *interfaces*
  - Declaração dos objetos associados, a classes referentes, aos elementos da interface, definidos previamente por XML.
  - Instanciado objeto " mNfcAdapter", da classe *NfcAdapter* que representa o *chip* NFC local no dispositivo móvel.
  - Declaração de um *handler* para confirmação de envio de mensagem, após a operação de *beaming* do utilizador. Consiste numa mensagem *toast*[3], com o conteúdo "Message Sent".
- Definição do conteúdo da função *onCreate*. Esta função é chamada pelo sistema operativo quando a operação é aberta, e a atividade iniciada.

[3]mensagem de notificação do sistema operativo Android, que aparece durante alguns segundos na atividade em uso, desaparecendo de seguida.

  - Exposição do *layout* gráfico através da função *setContentView*;
  - Verificação da existência da tecnologia NFC no dispositivo móvel, através do método *getDefaultAdapter*, associado ao objeto *mNfcAdapter*. Caso não se verifique a sua existência a *textView* destinada para o efeito (já referida), é atualizada com a *string* "NFC is not available on this device";
  - registo das *callback's setNdefPushMessageCallback* e *setNdefPushCompleteCallback*, ambas associadas ao objeto *mNfcAdapter*.
    * **setNdefPushMessageCallback**
      Trata-se de uma *interface* da classe *android.nfc.NfcAdapter*. É uma função do tipo *callback* que é invocada quando outro dispositivo NFC capaz de comunicar em modo P2P, se aproxima até uma distância tal, onde a comunicação pode ser estabelecida.
    * **setNdefPushCompleteCallback**
      Trata-se de uma *interface* da classe *android.nfc.NfcAdapter*. É uma função do tipo *callback* que é invocada quando o dispositivo móvel é bem sucedido a enviar uma mensagem NDEF para outro dispositivo.

- Definição do conteúdo da função *onResume*. Esta função é chamada pelo sistema operativo quando a atividade é reaberta após pausa. Estamos perante uma situação de *onPause - onResume*, quando por exemplo, se interrompe a visualização de um vídeo no YouTube®, sob a forma de abrir outra atividade sem fechar a do *browser* em utilização. Como a atividade do *browser* não foi fechada, mas "sobreposta", logo que aberta, é o evento *onResume* que é iniciado e não o *onCreate*, permitindo assim, a continuação da visualização do *stream* de vídeo no momento interrompido.

  - Verificação de se a atividade se iniciou devido a um *Android Beam*. Caso se verifique a condição, é chamada uma função auxiliar que trata a mensagem;

- Definição da *callback onNdefPushComplete*, que recorre/chama o *handler* de notificação de mensagem enviada (já referido). Existe a necessidade de chamar um *handler*, ao invés de ser a própria *callback* a proceder com as respetivas operações, pois esta está associada a uma *binder thread*;

- Definição da *callback* "*createNdefMessage*" a ser invocada aquando a deteção de um dispositivo capaz de comunicar em modo P2P NFC, está dentro do raio de ação do dispositivo *initiator*. Portanto, é uma função controlada diretamente pelo SO Android®.

  Definiu-se a chamada de uma função auxiliar de construção do registo único, que compõem a mensagem NDEF. Depois do retorno do registo, todos os dados são encapsulados numa mensagem NDEF pronta para envio.

- Definição do método público "*NdefRecord createMime*", pertencente à classe *NdefRecord*, que codifica dados *Multipurpose Internet Mail Extensions* (MIME) em registos NDEF, como texto ou imagens *Joint Photographic Expert Group* (JPEG). Este método é chamado pela *callback* anterior, no momento em que o utilizador efetua uma operação de "*beam message*". Nesta função é definido que o registo MIME encapsulará nos campos respetivos de dados, os *bytes* associados à caixa de texto de inserção da *password* do acesso físico.

# Capítulo 6

# Considerações Finais

## 6.1 Conclusões

O trabalho realizado no âmbito desta dissertação assentou num pressuposto pouco comum, em que se considerou que seria interessante incorporar no seu processo um caráter de investigação, que permitisse atingir um nível de definição de objetivos, em que qualquer que estes fossem, seriam um contributo ao nível de sistemas de controlo de acessos.

Esta fase revelou-se temporalmente bastante dispendiosa, mas no limite considerou-se de suma importância, relativamente ao teor conclusivo atingindo, e na definição da solução proposta. Por este fato o título da dissertação aparenta alguma indefinição relativamente ao conteúdo do documento. Embora o mesmo pudesse induzir o leitor para os objetivos e implementação, respetivamente, definidos e caracterizados num ponto avançado da dissertação, o autor considerou que pelo processo global levado a cabo, numa perspetiva de valorização, de não só do trabalho implementado, mas também da investigação e revisão de todo o conceito que levaram ao mesmo, manter o título como representação de toda a demanda.

Durante a extensa pesquisa efetuada, apercebeu-se de que os sistemas de controlo de acessos, quer físicos, quer não físicos, atingiram um nível de funcionalidade bastante robusto, assentes numa grande variedade de mecanismos e tecnologias de suporte ao seu funcionamento. Esta diversidade está associada aos distintos elementos destes sistemas, desde ao conjunto, quase infindável, de tecnologias de identificação/autenticação (ou puramente mecanismos de acesso) aplicados, aos modelos de rede implementados ao nível de sistemas com multi-nós de acesso (os mais comuns) numa dada implantação, tipos de leitores, modelos de controlo de acessos aplicados, entre muitos outros funcionalismos. Assim, ainda na fase de definição de objetivos, concluiu-se de forma clara, que estes sistemas apresentam um versatilidade altíssima, associada a um flexibilidade forçada pelo mercado, induzida pelos mais distintos fatores (níveis de segurança exigidos; quantidade de constrangimentos dos sistemas a assegurar, quer ao nível das arquiteturas das implantações, quer ao nível dos modelos de gestão pretendidos pelas corporações; preço dos sistemas; etc.).

Desta forma considerou-se uma mais valia, e bastante válido, dada a conjuntura de crescente incorporação (centralização) de sistemas e serviços alheios a dispositivos móveis (até muito recentemente unicamente dedicados à intercomunicação entre pessoas, sob a forma de chamadas e mensagens escritas), aplicar e tentar validar a tecnologia NFC (tecnologia emergente como meio de autenticação), e comunicação *wireless* ZigBee (como

meio de comunicação entre os nós de acessos e o módulo gestor), como recursos base para a prototipagem de um sistema de controlo de acessos físicos, focado num mercado em aberto, destes para habitações comuns.

A partir daí, o trabalho foi-se desenvolvendo, apresar de por vezes conturbado pela complexidade da solução proposta, principalmente pela necessidade de domínio de conteúdos bastante distintos associados aos diferentes subsistemas, e genericamente alheios à área de formação do autor.

Relativamente ao NFC apresentaram-se sérias dificuldades, quer ao nível da montagem do hardware do circuito (por a placa de desenvolvimento ser desenhada como uma *shield* para acoplamento direto num Arduino UNO, implementando-se a comunicação I2C com esta, num microcontrolador PIC), quer ao nível da inexistência de bibliotecas de funções para comunicar com o microcontrolador aplicado. Por esta razão, a dada altura da dissertação, é definido como objetivo secundário e indispensável, o desenvolvimento de uma biblioteca de funções capazes de implementar a comunicação P2P entre o *chip* "leitor", e o *chip* de autenticação. Numa fase mais avançada, e claramente a mais complexa de todo o trabalho, foi a implementação da comunicação P2P entre os subsistemas (gestão e definição das mensagens). Esta fase requereu uma análise e estudo bastante moroso de alguns protocolos, que especificam o modo de operação utilizado. Destaca-se a fase mais crítica, como tendo sido a definição dos parâmetros de configuração do PN532 do leitor, como dispositivo alvo/*target*, e a gestão e troca de PDUs no momento de interação entre os dois *chips*.

O desenvolvimento da aplicação do módulo central em *Visual Basic*, foi realizada de forma bastante fluída, por se tratar de uma linguagem previamente conhecida pelo autor. Pode-se destacar a implementação de *thread's*, e a atuação sobre objetos instanciados por uma, noutra, o que apresentou algum caráter de novidade, e talvez por isso alguma complexidade. A implementação destes mecanismos baseou-se na necessidade de tornar o programa mais autónomo, permitindo a atualização de campos de *display* de informações genéricas, automaticamente. A comunicação com a base de dados e linguagem SQL também não foi muito exigente, embora, o facilitismo tenha sido, de alguma forma, induzido pela utilização do serviço *MySQL*, que permitiu elaborar algumas etapas de forma simplista. Todo o trabalho ao nível do dispositivo móvel, único e exclusivamente a aplicação, embora apresente um teor quantitativo menor, foi de enorme exigência. O autor necessitou de aprender os conceitos base de programação Java, classes de funções Android (e destas, as associadas ao NFC), métodos de gestão de uma "atividade" em sistema operativo *Android*, conhecimentos de criação de interface gráfica, instanciação-associação dos objetos relativos às "view's" definidas por XML, entre outros aspetos.

A programação do microcontrolador PIC não apresentou novidade, mas poder-se-á dizer que os algoritmos de gestão de todos os elementos controlados por este, e alguns parâmetros associados às comunicações tiveram de ser alterados, pela interferência que estes tinham nuns, quando ajustados para outros (destaca-se a definição da frequência do sinal de relógio adotado, como o principal). Outro aspeto, ainda ao nível do microcontrolador, que revelou algumas complicações não expectadas, foi a implementação da comunicação I2C com o PN532 (mais ao nível da gestão das tramas de receção, sua interpretação, e ação tomada com base nestas).

A implementação dos módulos XBee foi provavelmente a etapa mais simplista da implementação, bastando que para isso, se procedesse a uma configuração bastante interativa e simples, suportada pela boa documentação fornecida e material de suporte

existente.

No geral, toda implementação efetuada foi validada e todos os objetivos cumpridos. Relativamente à tecnologia NFC, esta apresentou ser solução como tecnologia de autenticação, destacando-se o fato de ser um meio para o efeito bastante prático e com taxas de erros (associadas à falha da comunicação, durante o estabelecimento desta, ou durante a troca de PDUs) baixas. Apesar de algumas das especificações do NFC Forum ainda estarem sob revisão, não foram detetados problemas associadas às mesmas, destacando-se o fato de terem sido ensaiados dois dispositivos móveis distintos (com *chips* NFC de marca diferentes), e ambos terem validado a aplicação. Destaque-se talvez, a perceção do autor de que, o dispositivo móvel com o chip NFC do mesmo fabricante do chip do leitor, apresentou menor taxas de erros. Porém, a maior parte dos ensaios foram efetuados com este contido numa capa de proteção de plástico flexível, enquanto o dispositivo utilizado durante todo o desenvolvimento da implementação (com chip NFC da Broadcom - fabricante diferente do chip do "leitor") com uma capa rígida de plástico (possivelmente maior interferência). Como desvantagem a este modo de autenticação, detetou-se o fato, de pressupor um conjunto de procedimentos, que embora simples, possam levar alguns segundos, ao contrário, do simples ato de aproximação de um cartão de proximidade, que fornecendo o seu ID, rapidamente valida o acesso(na maioria das vezes com o utilizador em movimento). Por outro lado, o conjunto de procedimentos, sob a forma de etapas de um algoritmo que se deve fazer cumprir, este protótipo apresenta um padrão de segurança bastante fiável. Quer isto dizer, que no limite para uma autenticação num dado acesso, ilícita, é necessário estar provido de um dispositivo com tecnologias NFC, ter a aplicação em causa, conhecer a password, e o acesso correspondente. Além disso, esta tecnologia wireless é praticamente impossível, pelo seu carácter de comunicação de curta distância, de sofrer ataques que se baseiem em interceção de sinais, e ainda, pelo modo de operação P2P bidirecional, permitir elaborar as mais distintas dinâmicas de comunicação(e.g. elaborar um algoritmo inteligente de autenticação, por exemplo, baseado na autenticação anterior).

Finalmente, destacar o valor induzido para o autor após realização desta dissertação, quer pela satisfação própria de ter conseguido implementar toda a solução proposta, e por no processo, ter adquirido conhecimentos quase absolutos nalguns tópicos em que apresentava desconhecimento considerável.

## 6.2 Trabalhos Futuros

Como o promotor do ciclo *Plan-Do-Check-Act* (PDCA), Dr. W. Edwards Deming, acreditava, e consagrou que todo e qualquer processo ou produto, são infindavelmente passíveis de sofrerem melhoria, também o autor desta dissertação, acredita e propõem as seguintes propostas, para que estas mesmas, pós-implementadas, possam ser objeto de verificação e crítica, fomentando novas propostas e soluções de otimização.

1. Redução de consumo energético, do módulo PAP, aplicando os mecanismos já existentes do microcontrolador aplicado, e do chip *PN532*;

2. Otimização da comunicação P2P entre os dispositivos NFC, visando o aumento de rapidez do mecanismo de decisão no momento de autenticação(no microcontrolador);

3. Elaboração de uma rotina que verifique ambos os estados dos sub-módulos (ligado ou desligado), para que cada um destes, no pedido de ordens para o sistema "paralelo", possam em caso de um se apresentar indisponível, deixar a operação pendente, processando-a na próxima vez que o sistema visado se encontre capaz de processar a ordem;

4. Fazer estudo comparativo entre os dois modos operação NFC, aplicáveis para funções de autenticação, P2P e modo de emulação;

5. Implementar a aplicação móvel em dispositivos de sistema operativo distinto ao aplicado nesta implementação (Symbian®, iOS®, etc.);

6. Implementação de um modelo de controlo de acessos, com base num existente, ou de modelo proposto completamente distinto(preferencialmente com um carácter simplista), no *software* de interação do módulo central;

7. Explorar mecanismos dos dispositivos móveis como recurso de autenticação. Por exemplo, explorar a possibilidade, de aplicar os mecanismos de reconhecimento facial do sistema operativo *Android* com base na análise das imagens recolhidas pela câmara, e com base num possível *template* recolhido, enviar uma mensagem estruturada relatva ao mesmo (por NFC, como meio de autenticação). Esta proposta assenta no fato das tecnologias biométricas serem tipicamente dispendiosas.

8. Desenvolvimento de um servidor *WEB*, com características similares ao programa do módulo central desenvolvido, que permita operar o sistema remotamente;

9. Implementação ao nível do PAP, de um sistema anexo, que permita este ser energéticamente autónomo;

# Bibliografia


[1] MEYERS', Mike - **CISSP(R) Certification Passport**. 1ª ed. California: Brandon A.Nordin, Outubro 17, 2002. ISBN-13: 978-0072225785. Capítulo 2, pág.29-32.

[2] SANDHU, R.S., SAMARATI, P. - **Access control: principle and practice**, Communications Magazine, IEEE , vol.32, no.9, pág.40,48, Setembro 1994

[3] MOREIRA, Pedro Alexandre - **Gestão de Controlo de Acessos**. Porto: Faculdade de Engenharia da Universidade do Porto, 2008. Dissertação de Mestrado em Engenharia Electrotécnica e de Computadores.

[4] [autor desconhecido] - **What is Multifactor or Strong Authentication Software?** [on-line]. Citado em 2013-03-21. Disponível em: <`http://veritrix.com/multifactor-authentication/`>.

[5] GRANCE, Timothy; STEVENS, Marc; MYERS, Marissa - **Guide to Selecting Information Technology Security Products** - *Recommendations of the National Institute of Standards and Technology.* Gaithersburg: *National Institute of Standards and Technology*, Outubro 2003. *NIST Special Publication 800-36 - Computer Security Division.*

[6] United States Regulatory Commission - **Access Control Systems - Technical Information for NRC Licensees**. NUREG-1964: *Office of Nuclear Security and Incident Response.*

[7] CHAPPLE, Mike. **Multifactor Authentication Made Simple** [on-line]. 15 de Dezembro, 2011. Citado em 2013-03-08. Disponível em: <`http://www.biztechmagazine.com/article/2011/12/multifactor-authentication-made-simple`>.

[8] LUPU, C.; LUPU, V. - **Multimodal Biometrics for Access Control in an Intelligent Car**. *Computational Intelligence and Intelligent Informatics*, 2007. *ISCIII '07. International Symposium.* pág.261,267, 28-30 Março 2007

[9] MERKERT, R. J. - **Smart Cards and Biometrics in Physical Access Control Systems**. *Biometric Consortium 2005 Conference. SCM Microsystems, 2005.*

[10] [autor desconhecido] - **What are Access Control Models?** [on-line]. Terça-feira, 28 de Julho, 2010 às 11:48. Citado em 2013-03-08. Disponível em: <`http://www.computer-network-security-training.com/what-are-access-control-models`>.

[11] SOUZA, Marcos Tork - **Controle de Acesso para Sistemas Distribuídos**. São Paulo: Escola Politécnica de São Paulo, 2010. Dissertação de Mestrado em Engenharia de Computação.

[12] SALTZER, J. H.; SCHROEDER, M. D.. **The Protection of Information in Computer Systems. In Proceedings of the IEEE**, Vol. 63, N. 9. (1975), pág. 1278-1308.

[13] BLAZE, Matt - **Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks**. AT&T Labs - Research: 15 de Setembro 2002 (Revisão: 2 Março 2003).

[14] [autor desconhecido] - **What is MagnePrint®** [on-line]. Citado em 2013-03-14. Disponível em: <`http://www.magneprint.com/`>.

[15] [autor desconhecido] - **Magnetic Stripe Card Standards** [on-line]. Citado em 2013-05-12]. Disponível em: <`http://www.ded.co.uk/magnetic-stripe-card-standards/`>.

[16] ZALUD, Bill - **Smart Cards: More or 'Less'**. Security: Solutions for Enterprise Security Leaders; Junho 2008, Vol. 45 *Issue* 6, pág.80.

[17] smartcardbasics - **Types of Smart Card: Contact Cards** [on-line]. Citado em 2013-05-12. Disponível em: <`http://www.smartcardbasics.com/smart-card-types.html`>.

[18] HU, Vincent C.; FERRAIOLO, David F.; KUHN, D. Rick - **Assessment of Access Control Systems**. Gaithersburg: *National Institute of Standards and Technology, Septembro 2006. Interagency Report 7316 - Computer Security Division.*

[19] STANLEY, P.; JEBERSON, W.; KLINSEGA, V. V. - **"Biometric Authentication: A Trustworthy Technology for Improved Authentication"**. *Future Networks, 2009 International Conference em pp.171,175, 7-9 Março 2009*

[20] SEMEANO, Pedro Nuno Extreia Ribeiro - **Programa de Controlo de Acessos com Configuração de Regras em XML**. Lisboa: Universidade Nova de Lisboa - Faculdade de Ciência e Tecnologia, 2009. Dissertação de Mestrado em Engenharia Electrotécnica.

[21] PEDROSA, Felipe Negreiros; HEMERLY, Elder Moreira - **Autenticação de Impressões Digitais**. Brasil:[s.l.] ,Instituto Tecnológico de Aeronáutica [data desconhecida].

[22] GORANIN, N.; CENYS, A. - **Evolutionary Algoriths Application Analysis in Biometric Systems**. *Information Security Laboratory, Department of Information Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University Sauletekio al. 11, SRL-I-415, LT-10223, Vilnius, Lithuania. Journal of Engineering Science and Technology Review 3 (1) (2010) 70-79 - Received 19 February 2010; Accepted 13 March 2010.*

[23] SUKHAI, N. B. - **Access Control & Biometrics**. *InfoSecCD Conference*, 8 de Outubro de 2004, Kennesaw, GA, USA. ACM, 2004.

[24] [autor desconhecido] - **Forensic Implications of Identity Management Systems**. FIDIS Consortium,2006.

[25] WU,Wenhai; LU,Feiyuan; CHENG,Guojian; SHI,Caiyun. **A Vein Based Biometric Experiment and Some New Developments**. Intelligent Systems (GCIS), 2012 Third Global Congress on , vol., no., pp.131,135, 6-8 Nov. 2012

[26] LI,Xi; LIU,Xiangbin; LIU,Zhicheng. **A dorsal hand vein pattern recognition algorithm**. Image and Signal Processing (CISP), 2010 3rd International Congress on , vol.4, no., pp.1723,1726, 16-18 Oct. 2010

[27] HARTUNG, D.; OLSEN, M.A.; XU,Haiyun; BUSCH, C.. **Spectral minutiae for vein pattern recognition**. Biometrics (IJCB), 2011 International Joint Conference on , vol., no., pp.1,7, 11-13 Oct. 2011

[28] Subcommittee of Biometrics. **Iris Recognition**. National Science and Technology Council (INSTC) - Committee of Technology: Committee of Homeland and National Security

[29] Chia-Te Chou; Sheng-Wen Shih; Wen-Shiung Chen; Victor W. Cheng; Duan-Yu Chen - **Non-Orthogonal View Iris Recognition System**. IEEE Transactions On Circuits And Systems For Video Technology, Vol. 20, N. 3, Março 2010.

[30] DAUGMAN,J. - **High confidence visual recognition of persons by a test of statistical independence**.IEEE Trans. Pattern Anal. Mach. Intell.,vol. 15, n. 11, pág. 1148-1161, Nov. 1993.

[31] DAS, Ravi - **Retinal Recognition - Biometric Technology in Practice**.*Keesing Journal of Documents* & Identity, 22, 2007.

[32] KINNUNEN,Tomi; LIB,Haizhou - **An Overview of Text-Independent Speaker Recognition: from Features to Supervectors**. Department of Computer Science and Statistics, Speech and Image Processing Unit & Department of Human Language Technology, Institute for Infocomm Research.

[33] MYERS,Lisa - **An Exploration of Voice Biometrics**. *GSEC Practical Assignment* versão 1.4b Opção 1. Data de submissão: Segunda-Feira, 19 de Abril, de 2004.

[34] BioPassword® - Security,Software,Science - **Authentication Solutions Through Keystroke Dynamics**. BioPassword Whitepaper.

[35] NISO RFID Working Group - **RFID in U.S. Libraries**. Baltimore: A Recommended Practice of the National Information Standards Organization. Dezembro de 2007. ISBN (13): 978-1-880124-75-8

[36] VIOLINO, Bob - **A Summary of RFID Standards** RFID Journal®[on-line]. Citado em 2013-07-09. Disponível em: <`http://www.rfidjournal.com/articles/view?1335/`>.

[37] [autor desconhecido] - **ISO RFID Standards: A Complete List** [on-line]. Terça-Feira, 13 de Março, de 2012 às 11:18. Citado em 2013-07-09. Disponível em: <`http://rfid.net/basics/rfid-basics/186-iso-rfid-standards-a-complete-list-`>.

[38] [autor desconhecido] - **RFID Standards 101** [on-line]. Terça Feira, 13 Março 2012 às 11:17. Citado em 2013-07-09. Disponível em: <http://rfid.net/basics/rfid-basics/196-rfid-standards-101->.

[39] ScienceProg® - **How does RFID tag technology works** [on-line]. 16 de Outubro, 2007. Citado em 2013-07-09. Disponível em: <http://www.scienceprog.com/how-does-rfid-tag-technology-works/>.

[40] HarlandSimon® - **RFID Tagging Technology** [on-line]. Citado em 2013-07-09. Disponível em: <http://www.harlandsimon.com/RF_Tags.php>.

[41] CAVOUKIAN, Ann - **Mobile Near Field Communications(NFC) "Tap ´n Go" Keep it Secure & Private**. Canada, Ontario: Information and Privacy Commissioner.

[42] Innovision Research & Technology®- **Near Field Communication in the real world - Turning the NFC promise into profitable, everyday applications** .

[43] "pranav"(*nickname*) - **5 Ways Near Field Communication (NFC) will revolutionize our lives.** [on-line]. 26. Novembro de 2011 às 18:42. Citado em 2013-07-20. Disponível em: <http://gm.kochar.com/post/5-ways-near-field-communication-(nfc)-will-revolutionize-our-lives.aspx>.

[44] [autor desconhecido] - *NFC Forum*® [on-line]. Citado em 2013-07-09. Disponível em: <http://www.nfc-forum.org/>.

[45] Forum.Nokia® - **Introduction to NFC**. 19 de Abril de 2011. Versão 1.0.

[46] BILGINER, Bekir; LJUNGGREN, Paul-Luis - **An introduction to Near Field Communication**. Março de 2011.

[47] Nokia Developer® - **Inside NFC: Usages and Working Principles**[on-line]. Citado em 2013-07-10. Disponível em: <http://developer.nokia.com/Community/Wiki/Inside_NFC:_Usages_and_Working_Principles>.

[48] Nokia® - **Review: Nokia 700, part 2: Camera, Multimedia and NFC**[on-line]. Citado em 2013-07-09. Disponível em: <http://www.allaboutsymbian.com/reviews/item/13512_Nokia_700_part_2_Camera_Multim.php>.

[49] BISHOP, Todd - **Microsoft Tag adding support for QR codes and NFC, says it sees room for alternatives**[on-line].13 de Dezembro de 2011 às 6:04. Citado em 2013-07-09. Disponível em: <http://www.geekwire.com/2011/microsoft-tag-adding-qr-nfc-support-barcode-scanning-apps/>.

[50] ZALOKER, Joseph - **Near Field Communication(NFC)**.

[51] *Smart Card Alliance*® - **NFC Frequently Asked Questions**[on-line]. Citado em 2013-07-19. Disponível em: <http://www.smartcardalliance.org/pages/publications-nfc-frequently-asked-questions#7>.

[52] RAJANNA, Vijay - **Tap to Pair, to Share and to Pay - NFC Let's Unlock The World**[on-line].22 de Setembro de 2011. Citado em 2013-07-19. Disponível em: <http://www.codeproject.com/Articles/258268/Tap-to-Pair-to-Share-and-to-Pay-NFC-Lets-Unlock-Th>.

[53] SASLIS, Giorgos - **What is NFC? - Definition Near-Field Communications**[on-line].Terça-Feira, 5 de Abril de 2011. Citado em 2013-07-19. Disponível em: <http://www.mobile-marketing-blog.net/2011/04/what-is-nfc-definition-near-field.html>.

[54] "th"(*nickname*). **NFC Makes Simple Connection Between Gadget**[on-line]. Citado em 2013-07-19. Disponível em: <http://allinonegadget.blogspot.pt/2011/11/nfc-makes-simple-connection-between.html>.

[55] KIM, J.H. - **Secure Element, Key to Absolute Power?**[on-line]. Citado em 2013-07-19. Disponível em: <http://www.windblazer.pe.kr/wordpress/index.php/2011/03/24/secure-element-key-to-absolute-power/>.

[56] CHANDLER, Nathan - **What is Android Beam?**[on-line]. Citado em 2013-07-22. Disponível em: <http://electronics.howstuffworks.com/android-beam.htm>.

[57] RICKER, Thomas - **Android 0-click NFC sharing demonstrated in Ice Cream Sandwich (video)**[on-line]. 11 de Maio de 2011 à 01:45. Citado em 2013-07-22. Disponível em: <http://www.engadget.com/2011/05/11/android-0-click-nfc-sharing-demonstrated-in-ice-cream-sandwich/>.

[58] Symphony-Teleca® - (Stephan) - **NFC:caught between hype and compromise**.

[59] NFCtags.com® - **How to Select the Right NFC Tag**[on-line]. Citado em 2013-08-23. Disponível em: <http://www.nfctags.com/nfc-applications-which-tag>.

[60] Innovision Research & Technology® - **Near Field Communication in the real world - Using the right NFC tag type for the right NFC application**.

[61] CardWerk - Smarter Card Solutions® - **ISO 7816 Part 1: Physical Charcteristics of Integrated Circuit Cards**[on-line]. Citado em 2013-08-23. Disponível em: <http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-1.aspx>.

[62] *NFC Forum* - **LLCP - Technical Specification**. Versão 1.1. 2011-06-20.

[63] [autor desconhecido] - **Security PACE Book 6 - Basic Access Control Concepts**[on-line].Citado em 2013-08-22. Disponível em: <http://www.simplexgrinnell.com/SiteCollectionDocuments/Training/PACEBook6.pdf>.

[68] [autor desconhecido] - **Security Access Control System Basic Elements and Architecture**[on-line].[citado em 2013-08-22]. Disponível em: <http://en.wikipedia.org/wiki/Access_control>.

[65] System I/O- Inc.® - **Security Access Control System Basic Elements and Architecture**[on-line]. Citado em 2013-08-22. Disponível em: <http://www.systems-io.com/AccessControl.html>.

[66] GALLEN, Dennis - **Access Control Systems - Technology Review: Review of door entry systems and integration with IP cameras** [on-line].Citado em 2013-08-22. Disponível em: <http://www.imakenews.com/kin2/e_article001411581.cfm?x=b8v5FDQ,b25tl0b3,w>.

[67] Sunbelt: Gated Access Systems® - **Frequently Asked Questions: Access Control Systems, Modern System Designs**[on-line]. Citado em 2013-08-22. Disponível em: <http://www.sunbeltsys.com/faq/Access%20Ctrl%20FAQs/acs_faq_3.htm>.

[68] OCOM® - **Access Control Systems Topologies**[on-line].2011-08-23. Citado em 2013-08-22. Disponível em: <http://www.ocom.cn/en/Technical_page_479.html>.

[69] [autor desconhecido] - **PHYSICAL SECURITY DOMAIN**, Presentation with CBK Review.[on-line]. Citado em 2013-08-22. Disponível em: <http://www.slideshare.net/amiable_indian/physical-security-domain>.

[70] JACKSON, Chris - **Network Security Auditing**. Cisco Press: 2 de Junho de 2010. Print ISBN-13: 978-1-58705-3528; Web ISBN-13: 978-1-58705-940-7.

[71] ALMEIDA, João C.S.C.B. - **Novo Sistema de Rastreabilidade Industrial**. Aveiro: Universidade de Aveiro, 2012. Dissertação de Mestrado em Engenharia de Automação Industrial.

[79] National Instruments® - **A Quick Comparison of RS-232, RS-422, and RS-485 Serial Communication Interfaces**[on-line]. Citado em 2013-09-01. Disponível em: <http://digital.ni.com/public.nsf/allkb/2CABB3FD5CAF2F8686256F1D005AD0CD>.

[73] SANTOS, José P. - **PROTOCOLO DE COMUNICAÇÃO SÉRIE EIA232**. Aveiro: Universidade de Aveiro - Informática Industrial(2010/2011).

[74] [autor desconhecido] - **Interfaces for Use with ALE (Computer to Radio), DB9 Connector RS-232 Pinout**[on-line]. Citado em 2013-09-02. Disponível em: <http://hflink.com/interface/>.

[75] KRON Medidores®. **Conceitos Básicos de RS-485 e RS-422**

[76] SANTOS, José P. - **PROTOCOLO DE COMUNICAÇÃO SÉRIE EIA485**. Aveiro: Universidade de Aveiro - Informática Industrial(2010/2011).

[77] FRENZEL, Lou - **Transceivers Bring New Life To RS-485 And RS-422 Networks**[on-line]. Citado em 2013-09-10. Disponível em: <http://electronicdesign.com/lighting/transceivers-bring-new-life-rs-485-and-rs-422-networks>.

[78] SANTOS, José P. - **PROTOCOLO DE COMUNICAÇÃO MODBUS**. Aveiro: Universidade de Aveiro - Informática Industrial(2010/2011).

[79] Javvin® - Network management & security - **Ethernet: IEEE 802.3 Local Area Network (LAN) protocols**[on-line]. Citado em 2013-09-20. Disponível em: <http://www.javvin.com/protocolEthernet.html>.

[80] SANTOS, José P. - **Capítulo 8: IP - INTERNET PROTOCOL**. Aveiro: Universidade de Aveiro - Informática Industrial(2010/2011).

[81] VASQUES, Bruna; COUTINHO, Igor; LIMA, Manuela; CARNEVAL, Vitor - **ZigBee**. Brasil: Universidade Federal do Rio de Janeiro - Departamento de Engenharia Eletrônica e de Computação (Redes de Computadores I - 2010.1)[on-line]. Citado em 2013-09-30. Disponível em: <http://www.gta.ufrj.br/grad/10_1/zigbee/index.html>.

[82] SRM Technologies - *Embedded360*. **WIRELESS PAN - ZigBee** [on-line]. Citado em 2013-10-01. Disponível em: <http://www.embedded360.com/wireless_pan/zigbee.htm>.

[83] SANKARANARAYANAN, Dinakaran - **Understanding the Technology Hype Cycle** [on-line]. 3 de Setembro de 2012. Citado em 2013-10-22. Disponível em: <http://socialmediatoday.com/dinakaranonline/774531/understanding-technology-hype-cycle>.

[84] GARTNER® - **Hype Cycles** [on-line]. Citado em 2013-10-22. Disponível em: <http://www.gartner.com/technology/research/methodologies/hype-cycles.jsp>.

[85] User: "admin" - **ABI expects NFC to come out of the trial phase next year**.29 de Novembro de 2012 [on-line]. Citado em 2013-10-22. Disponível em: <http://mobile-web.me/abi-expects-nfc-to-come-out-of-the-trial-phase-next-year/>.

[86] ABI Research® - **NFC Mobile Payment Transaction Spend to Hit the $100 billion Mark in 2016**. 18 de Outubro de 2012 [on-line]. Citado em 2013-10-22. Disponível em: <https://www.abiresearch.com/press/nfc-mobile-payment-transaction-spend-to-hit-the-10>.

[87] Ip Carrier® - **A chronicle of business model change and end user transformation in the global communications industry** [on-line]. Citado em 2013-10-22. Disponível em: <http://ipcarrier.blogspot.pt/2012/10/nfc-mobile-payment-transaction-spend-to.html>.

[88] *IHS(iSuppli)®* - REBELLO, Jagdish - **US Wireless Carriers Partner with Big Credit Card Companies, Boosting Cell Phone NFC Market** [on-line]. 12 de Maio de 2011. Citado em 2013-10-22. Disponível em: <http://www.isuppli.com/mobile-and-wireless-communications/news/pages/us-wireless-carriers-partner-with-big-credit-card-companies-boosting-cell-phone-nfc-market.aspx>.

[89] *Microchip*® - **PIC18F4620** [on-line]. Citado em 2013-10-24. Disponível em: <http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010304>.

[90] *Microchip*® - **PIC18F2525/2620/4525/4620 Data Sheet 28/40/44-Pin Enhanced Flash Microcontrollers with 10-Bit A/D and nanoWatt Technology** [on-line]. Citado em 2013-10-24. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/39626e.pdf>.

[91] *Adafruit*® - **Adafruit PN532 Brekout Schematic** [on-line]. Citado em 2013-10-24. Disponível em: <http://www.adafruit.com/datasheets/PN532_Breakout_Schematic_v1.0.pdf>.

[92] *Digee*® - **Solutions and Specifications** [on-line]. Citado em 2013-10-24. Disponível em: <http://www.digi.com/pdf/chart_xbee_rf_features.pdf>.

[93] *Adafruit*® - ***Adafruit PN532 NFC/RFID Controller Shield for Arduino + Extras***[on-line]. Citado em 2013-10-24. Disponível em: <http://www.adafruit.com/products/789>.

[94] *Microchip*® - ***PIC DEM 2 PLUS Schematics*** [on-line]. Citado em 2013-10-24. Disponível em: <http://ww1.microchip.com/downloads/en/DeviceDoc/Pages%20from%2014-00504-1R5.pdf>.

[95] *NXP*® - ***UM0701-02 PN532 - User Manual Rev.02*** [on-line]. Citado em 2013-10-24. Disponível em: <http://www.nxp.com/documents/user_manual/141520.pdf>.

[96] *ECMA Internation*® - ***Near Field Communication - Interface and Protocol (NFCIP-1) 3ºEdition*** [on-line]. Junho, 2014. Citado em 2013-10-24. Disponível em: <http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf>.

[97] *Android*® - ***Ativity Class*** [on-line]. Citado em 2013-11-01]. Disponível em: <http://developer.android.com/reference/android/app/Activity.html>.

[98] SANTOS, José P. - **COMUNICAÇÃO SÉRIE Rs232 através de módulos XBee.**. Aveiro: Universidade de Aveiro - Tecnologias de Accionamento e Comando(2009/2010).

[99] *Digi*® - ***XBee Command ReferenceTables*** [on-line]. Citado em 2013-11-10. Disponível em: <http://examples.digi.com/wp-content/uploads/2012/07/XBee_ZB_ZigBee_AT_Commands.pdf>.

# Apêndice A

# *Material de Suporte*

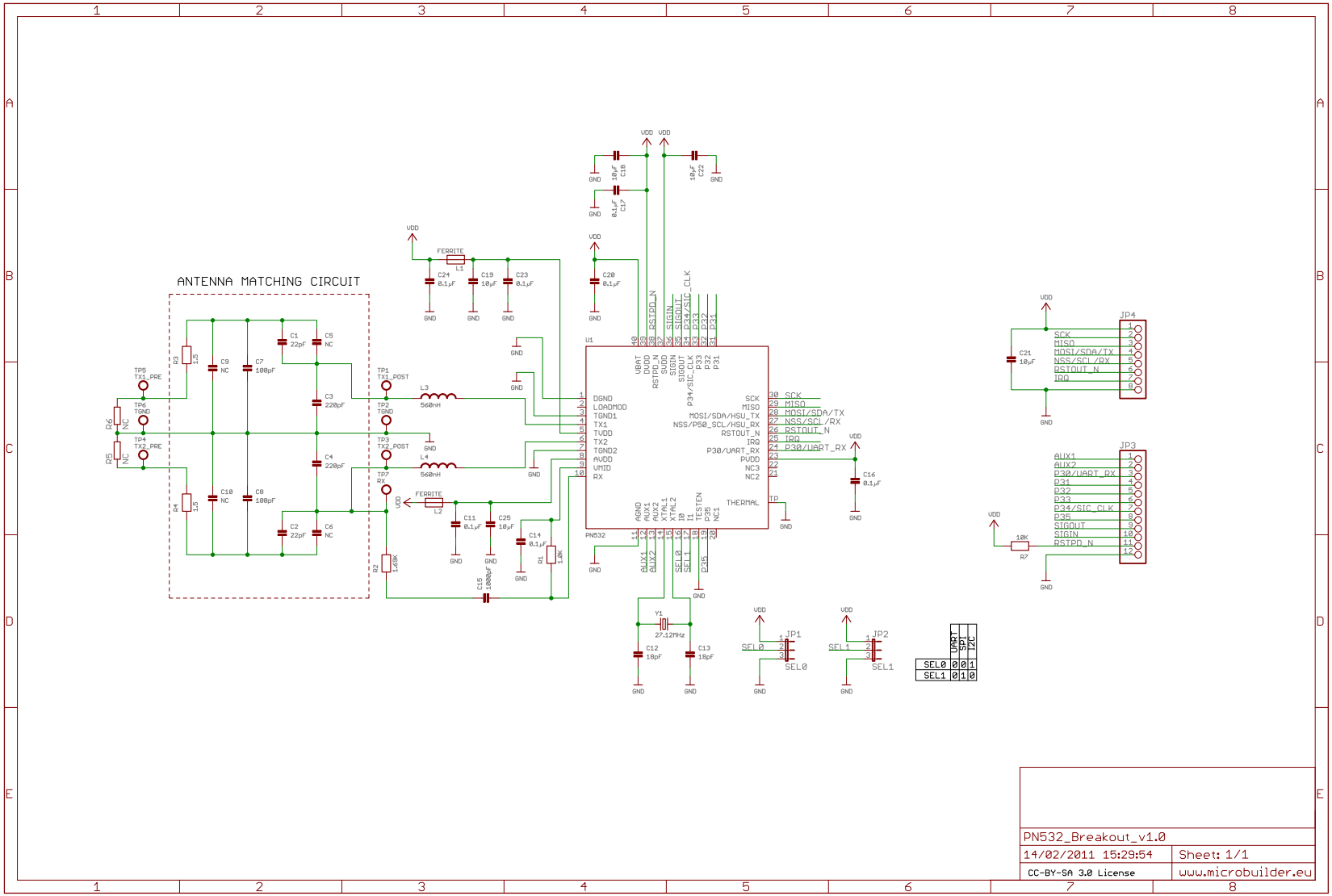
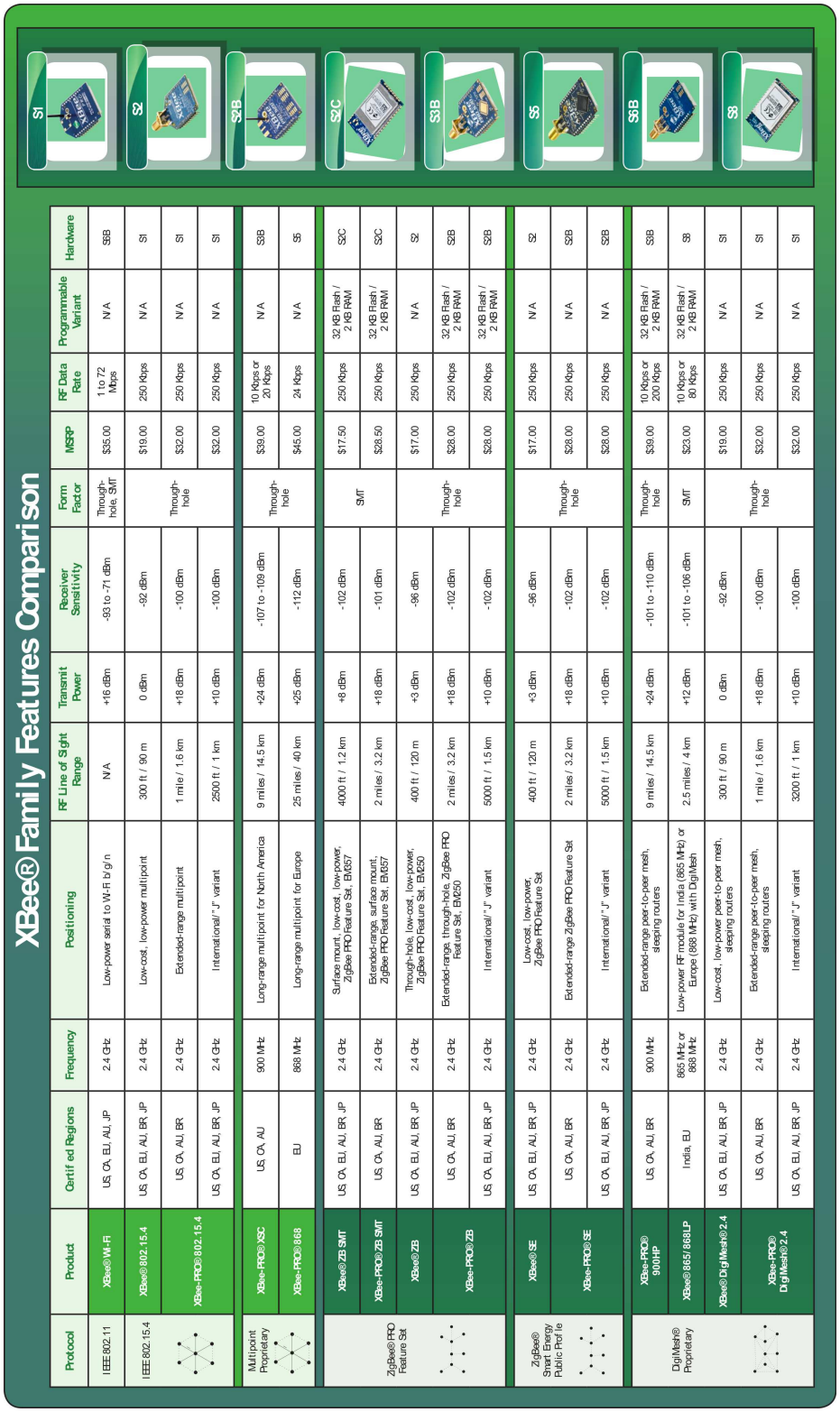



Figura A.1: Esquemático da placa NFC utilizada - *PN532 Breakout Schematic v1* [91]




| Protocol | Product | Certified Regions | Frequency | Positioning | RF Line of Sight Range | Transmit Power | Receiver Sensitivity | Form Factor | MSRP | RF Data Rate | Programmable Variant | Hardware |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IEEE 802.11 | XBee® Wi-Fi | US, CA, EU, AU, JP | 2.4 GHz | Low-power serial to Wi-Fi b/g/n | N/A | +16 dBm | -93 to -71 dBm | Through-hole, SMT | $35.00 | 1 to 72 Mbps | N/A | S6B |
| IEEE 802.15.4 | XBee® 802.15.4 | US, CA, EU, AU, BR, JP | 2.4 GHz | Low-cost, low-power multipoint | 300 ft / 90 m | 0 dBm | -92 dBm | Through-hole | $19.00 | 250 Kbps | N/A | S1 |
| | XBee-PRO® 802.15.4 | US, CA, AU, BR | 2.4 GHz | Extended-range multipoint | 1 mile / 1.6 km | +18 dBm | -100 dBm | | $32.00 | 250 Kbps | N/A | S1 |
| | | US, CA, EU, AU, BR, JP | 2.4 GHz | International/"J" variant | 2500 ft / 1 km | +10 dBm | -100 dBm | | $32.00 | 250 Kbps | N/A | S1 |
| Multipoint Proprietary | XBee-PRO® XSC | US, CA, AU | 900 MHz | Long-range multipoint for North America | 9 miles / 14.5 km | +24 dBm | -107 to -109 dBm | Through-hole | $39.00 | 10 Kbps or 20 Kbps | N/A | S2B |
| | XBee-PRO® 868 | EU | 868 MHz | Long-range multipoint for Europe | 25 miles / 40 km | +25 dBm | -112 dBm | | $45.00 | 24 Kbps | N/A | S5 |
| ZigBee® PRO Feature Set | XBee® ZB SMT | US, CA, EU, AU, BR, JP | 2.4 GHz | Surface mount, low-cost, low-power, ZigBee PRO Feature Set, EM357 | 4000 ft / 1.2 km | +8 dBm | -102 dBm | SMT | $17.50 | 250 Kbps | 32 KB Flash / 2 KB RAM | S2C |
| | XBee-PRO® ZB SMT | US, CA, AU, BR | 2.4 GHz | Extended-range, surface mount, ZigBee PRO Feature Set, EM357 | 2 miles / 3.2 km | +18 dBm | -101 dBm | | $28.50 | 250 Kbps | 32 KB Flash / 2 KB RAM | S2C |
| | XBee® ZB | US, CA, EU, AU, BR, JP | 2.4 GHz | Through-hole, low-cost, low-power, ZigBee PRO Feature Set, EM250 | 400 ft / 120 m | +3 dBm | -96 dBm | Through-hole | $17.00 | 250 Kbps | N/A | S2 |
| | XBee-PRO® ZB | US, CA, AU, BR | 2.4 GHz | Extended-range, through-hole, ZigBee PRO Feature Set, EM250 | 2 miles / 3.2 km | +18 dBm | -102 dBm | | $28.00 | 250 Kbps | 32 KB Flash / 2 KB RAM | S2B |
| | | US, CA, EU, AU, BR, JP | 2.4 GHz | International/"J" variant | 5000 ft / 1.5 km | +10 dBm | -102 dBm | | $28.00 | 250 Kbps | 32 KB Flash / 2 KB RAM | S2B |
| ZigBee® Smart Energy Public Profile | XBee® SE | US, CA, EU, AU, BR, JP | 2.4 GHz | Low-cost, low-power, ZigBee PRO Feature Set | 400 ft / 120 m | +3 dBm | -96 dBm | Through-hole | $17.00 | 250 Kbps | N/A | S2 |
| | XBee-PRO® SE | US, CA, AU, BR | 2.4 GHz | Extended-range ZigBee PRO Feature Set | 2 miles / 3.2 km | +18 dBm | -102 dBm | | $28.00 | 250 Kbps | N/A | S2B |
| | | US, CA, EU, AU, BR, JP | 2.4 GHz | International/"J" variant | 5000 ft / 1.5 km | +10 dBm | -102 dBm | | $28.00 | 250 Kbps | N/A | S2B |
| DigiMesh® Proprietary | XBee-PRO® 900HP | US, CA, AU, BR | 900 MHz | Extended-range peer-to-peer mesh, sleeping routers | 9 miles / 14.5 km | +24 dBm | -101 to -110 dBm | Through-hole | $39.00 | 10 Kbps or 200 Kbps | 32 KB Flash / 2 KB RAM | S3B |
| | XBee® 865/868LP | India, EU | 865 MHz or 868 MHz | Low-power RF module for India (865 MHz) or Europe (868 MHz) with DigiMesh | 2.5 miles / 4 km | +12 dBm | -101 to -106 dBm | SMT | $23.00 | 10 Kbps or 80 Kbps | 32 KB Flash / 2 KB RAM | S8 |
| | XBee® DigiMesh® 2.4 | US, CA, EU, AU, BR, JP | 2.4 GHz | Low-cost, low-power peer-to-peer mesh, sleeping routers | 300 ft / 90 m | 0 dBm | -92 dBm | | $19.00 | 250 Kbps | N/A | S1 |
| | XBee-PRO® DigiMesh® 2.4 | US, CA, AU, BR | 2.4 GHz | Extended-range peer-to-peer mesh, sleeping routers | 1 mile / 1.6 km | +18 dBm | -100 dBm | Through-hole | $32.00 | 250 Kbps | N/A | S1 |
| | | US, CA, EU, AU, BR, JP | 2.4 GHz | International/"J" variant | 3200 ft / 1 km | +10 dBm | -100 dBm | | $32.00 | 250 Kbps | N/A | S1 |

Figura A.2: Tabela com soluções XBee® e especificações respetivas [92]

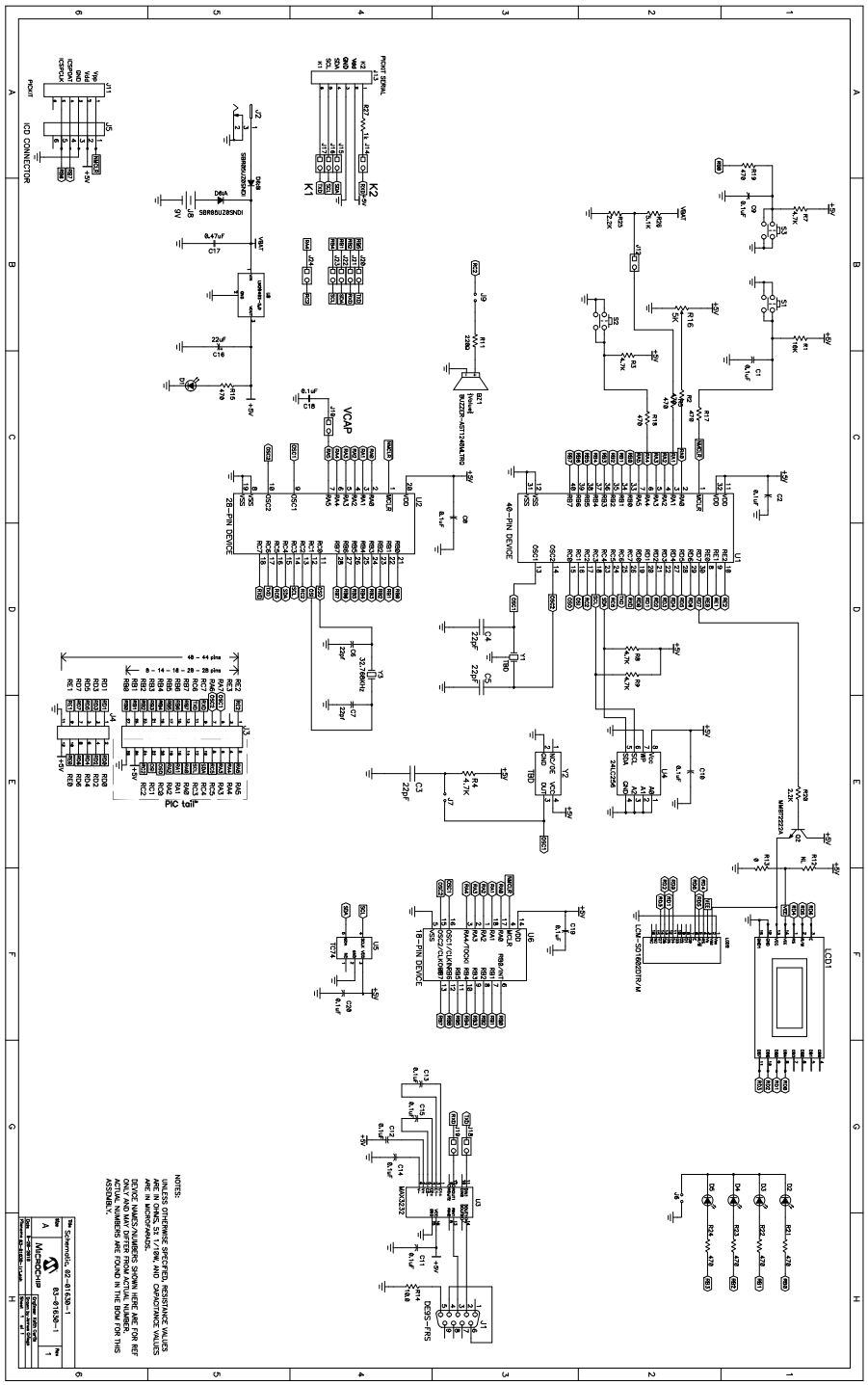


Figura A.3: Esquema elétrico da PIC DEM 2 PLUS - placa de desenvolvimento da Microchip [94]

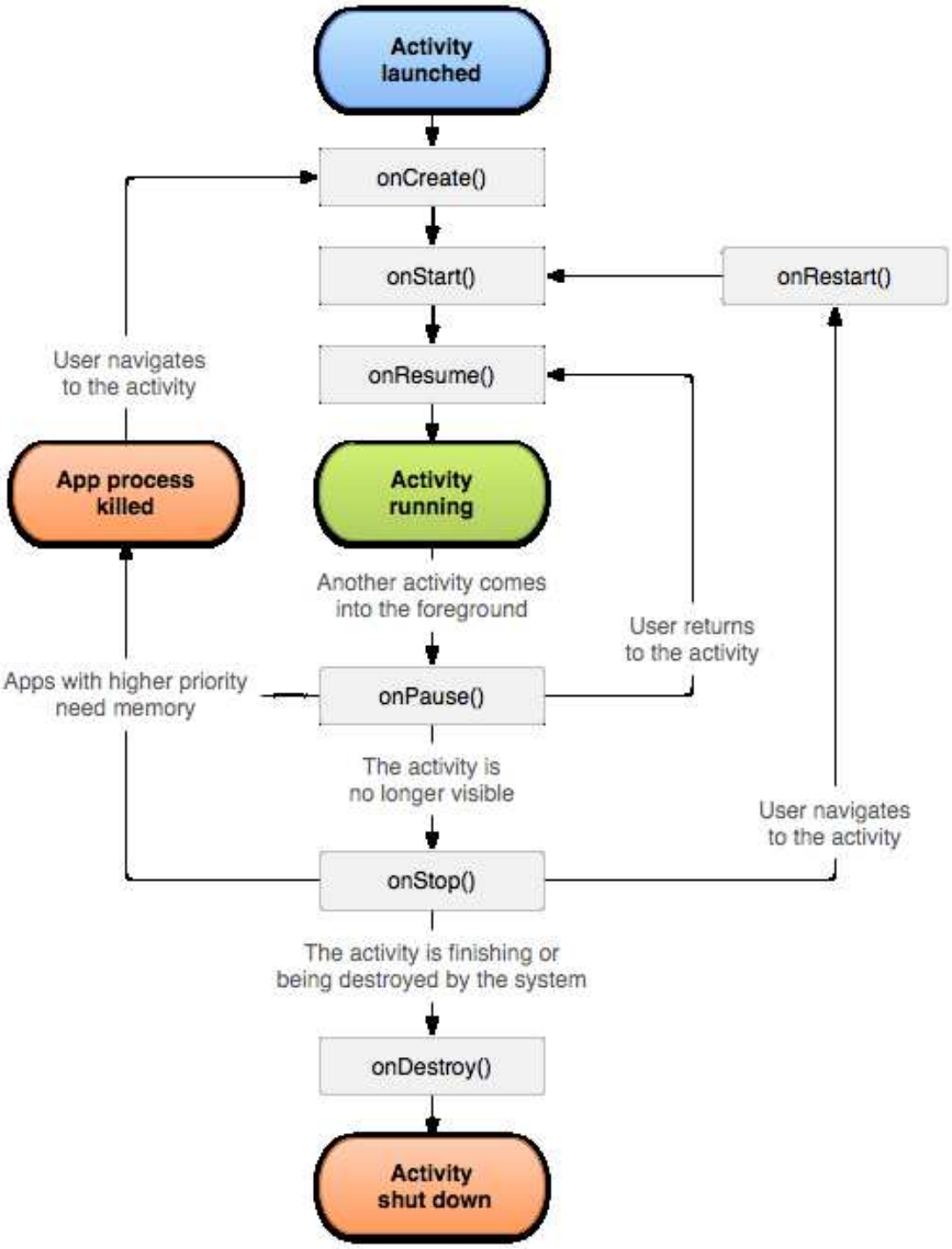



Figura A.4: Ciclo de vida, e funcionamento, de uma atividade *Android* [97]

Apêndice B

# Esquemas Elétricos

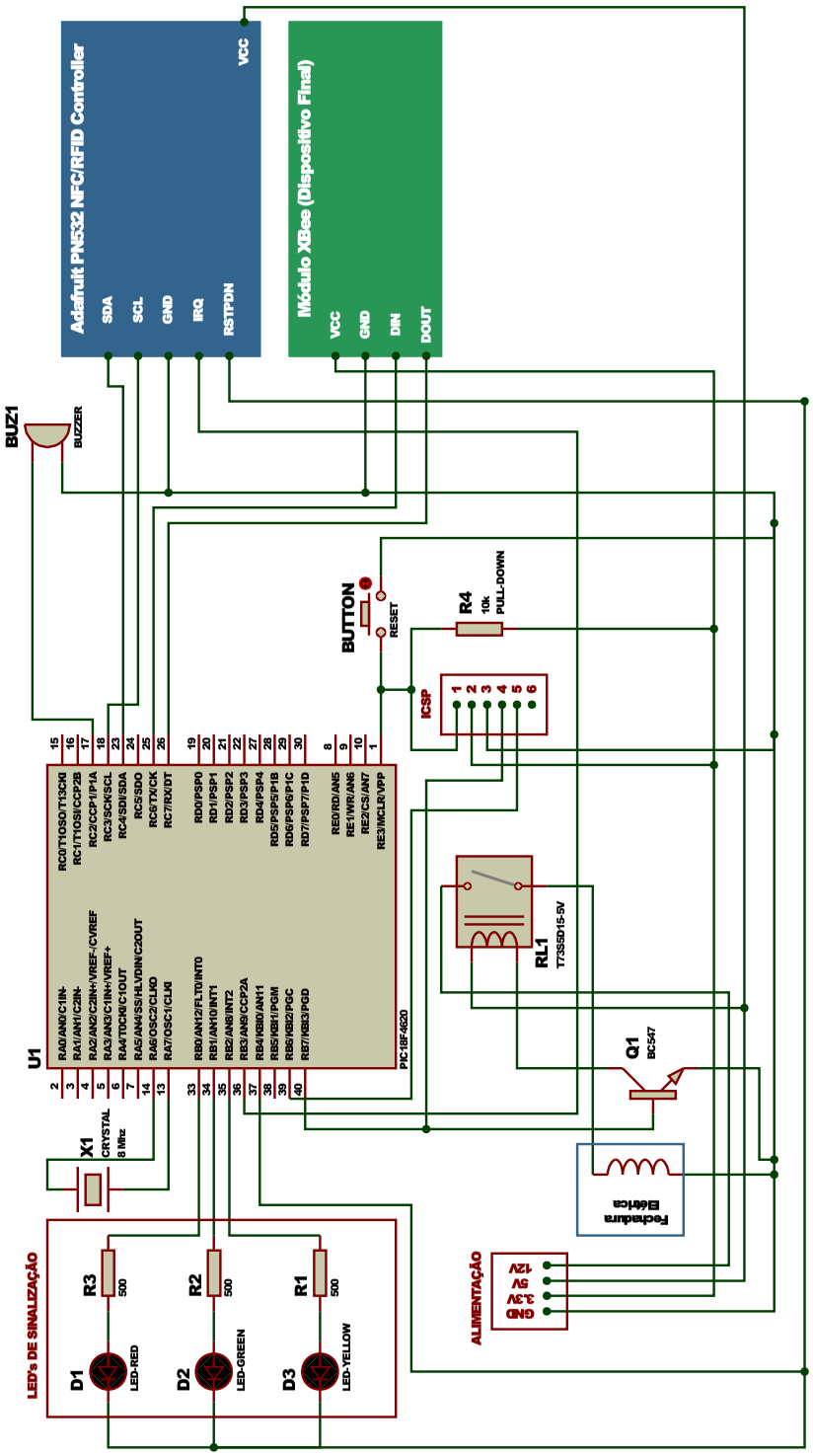



Figura B.1: Esquema Elétrico do módulo PAP

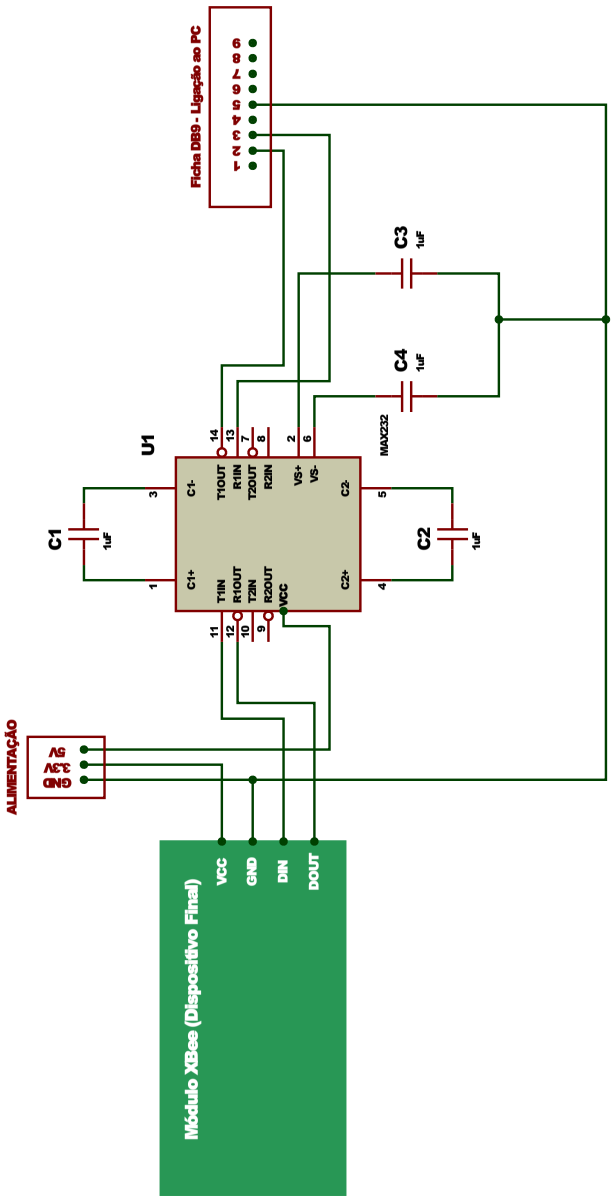



Figura B.2: Esquema Elétrico do módulo central - Sistema de ligação do módulo XBee ao computador central

Apêndice C

# Diagramas de Casos de Uso

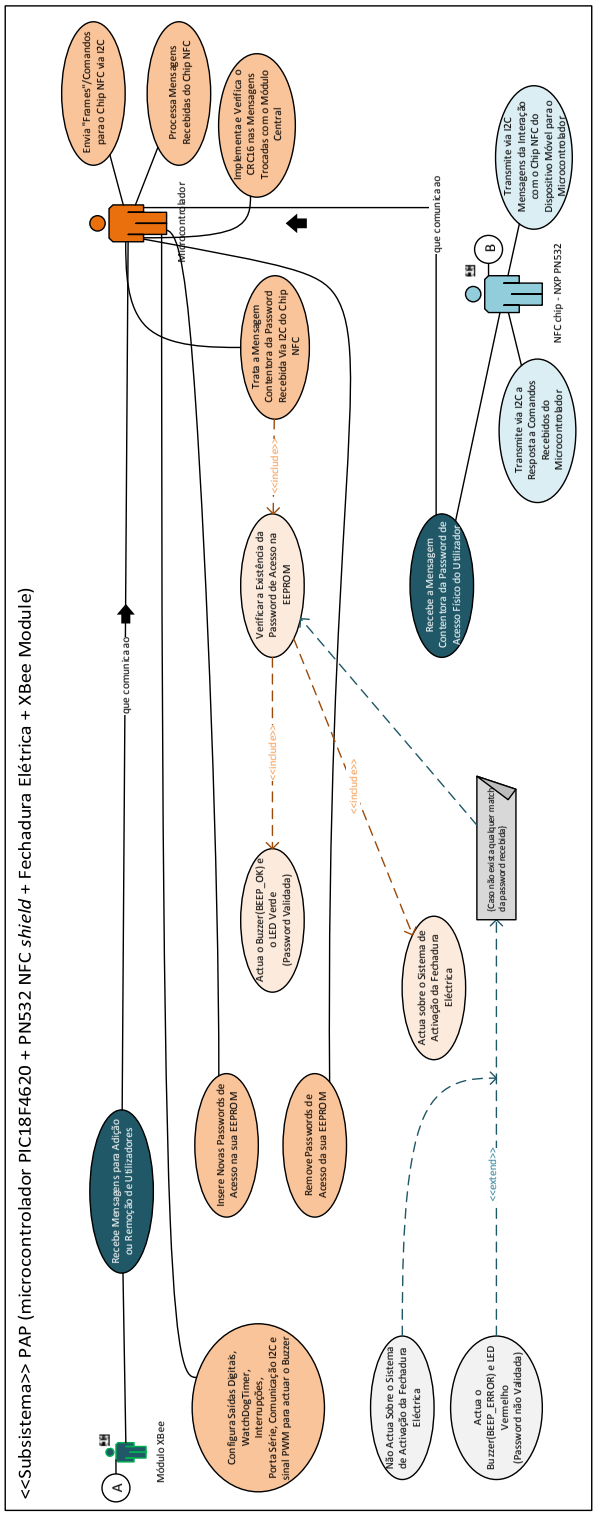



Figura C.1: Diagrama de casos de uso do módulo do PAP

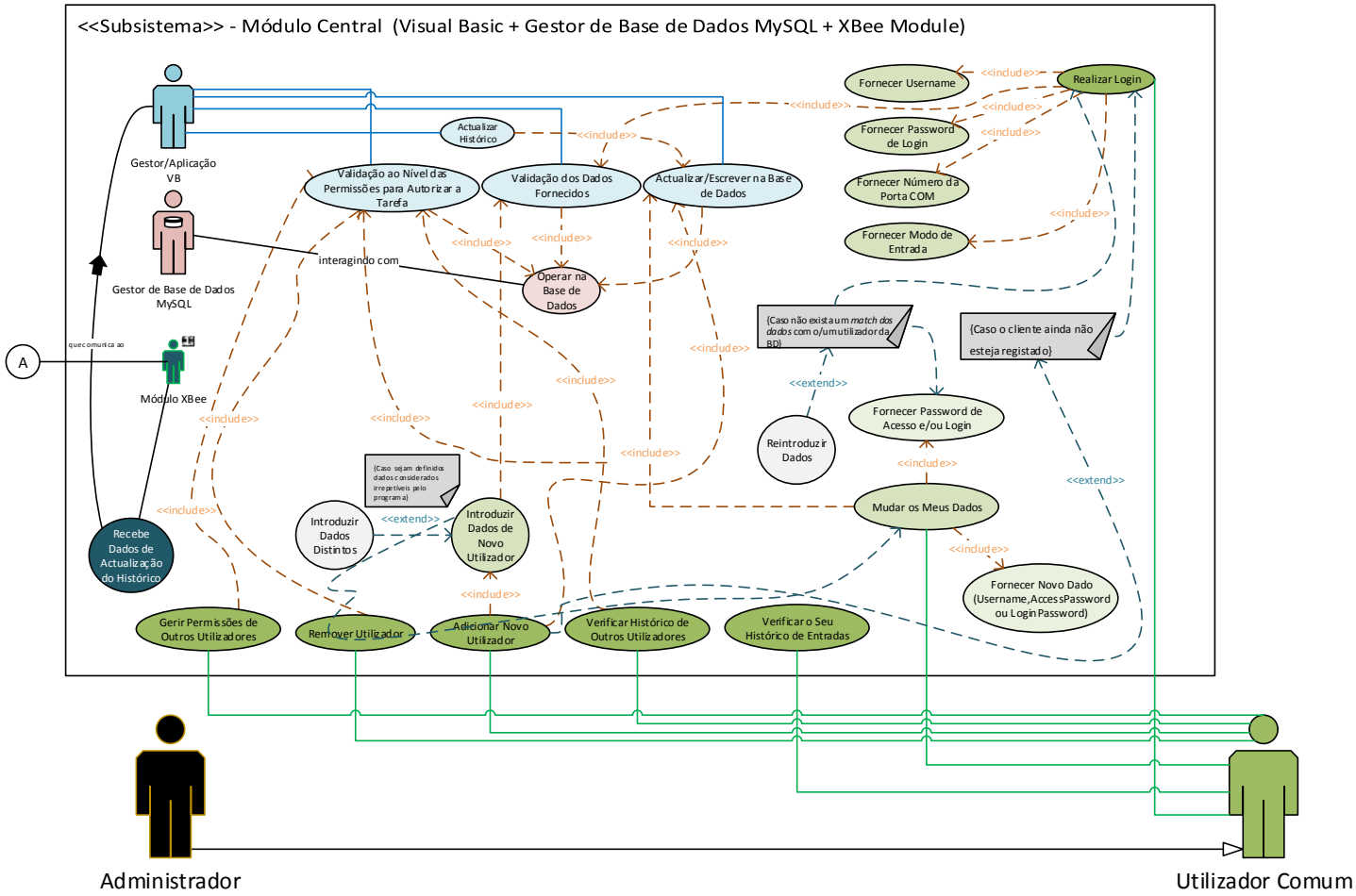



Figura C.2: Diagrama de casos de uso do módulo central

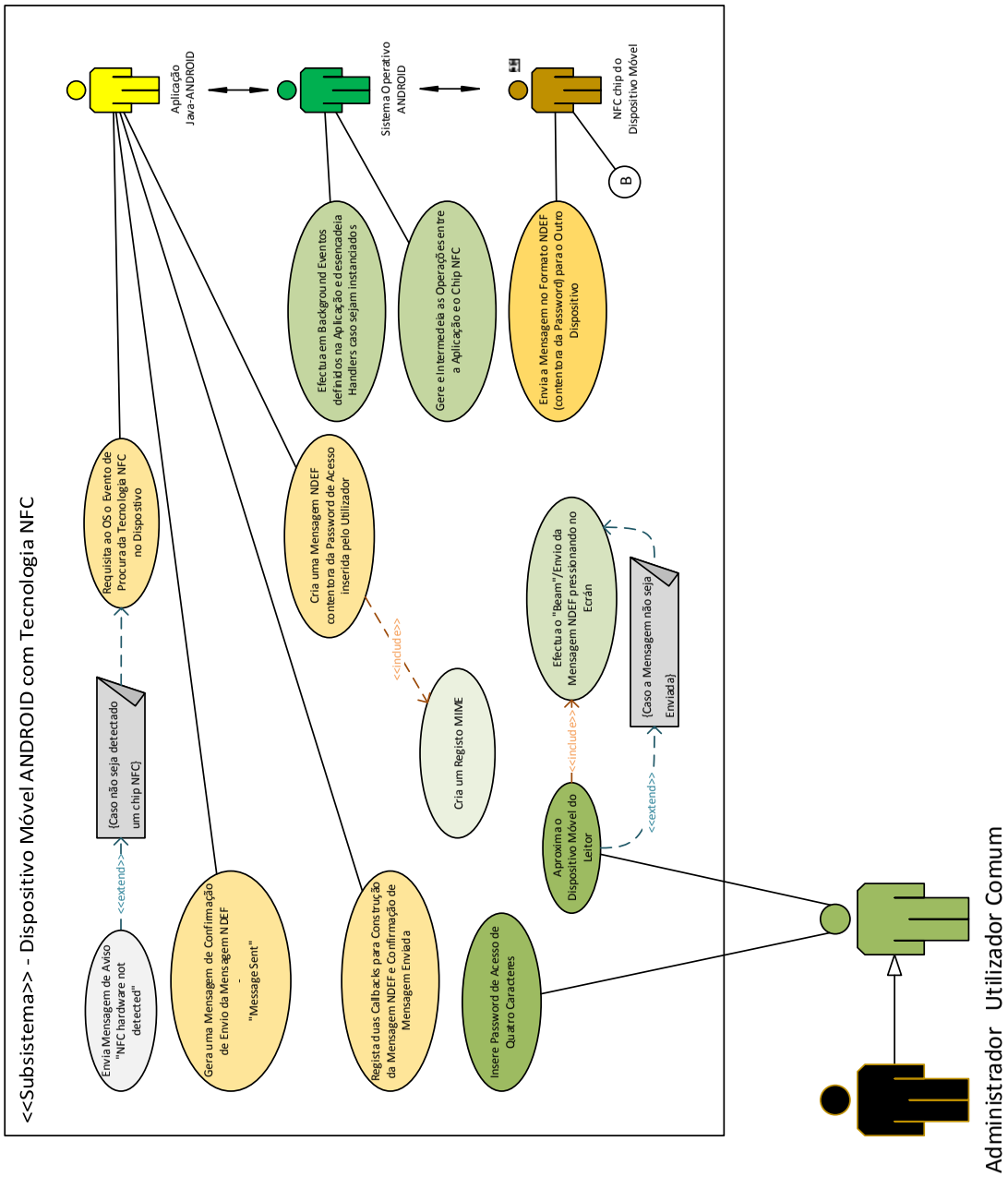



Figura C.3: Diagrama de casos de uso da aplicação do dispositivo móvel

# Apêndice D

# Diagramas de Sequência

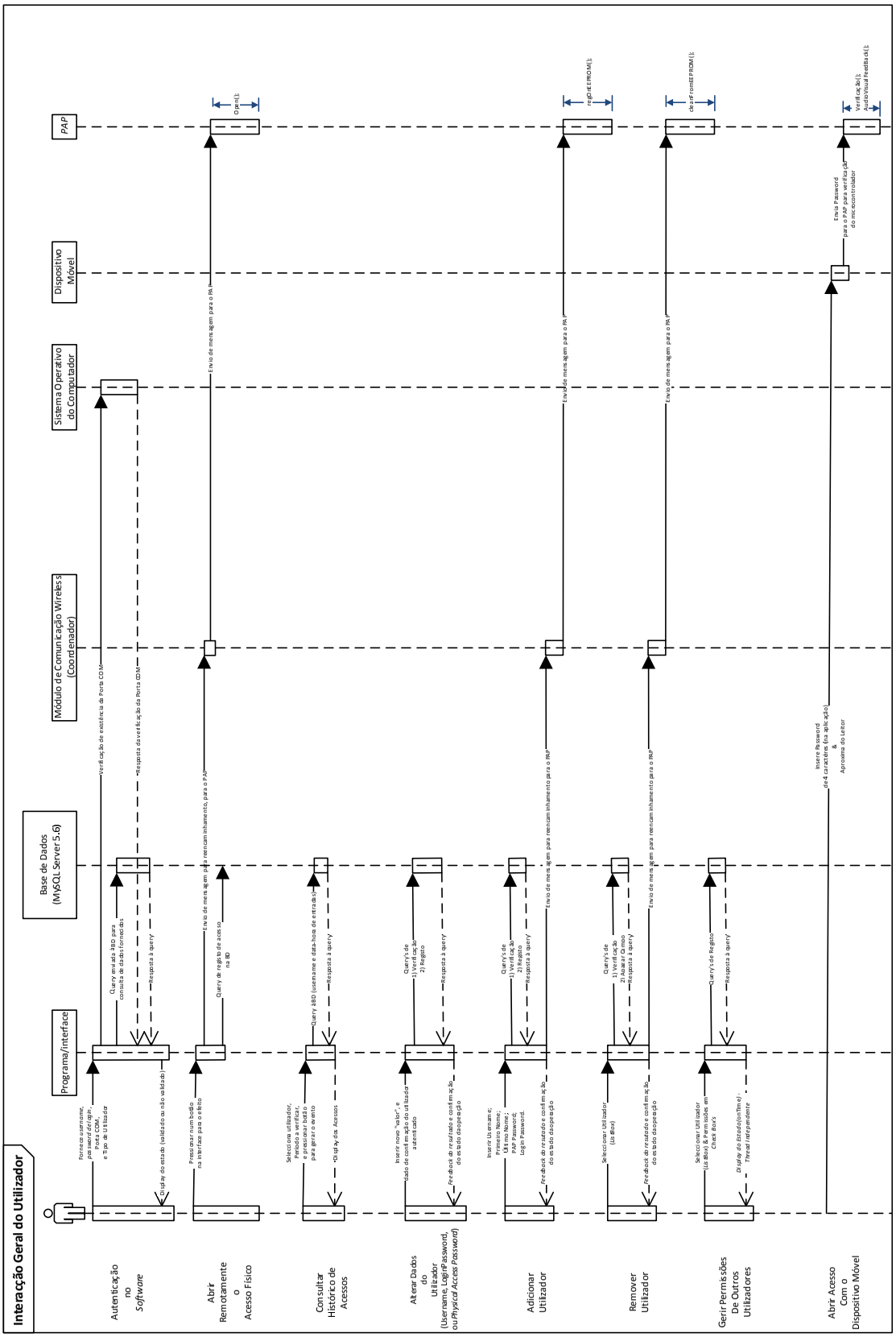



Figura D.1: Diagrama de sequência das operações gerais do utilizador sobre o sistema global