

Faculdade de Engenharia da Universidade do Porto



**FEUP**

## Sistema de Controlo de Acessos e Ponto Integrado Betronic

Tiago Daniel Vilela Ferreira

Relatório de Projecto realizado no âmbito do  
Mestrado Integrado em Engenharia Electrotécnica e de Computadores  
Major Telecomunicações

Orientador: Prof. José Alberto Peixoto Machado da Silva

Julho de 2008

© Tiago Daniel Vilela Ferreira, 2008

# Resumo

Este projecto teve como objectivo a implementação de um novo sistema de controlo de ponto e acesso para a empresa New Betronic. No desenvolvimento deste sistema foram realizadas diferentes tarefas incluindo estudo de mercado, pesquisa de componentes, integração eléctrica e concepção de *firmware* até à obtenção do produto final. O sistema desenvolvido tem como núcleo central uma placa já existente na empresa, a SIB3000, com a qual foram integrados, por exemplo, os periféricos de leitura de cartões de proximidade, impressão digital, cartões magnéticos, sistema de comunicações e teclado. O sistema faz parte dos produtos comercializados pela empresa, estando já instalado em diversos clientes de reconhecida importância.



# Abstract

This project had as the main objective the implementation of a new access and attendance control system for the New Betronic Company. For this implementation, one had to carry-out different tasks including market study, component research, electrical integration and firmware conception to get the final product. The developed system relies on an already existing central core board, the SIB 3000, in which the different peripherals like proximity card readers, fingerprint reader, magnetic card readers, communication system and keyboard were integrated. The system belongs now to the set of products commercialized by the company, being now installed in several important clients.



# Agradecimentos

Gostaria muito de agradecer a todos os que contribuíram para o meu percurso académico e profissional que já percorri.

Ao meu orientador, professor Alberto Peixoto Machado da Silva, pois apesar da distância de aproximadamente 300km, conseguiu ajudar-me sempre que necessário.

A todas as pessoas que constituem a New Betronic, pelo carinho com que sempre me trataram.

Aos meus colegas de curso por todo o apoio que me deram durante estes anos.

Aos meus pais e restante família por sempre acreditarem e confiarem em mim.

À Sara, minha esposa, pelo amor, carinho e incentivo sempre presente.

A Todos, o meu Muito Obrigado.





# Índice

Resumo .....	iii
Abstract .....	v
Agradecimentos .....	vii
Índice .....	ix
Lista de Figuras .....	xi
Lista de Tabelas .....	xiii
Abreviaturas e Símbolos .....	xv
1 Introdução .....	1
1.1 Estrutura do relatório .....	1
1.2 Enquadramento .....	1
1.3 Objectivos .....	2
1.4 Panorama actual .....	2
2 Tecnologias escolhidas .....	5
2.1 Arquitectura base .....	6
2.2 Periféricos .....	8
2.2.1 Leitor Biométrico .....	8
2.2.1.1 Leitor de impressão digital da Daemin .....	14
2.2.1.2 Leitor de impressões digitais da Suprema .....	15
2.2.2 Leitor de Proximidade .....	15
2.2.2.1 Leitor de proximidade i-class da HID .....	16
2.2.2.2 Leitor de proximidade MIFARE .....	17
2.2.2.3 Leitor de proximidade ISOPROX da HID .....	18
2.2.3 Teclado .....	19

2.2.4 Leitor de cartões magnéticos.....	19
2.2.5 Módulos de comunicações .....	20
2.3 Conclusão do capítulo .....	21
3 Integração e desenvolvimento .....	23
3.1 Identificação de funcionalidades .....	24
3.2 Integração de Periféricos.....	24
3.2.1 Leitor Biométrico.....	24
3.2.2 Antena de Proximidade .....	26
3.2.3 Teclado .....	26
3.2.4 Leitor Magnético .....	27
3.2.5 Comunicações .....	28
3.3 Firmware .....	28
3.4 Conclusão do capítulo .....	39
4 Aplicação e utilização .....	41
4.1 Terminais .....	42
4.1.1 Terminal SibZone .....	42
4.1.2 Terminal SibTower.....	43
4.1.3 Terminal MiniSib .....	43
4.1.4 Terminal SibStrong .....	44
4.1.5 Terminal SibPark .....	45
4.1.6 Terminal SibZone Enterprise.....	45
5 Conclusões e Perspectivas de Desenvolvimento .....	47
Referências .....	49
Anexos.....	51

# Lista de Figuras

Figura 2.1 - Imagem da placa B023 Rev.03 da New Betronic, com arquitectura SIB3000.....	7
Figura 2.2 - Imagem de um <i>software</i> de reconhecimento de face [5]. .....	9
Figura 2.3 - Amostra de uma impressão digital com alguns pontos de referência [6].....	9
Figura 2.4 - Imagem captada por um sistema de reconhecimento da geometria da mão [7]. ...	10
Figura 2.5 - Imagem da íris analisada pelo sistema de reconhecimento da íris [8]. .....	10
Figura 2.6 - Exemplo de um sistema de reconhecimento de assinatura [9].....	11
Figura 2.7 - Exemplo das ondas da fala captadas e analisadas em <i>software</i> [11]. .....	12
Figura 2.8 - Comparativo de diferentes sistemas de controlo biométrico [12].....	12
Figura 2.9 - Imagem de um Daemin DFZ-2002S [13].....	14
Figura 2.10 - Imagem de um Suprema SFM-3030-OP [15].....	15
Figura 2.11 - Imagem de um leitor i-class da HID [17]. .....	17
Figura 2.12 - Imagem de um leitor Mifare da STID [18].....	18
Figura 2.13 - Imagem de um leitor Isoprox da HID [19].....	18
Figura 2.14 - Imagem do teclado utilizado para integração no sistema [20]. .....	19
Figura 2.15 - Imagem do leitor magnético tipo <i>swipe</i> da KDR [21]. .....	20
Figura 2.16 - À esquerda um X-port da Lantronix. À direita, um Matchport da Lantronix [22]. ..	20
Figura 2.17 - Imagem de um modem GSM/GPRS da Comtech M2M [24].....	21
Figura 3.1 - Diagrama dos periféricos ligados ao microcontrolador ATmega64. ....	23
Figura 3.2 - Esquema de ligações do teclado à porta paralela do microcontrolador [25]..	27
Figura 3.3 - Exemplo de uma leitura de um cartão magnético [26]. .....	27
Figura 3.4 - Diagrama da arquitectura do <i>firmware</i> do sistema.....	29
Figura 3.5 - Estrutura do protocolo de comunicações do sistema.....	36
Figura 4.1 - Imagem do terminal SibZone. ....	42
Figura 4.2 - Imagem do terminal SibTower.....	43
Figura 4.3 - Imagem do terminal MiniSib. ....	44
Figura 4.4 - Imagem do terminal SibStrong. ....	44
Figura 4.5 - Imagem do sistema SibPark.....	45
Figura 4.6 - Imagem do sistema SibZone Enterprise. ....	46
Figura 5.1 - Ilustração do método de autenticação por reconhecimento das veias [27]. .....	48



# Lista de Tabelas

Tabela 3.1 - Comandos do leitor biométrico da Suprema utilizados no sistema.....	25
Tabela 3.2 - Versões Compiladas do Firmware.....	38



# Abreviaturas e Símbolos

## Lista de abreviaturas

CLS	<i>Card Load Signal</i>
CR	<i>Carriage Return</i>
CRC	<i>Cyclic Redundancy Code</i>
CSD	<i>Circuit Switched Data</i>
DC	<i>Direct Current</i>
DNA	<i>Deoxyribonucleic Acid</i>
DPI	<i>Dots per Inch</i>
EEPROM	<i>Electrically-Erasable Programmable Real-Only Memory</i>
EER	<i>Equal Error Rate</i>
EUA	Estados Unidos da América
FAR	<i>False Acceptance Rate</i>
FRR	<i>False Rejection Rate</i>
FVC	<i>Fingerprint Verification Competition</i>
GPRS	<i>General Packet Radio Service</i>
GSM	<i>Global System for Mobile Communications</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IP	<i>Internet Protocol</i>
LAN	<i>Local Area Network</i>
LED	<i>Light Emitting Diode</i>
LF	<i>Line Feed</i>
OEM	<i>Original Equipment Manufacturer</i>
PDA	<i>Personal Digital Assistant</i>
PIN	<i>Personal Identification Number</i>
RCK	<i>Read Clock</i>
RDT	<i>Read Data</i>
RFID	<i>Radio-frequency Identification</i>
RTC	<i>Real Time Clock</i>

SIB	Sistema Integrado Betronic
SIM	<i>Subscriber Identity Module</i>
SMS	<i>Short Message Service</i>
TCP	<i>Transmission Control Protocol</i>
TTL	<i>Transistor-Transistor Logic</i>
UART	<i>Universal Asynchronous Receiver/Transmitter</i>
WLAN	<i>Wireless Local Area Network</i>
XOR	<i>Exclusive Or</i>

#### Lista de símbolos

$\Omega$	Ohms
----------	------



# Capítulo 1

## Introdução

### 1.1 – Estrutura do relatório

Este relatório foi elaborado no seguimento do projecto relativo ao desenvolvimento de um sistema de controlo de ponto e acesso. Este encontra-se dividido em cinco grandes capítulos. No primeiro capítulo é feita uma introdução ao tema, mencionando o enquadramento e os objectivos do projecto. No segundo capítulo são abordadas as tecnologias escolhidas para o desenvolvimento do projecto. No terceiro capítulo são apresentados mais detalhes relativamente à integração e desenvolvimento do sistema. No quarto capítulo é demonstrada a aplicação prática e real do projecto, e no último capítulo são considerados futuros desenvolvimentos e conclusões.

### 1.2 - Enquadramento

A empresa New Betronic situa-se no mercado de controlo electrónico de ponto e acesso como uma das principais marcas nacionais. A sua área de acção está alargada às áreas do controlo electrónico de ponto, controlo de acesso físico a parques e edifícios, videovigilância, gestão de recursos humanos e controlo electrónico de rondas.

Esta é uma área com uma expressão cada vez maior no mercado português, uma vez que as empresas necessitam de controlar as suas equipas, de modo a obterem mais e melhores resultados. As grandes vantagens que a New Betronic oferece, face aos seus concorrentes, são a personalização das soluções à medida do cliente e o desenvolvimento e produção dos equipamentos em Portugal.

No processo de integração do aluno na equipa de investigação e desenvolvimento da referida empresa, em Lisboa, foi solicitado o desenvolvimento de uma solução de controlo de assiduidade e acesso que utilizasse uma placa de circuito impresso já existente na empresa, nomeadamente o Sistema Integrado Betronic (SIB) 3000. De acordo com as directivas dadas pela direcção da empresa, e utilizando a arquitectura já existente, foi iniciada a fase de pesquisa e desenvolvimento de forma a satisfazer os requisitos então exigidos.

### 1.3 - Objectivos

Este projecto foi iniciado com o objectivo de dotar a empresa New Betronic de uma nova solução de controlo de assiduidade e acesso para posterior comercialização no mercado.

Com uma linha de terminais ultrapassada, a empresa necessitava de algo novo para se reafirmar no mercado português. O novo sistema deveria apresentar novidades ao nível das tecnologias utilizadas, de modo a cativar novos clientes no sector.

Os sistemas anteriores da New Betronic baseavam-se em cartões magnéticos e de proximidade de baixa frequência para fazer a validação dos utilizadores nos terminais. Com o novo sistema, pretendia-se que o método de autenticação fosse biométrico, diminuindo assim as hipóteses do utilizador falsificar um acesso ao sistema utilizando o cartão de outro. Foi com este objectivo que nasceu o projecto para o novo sistema da New Betronic.

### 1.4 - Panorama actual

Actualmente, o controlo de assiduidade e de acesso são áreas muito distintas. Os métodos mais utilizados para controlo de ponto são os cartões de impressão (controlo analógico), cartões magnéticos e cartões de proximidade. No entanto, o controlo de assiduidade por métodos biométricos é uma realidade emergente e com cada vez mais oferta, visto oferecer aos seus utilizadores uma maior fiabilidade contra a fraude.

Um dos mais importantes factores impulsionadores dos sistemas de reconhecimento biométrico para controlo de assiduidade no mercado português foi o Despacho N.º 187 / 2007 do Gabinete do Secretário Geral de Estado da Saúde. Este obriga a *“sistemas de registo de assiduidade e pontualidade automáticos, mais concretamente, de registos biométricos”*

Esta medida do ministério da saúde criou uma “corrida” aos sistemas de controlo de assiduidade biométricos no sector da saúde, o que levou posteriormente a que outros sectores apostassem no mesmo.

Relativamente ao controlo de acesso, os métodos mais utilizados para controlo de acesso são sem dúvida os cartões de proximidade e os códigos de acesso através de teclado. Também as tecnologias relacionadas com a biometria são cada vez mais usadas no controlo

de acessos, mas o seu preço ainda é um pouco elevado comparativamente com os restantes métodos.

Com o desenvolvimento das tecnologias e com o aumento da exigência relativamente a questões de segurança, é necessário desenvolver novos sistemas, mais seguros, na área da identificação pessoal. As tecnologias emergentes são actualmente as relacionadas com o reconhecimento biométrico, ou seja, com uma parte biológica do indivíduo a ser reconhecido.



## Capítulo 2

### Tecnologias escolhidas

Pretendeu-se com este projecto escolher e integrar um conjunto de tecnologias de reconhecimento de indivíduos para controlo de assiduidade e acesso. Para isso foram identificados vários métodos de identificação pessoal, de acordo com as especificações definidas pela administração da empresa.

A verificação automática da identidade de um utilizador pode ser feita por uma ou mais destas três formas [10] [28]:

- a. Algo que o utilizador sabe (PINs, *Passwords*)
- b. Algo que o utilizador possui (chave, cartão de identificação)
- c. Algo que a pessoa é (aspecto, voz, tamanho, forma, comportamento)

No sistema a ser desenvolvido deveriam estar presentes as três formas de modo a maximizar o grau de segurança. Este sistema, de acordo com o estudo de mercado e a estratégia da empresa, deveria ter os seguintes elementos:

- Arquitectura SIB3000 (Base do Sistema) de processamento
- Leitor biométrico
- Leitor de cartões de proximidade
- Teclado para inserção de dados
- Leitor de cartões magnéticos
- Tecnologias de TCP/IP para comunicação com o *software*

A arquitectura do sistema central SIB3000 estava já desenvolvida, e foi utilizada para que a integração de novas tecnologias fosse feita de uma forma mais rápida, dotando a empresa de um novo sistema com um menor tempo de desenvolvimento.

O leitor biométrico é a mais-valia deste sistema, utilizando tecnologia de ponta para identificação e verificação de indivíduos no sistema.

O leitor de cartões de proximidade permite tornar o sistema mais flexível, pois é um método de autenticação rápido e fiável.

O teclado permite uma maior interacção do utilizador com o sistema, podendo ser utilizado para classificações especiais ou simplesmente para tornar o sistema de reconhecimento mais rápido, ao se fazer uma comparação 1:1 segundo o número de utilizador inserido.

O leitor de cartões magnéticos serve para integrar em clientes que já possuam um sistema antigo, e não estejam dispostos a fazer um novo investimento em cartões de proximidade. Também é útil pelo preço por unidade dos próprios cartões, muito abaixo do preço dos cartões de proximidade.

As tecnologias de comunicação por TCP/IP com o *software* são necessárias para uma mais fácil integração do sistema no caso de existirem as infra-estruturas de rede necessárias. O sistema utilizará uma rede convencional, por rede ou sem fios, para estabelecer a comunicação entre terminais e *software*.

## 2.1 - Arquitectura base

A empresa New Betronic é proprietária da placa principal, arquitectura SIB3000, sobre a qual foi desenvolvido o novo sistema. A placa não é aqui apresentada ao detalhe por motivos de confidencialidade. Esta contém os seguintes elementos a destacar:

Microcontrolador AVR ATmega64 com 64 Kbytes de memória de programa tipo Flash;

*Display* de caracteres retro-iluminado com 2 linhas e 16 colunas (16x2)

Duas memórias EEPROM de 256 Kbits cada;

*Real Time Clock* com alimentação bateria de *backup* independente;

4 Entradas de 12 V isolados electricamente;

4 Saídas de 12 V isolados electricamente;

Diversos conectores para ligação de periféricos;

Podem ver-se todas as ligações e componentes principais na imagem seguinte.

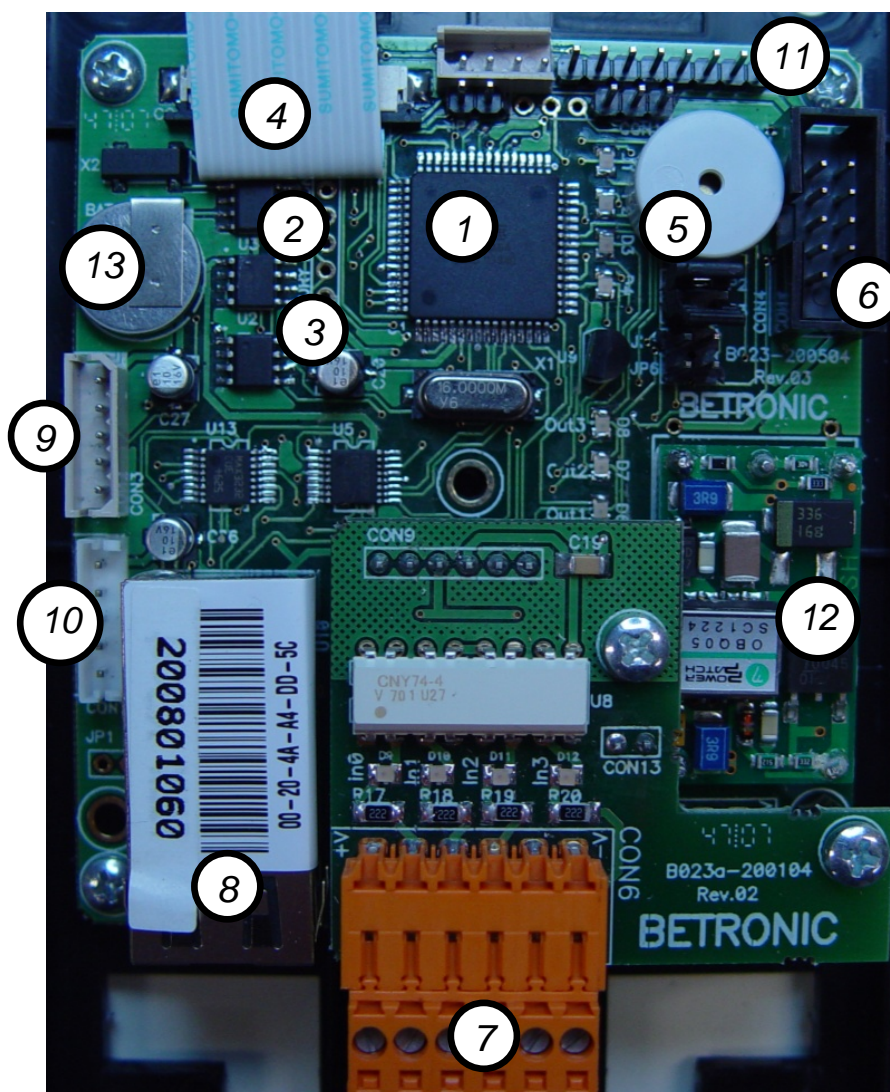


Figura 2.1 - Imagem da placa B023 Rev.03 da New Betronic, com arquitectura SIB3000.

Na figura 1 podem ver-se alguns elementos importantes assinalados. Estes são:

1. Microcontrolador ATmega64;
2. *Real Time Clock*;
3. 2 x EEPROM 256 Kbits;
4. *Flat-cable* de ligação com o ecrã;
5. Besouro;
6. Conector de programação;
7. Conector para entradas e saídas de potência;
8. Módulo TCP/IP X-port;
9. Conector do leitor de proximidade;
10. Conector do leitor biométrico;
11. Conector do teclado;
12. Conversor e estabilizador DC-DC 5V;
13. Bateria do *Real Time Clock*;

## 2.2 - Periféricos

O estudo dos periféricos foi feito por grupos distintos, separados pela função que desempenham. Esse estudo é apresentado de seguida.

### 2.2.1 - Leitor Biométrico

Para o reconhecimento inequívoco de um indivíduo é indispensável o uso de tecnologias de reconhecimento biométrico.

“A biometria promete a melhor segurança aos sistemas já existentes” [10].

“Biometria [bio (vida) + metria (medida)] é o estudo estatístico das características físicas ou comportamentais dos seres vivos. Recentemente este termo também foi associado à medida de características físicas ou comportamentais das pessoas como forma de identificá-las unicamente. Hoje a biometria é usada na identificação criminal, controlo de ponto, de acesso, entre outros. Os sistemas chamados biométricos podem basear o seu funcionamento em características de diversas partes do corpo humano, por exemplo: os olhos, a palma da mão, as impressões digitais do dedo, a retina ou íris dos olhos. A premissa em que se fundamentam é a de que cada indivíduo é único e possui características físicas e de comportamento (a voz, a maneira de andar, entre outros) distintas” [1].

Existem duas formas diferentes de descobrir a identidade de uma pessoa: verificação e identificação. Verificação (Sou eu quem afirmo ser?) envolve confirmar ou negar a identidade reclamada por alguém. Na identificação é necessário estabelecer a identidade de uma pessoa (Quem sou eu?). Cada uma destas abordagens tem as suas próprias complexidades e pode provavelmente ser melhor resolvida por um certo sistema biométrico.

Um crescente número de tecnologias biométricas tem sido proposto nos últimos anos. Algumas destas tecnologias são mais apropriadas para aplicações específicas do que outras [2], e algumas são mais aceitáveis pelos utilizadores. As seis tecnologias de reconhecimento biométrico que lideram o mercado são explicadas de seguida.

### Reconhecimento Facial

A tecnologia de reconhecimento facial identifica uma pessoa analisando características da face que não são facilmente alteradas – os contornos superiores dos olhos, as áreas à volta das bochechas, e os lados da boca [3]. A tecnologia é tipicamente utilizada para comparar um *scan* facial ao vivo com um *template* armazenado, mas também pode ser utilizado na comparação de imagens estáticas, tais como fotografias digitalizadas em passaportes. O reconhecimento facial pode ser utilizado em sistemas de verificação e identificação.



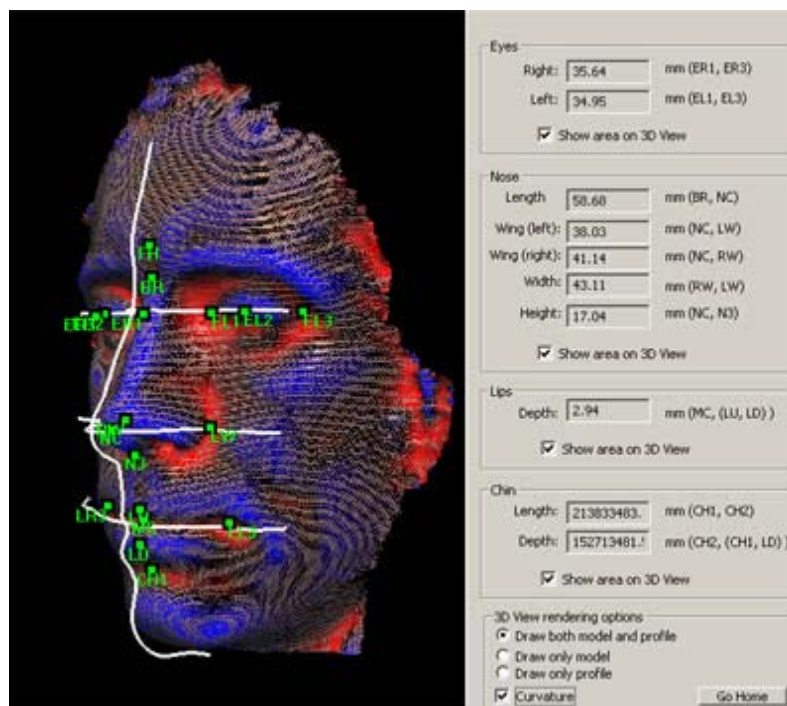


Figura 2.2 - Imagem de um *software* de reconhecimento de face [5].

## Impressão Digital

O reconhecimento da impressão digital é uma das mais conhecidas e mais utilizadas tecnologias biométricas. A tecnologia de reconhecimento de impressão digital extrai características das impressões feitas pelas distintas rugas nas impressões digitais [2]. As impressões digitais podem ser planas ou de rotação. Uma leitura plana captura apenas a impressão da zona central entre a ponta do dedo e a primeira junta; uma leitura de rotação captura as rugas de ambos os lados do dedo.



Figura 2.3 - Amostra de uma impressão digital com alguns pontos de referência [6].

## Geometria da Mão

A geometria da mão faz 96 medições da mão, incluindo largura, altura e comprimento dos dedos, distância entre junções, e forma das juntas. Os sistemas de geometria da mão utilizam uma câmara e díodos emissores de luz (LED) com espelhos e reflectores para capturar duas imagens em 2D ortogonais das costas e lado da mão.

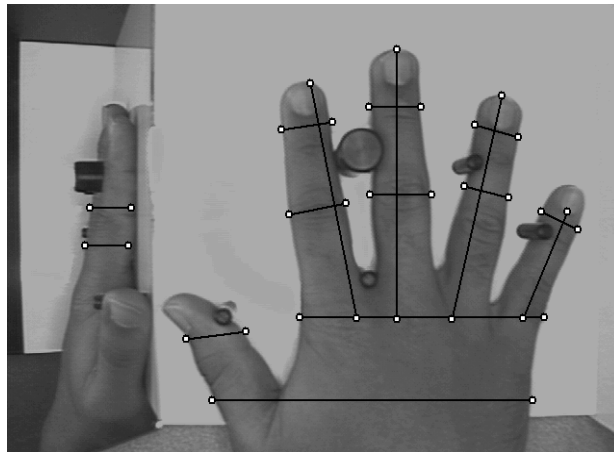


Figura 2.4 - Imagem captada por um sistema de reconhecimento da geometria da mão [7].

## Reconhecimento da Íris

A tecnologia de reconhecimento da íris é baseada no distintivo anel colorido que rodeia a pupila do olho. Feita de tecido de ligação elástico, a íris é uma fonte muito rica de informação biométrica, tendo aproximadamente 266 características distintas. Estas incluem a malha trabecular, um tecido que dá a aparência de dividir a íris radialmente. A tecnologia de reconhecimento de íris utiliza aproximadamente 173 destas características.

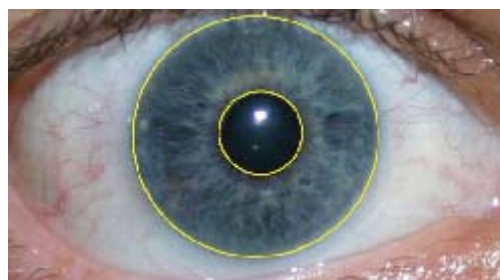


Figura 2.5 - Imagem da íris analisada pelo sistema de reconhecimento da íris [8].

## Reconhecimento da Assinatura

Num sistema de reconhecimento de assinatura, o utente assina o seu nome numa *tablet* gráfica digital ou num PDA e o sistema analisa os dinamismos da assinatura tal como a

velocidade relativa, ordem do traçado, contagem do traçado e a pressão. A tecnologia pode também seguir as flutuações naturais de cada pessoa com o tempo. A informação dos dinamismos da assinatura é encriptada e comprimida numa *template*.



Figura 2.6 - Exemplo de um sistema de reconhecimento de assinatura [9].

## Reconhecimento da Fala

As diferenças na forma como diferentes vozes soam são o resultado de uma combinação de diferenças fisiológicas na forma das cordas vocais e hábitos de fala aprendidos. A tecnologia do reconhecimento da fala utiliza estas diferenças para distinguir entre os utilizadores.

Os sistemas de reconhecimento da fala capturam amostras da fala do utente em resposta a um pedido de informação predeterminada um certo número de vezes. A frase é convertida de formato analógico para digital, e as características próprias do falar, tais como a afinação, cadência e tonalidade são extraídas, e o modelo é estabelecido. Uma assinatura de fala é então gerada e armazenada para futuras comparações [4] [10].

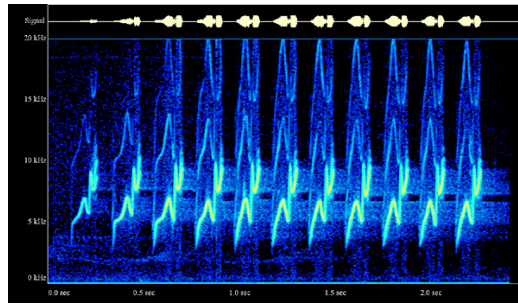


Figura 2.7 - Exemplo das ondas da fala captadas e analisadas em *software* [11].

A empresa tem com objectivo a comercialização de um sistema de reconhecimento biométrico fiável, de pequenas dimensões e de baixo custo, de forma a poder ser integrado facilmente em diversas estruturas e equipamentos. Desta forma, e analisando todos os métodos disponíveis no mercado, pode-se construir uma tabela de comparação. Seria impensável fazerem-se estes testes comparativos na empresa, visto que esta carece dos diferentes métodos de análise biométrica. Assim, recorreu-se à pesquisa de resultados já existentes nesta área. A melhor análise e comparação de métodos de reconhecimento biométrico encontrada é a publicada pelo Centro Nacional para Tribunais do Estado dos Estados Unidos da América (*National Center for State Courts*), apresentada em seguida. Nesta são publicados os resultados de três outros métodos biométricos, que são menos utilizados do que os anteriormente apresentados. São eles o *Scan* de retina do olho, o reconhecimento da digitação em teclado e o reconhecimento de DNA.

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	✓	✓	⊙⊙⊙⊙⊙	▶▶▶▶▶	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	✓	✗	⊙⊙⊙⊙	▶▶▶▶	no data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	✓	✗	⊙⊙⊙⊙	▶▶▶▶	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	✓	✗	⊙⊙⊙	▶▶▶▶	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	✓	✓	⊙⊙⊙⊙⊙	▶▶▶▶▶	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	✓	✓	⊙⊙⊙⊙⊙	▶▶▶▶▶	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	✓	✗	⊙⊙⊙	▶▶▶▶	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	✓	✗	⊙	▶▶▶▶	no data	hand injury, tiredness	Difficult	Easy
DNA	✓	✓	⊙⊙⊙⊙⊙	▶▶▶▶▶	no data	none	Ext. Diff.	Ext. Diff.

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Somewhat	▶▶▶▶▶	✓	Special, cheap	Yes
Facial Recognition	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✓	Common, cheap	?
Hand Geometry	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✗	Special, mid-price	?
Speaker Recognition	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✓	Common, cheap	?
Iris Scan	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✗	Special, expensive	?
Retinal Scan	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Very	▶▶▶▶▶	✗	Special, expensive	?
Signature Recognition	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✓	Special, mid-price	?
Keystroke Recognition	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Non	▶▶▶▶▶	✓	Common, cheap	?
DNA	▶▶▶▶▶	▶▶▶▶▶	▶▶▶▶▶	Extremely	▶▶▶▶▶	✗	Special, expensive	Yes

Figura 2.8 - Comparativo de diferentes sistemas de controlo biométrico [12].

Os parâmetros analisados são, pela ordem em que são apresentados:

Verificação – A verificação é o processo onde uma entrada é comparada com dados específicos previamente gravados do utilizador, para considerar se a pessoa é quem reivindica ser.

Identificação – A identificação é o processo onde uma entrada é comparada com uma grande base de dados gravada previamente dos vários utilizadores do sistema, para considerar quem a pessoa é.

Exactidão – Com qual exactidão o método consegue diferenciar os indivíduos.

Fiabilidade – Quão seguro é o método para a finalidade de reconhecimento.

Taxa de erro – Calculada com o cruzamento dos gráficos de falsa aceitação e falsa rejeição.

Erros – Causas típicas dos erros para este método.

Falsa aceitação – A facilidade com que o método reconhece falsos utilizadores como sendo utilizadores verdadeiros do sistema.

Falsa rejeição – A facilidade com que o método rejeita verdadeiros utilizadores como sendo utilizadores não registados no sistema.

Nível de segurança – O maior nível de segurança que este método é capaz de fornecer.

Estabilidade a longo prazo – Quão boa a biometria se mantém sem actualização dos dados passado um longo período de tempo.

Aceitação do utilizador – Quão dispostos os utilizadores estão para usar este método de reconhecimento biométrico.

Intrusão – Quão intruso é o método para o utilizador.

Facilidade de utilização – Quão fácil é o método de se utilizar.

Baixo custo – Se existe ou não uma opção económica para este método.

*Hardware* – Tipo e custo do *hardware* requerido para utilizar este método.

Padrões – Se existem ou não padrões para este método.

Analisando rapidamente a tabela, pode-se concluir que os métodos de reconhecimento da íris e retina são os que apresentam menor taxa de erro, sendo desta forma os mais fiáveis. Contudo, o seu preço é considerado caro, e é necessário *hardware* especial para o utilizar. Pelo contrário, os reconhecimentos de digitação em teclado e da fala são considerados baratos e não exigem *hardware* especial. Porém, estes têm valores muito baixos em exactidão e fiabilidade. Assim sendo, e analisando mais detalhadamente os dados, pode-se concluir que o reconhecimento da impressão digital é o método mais equilibrado, tendo um custo relativamente baixo e uma exactidão e fiabilidade elevadas. De destacar que este método possui a possibilidade para identificar um indivíduo comparando com os dados de vários indivíduos previamente registados numa base de dados, não necessitando de qualquer outro dado a não ser o da própria biometria da impressão digital para o reconhecimento do indivíduo.

Assim sendo, optou-se pela integração de um leitor biométrico de impressão digital no novo sistema. De acordo com a administração, e depois dos contactos do departamento comercial com diversas empresas da área, foram localizadas duas empresas fabricantes de leitores biométricos de impressão digital, os quais foram analisados, e cujos resultados são seguidamente referidos.

### 2.2.1.1 – Leitor de impressão digital da Daemin

O leitor de impressão digital anteriormente utilizado na empresa era o Daemin DFZ-2002S e tem as seguintes especificações:

- Processador de 32 bits
- Interface em RS232 níveis TTL
- Capacidade de armazenamento para 150 templates
- Sensor de captação de impressão digital óptico
- Resolução de imagem de 560 dpi
- FAR <0.1%
- FRR <0.0001%
- Temperatura de funcionamento -20°C até +60°C
- Peso 22 g
- Tensão de alimentação DC +3.3 V
- Corrente de alimentação <70 mA
- Corrente em modo suspenso <70 mA



Figura 2.9 - Imagem de um Daemin DFZ-2002S [13].

Este leitor tem o preço como factor favorável, mas tem uma limitada capacidade para 50 utilizadores e fraca qualidade do algoritmo de comparação. Por estes motivos, foi vontade da empresa a substituição deste módulo por outro com mais e melhores capacidades.

### 2.2.1.2 – Leitor de impressões digitais da Suprema

A Suprema é das mais prestigiadas marcas no segmento dos leitores de reconhecimento de impressão digital. Esta marca ganhou prémios na FVC (*Fingerprint Verification Competition*) nas últimas edições, em 2004 e 2006, sendo actualmente uma das mais fiáveis do mercado. A FVC é a maior competição do mundo para algoritmos de verificação de impressões digitais, e é organizada a cada dois anos pelas universidades de Bolonha (Itália), Universidade Estadual de San Jose (EUA), Universidade Estadual do Michigan (EUA) e a Universidade Autónoma de Madrid (Espanha) [14].

Assim sendo, e tendo em conta que este é um dos melhores fabricantes do mundo de leitores de impressão digital, escolheu-se o seu leitor OEM SFM3000, que tem as seguintes características:

- Processador de 32bits 400 MHz
- Interface em RS232 níveis TTL
- Capacidade de armazenamento para 1900 ou 9500 templates
- Sensor de captação de impressão digital óptico, capacitivo ou térmico
- Resolução de imagem até 508dpi
- EER <0.1%
- Tensão de alimentação DC +3.3 V
- Ver folha de especificações em ANEXO 1 para mais detalhes



Figura 2.10 - Imagem de um Suprema SFM-3030-OP [15].

### 2.2.2 - Leitor de Proximidade

Um dos requisitos obrigatórios para o desenvolvimento do terminal é a integração de um leitor para cartões de proximidade (RFID).

“RFID é um acrónimo do nome (**R**adio-**F**requency **I**Dentification) em inglês que, em português, significa Identificação por Radiofrequência. Trata-se de um método de identificação automática através de sinais de rádio, com leitura e armazenamento de dados remotamente através de dispositivos chamados de *tags* RFID.

Uma *tag* RFID é um pequeno objecto, que pode ser colocado numa pessoa, animal ou produto. Este contém chips de silício e antenas que lhe permitem responder aos sinais de rádio enviados por uma base transmissora” [16].

As tecnologias para cartões de proximidade por RFID podem ser divididas em duas categorias:

- Baixa frequência (125 KHz) - Cartões contêm apenas um número identificador não regravável, tipicamente com 26 ou 37 bits de comprimento e com um preço baixo.
- Alta frequência (13.56 MHz) – Cartões com possibilidade de leitura e escrita, com capacidade de memória, por exemplo, de 1 kbyte, e um preço moderado.

Ambas as tecnologias estão disponíveis nos fornecedores da empresa, sendo apenas necessária decidir qual das duas deverá ser utilizada.

No caso dos leitores de baixa frequência, o protocolo de comunicações é geralmente o *Wiegand*, protocolo de três linhas em que uma é a referência, outra é a linha do “zero” lógico e outra a linha do “um” lógico. Ou seja, são transmitidos sequencialmente nas duas linhas impulsos eléctricos. A correspondência a nível de dados será atribuída de acordo com a linha onde estes foram transmitidos.

Visto ambas terem vantagens e desvantagens, optou-se por se integrar as duas no sistema. Assim sendo, o cliente poderá definir que tipo de cartão pretende utilizar, dependendo da sua aplicação.

No caso a ser desenvolvido, as *tags* a utilizar deverão ter, na sua maioria, o formato de cartões de proximidade. Para isso, recorreu-se à pesquisa destas tecnologias nos habituais fornecedores da empresa. Os resultados obtidos serão agora referidos.

### 2.2.2.1 – Leitor de proximidade i-class da HID

O leitor de alta-frequência já utilizado pela empresa é de uma conhecida marca no ramo das RFID. A grande desvantagem da tecnologia i-class da HID é o facto de esta ser propriedade exclusiva da marca, o que faz com que os preços dos leitores e dos cartões sejam elevados. As características deste leitor são:

- Tensão de alimentação 5 VDC
- Corrente de pico 93 mA
- Interface em RS232 níveis TTL
- Temperatura de funcionamento de -35°C até +65°C
- Humidade de funcionamento de 5% até 95% de humidade relativa não condensada



- Frequência de funcionamento 13.56 MHz
- Capacidade para leitura e escrita
- Ver folha de características em ANEXO 2 para mais detalhes



Figura 2.11 - Imagem de um leitor i-class da HID [17].

Esta é uma tecnologia bastante avançada, mas cujos preços são pouco competitivos. Por este motivo, foi necessário encontrar uma alternativa, descrita de seguida.

#### 2.2.2.2 – Leitor de proximidade MIFARE

A tecnologia MIFARE é extremamente conhecida no ramo da RFID, e amplamente utilizada por diversos fabricantes e integradores. Esta tecnologia é propriedade da Philips, que vende os *chips* MIFARE para que outros fabricantes possam desenvolver os seus próprios leitores e cartões. No caso da New Betronic, o fabricante fornecedor desta tecnologia é a STID, e o produto utilizado é o leitor OEM W31-A PH1-5D. As suas características são as seguintes:

- Tensão de alimentação 5 VDC
- Corrente de pico 100 mA
- Interface em série com níveis
- Frequência de funcionamento 13.56 MHz
- Capacidade para leitura e escrita
- Ver folha de características em ANEXO 3 para mais detalhes



Figura 2.12 - Imagem de um leitor Mifare da STID [18].

### 2.2.2.3 – Leitor de proximidade ISOPROX da HID

Este é o leitor de RFID com tecnologia de baixa frequência que é utilizado pela empresa, e que foi também integrado no novo sistema. Assim como o i-class, o sistema ISOPROX também é propriedade da HID. O facto de esta tecnologia utilizar o protocolo de comunicações *Wiegand* facilita a integração de outros leitores, pois o protocolo não se altera de fabricante para fabricante, sendo apenas necessário a integração eléctrica de novos leitores de 125 kHz. As suas características técnicas são as seguintes:

- Tensão de alimentação de 4.75 VDC a 16 VDC
- Corrente de pico 100 mA
- Interface tipo *Wiegand*
- Frequência de funcionamento 125 KHz
- Capacidade para leitura e escrita



Figura 2.13 - Imagem de um leitor Isoprox da HID [19].

### 2.2.3 - Teclado

Para integração com o terminal, optou-se por utilizar um teclado de 16 teclas (4x4) do tipo matriz, não havendo um modelo específico a ser utilizado. A escolha do teclado vai depender o tipo de terminal a ser montado, e do tipo objectivo para o qual o terminal vai ser utilizado (por exemplo interior, exterior, anti-vandalismo). A folha de características pode ser consultada no ANEXO 4.

O aspecto exterior do teclado é o seguinte:



Figura 2.14 - Imagem do teclado utilizado para integração no sistema [20].

### 2.2.4 - Leitor de cartões magnéticos

A maioria dos leitores magnéticos obedece a um certo protocolo de comunicações. A integração deste protocolo no sistema permite a utilização de vários tipos de leitor magnético, consoante a aplicação em questão. No caso da New Betronic, o padrão utilizado para cartões magnéticos é:

- Leitura da pista magnética 2 (Codificação a 5 bits)
- 3 algarismos de série
- 5 algarismos de número de identificação

Relativamente aos leitores, estes possuem as seguintes características:

- Alimentação a +5V
- Saída dividida em 3 linhas (CLS, RCL, RDT) com níveis TTL



Figura 2.15 - Imagem do leitor magnético tipo *swipe* da KDR [21].

## 2.2.5 – Módulos de comunicações

Relativamente a comunicações com o exterior, procurou-se utilizar tecnologias recentes e facilmente integráveis. Desta forma, o método principal escolhido foi o uso de redes (LAN) cabeadas ou sem fios para comunicação com os terminais. Como a empresa tinha já um fornecedor fiável deste tipo de tecnologias (Lantronix®), foi escolhido um módulo *Wireless* do mesmo.

Este módulo converte o protocolo série com níveis TTL para protocolo de rede local sem fios. Esta conversão é transparente para o utilizador, pois todo o encapsulamento TCP/IP da rede local é feito automaticamente. Assim sendo, cada terminal é identificado por um endereço de IP único na rede local. Ver folha de características em ANEXO 5 e ANEXO 6 para mais detalhes.



Figura 2.16 - À esquerda um X-port da Lantronix. À direita, um Matchport da Lantronix [22].

Para comunicações de longa distância, escolheu-se a tecnologia GPRS, pois é a que melhor se adapta às requisições do sistema.

“O GPRS - *General Packet Radio Service* é uma tecnologia que aumenta as taxas de transferência de dados nas redes GSM existentes. Esta permite o transporte de dados por pacotes (comutação por pacotes). Sendo assim, o GPRS oferece uma taxa de transferência de dados muito mais elevada que as taxas de transferência das tecnologias anteriores, que usavam comutação por circuito, que eram em torno de 12 kbps. Já o GPRS, em situações

ideais, pode ultrapassar a marca dos 170kbps. No entanto na prática, essa taxa está em torno dos 40 kbps” [23].

No caso da placa SIB3000, a memória disponível para eventos é de 512 Kbits. Assim sendo, uma velocidade média de 40kbps é perfeitamente aceitável, dada a pequena escala da memória do aparelho a ser desenvolvido.

Segundo um estudo de mercado feito, e tendo em conta os prazos de entrega dos fornecedores, foi escolhido o modem OEM-GPRS2E da Comtech M2M. As suas características são as seguintes:

- GSM (CSD, SMS, voz)
- GPRS (Class B 4+2 Class 10), 57.6 Kbps (down), 28.8 Kbps (up)
- *Quad Band* (900/1800 MHz, 850/1900 MHz)
- Suporte integrado para cartão SIM
- Comunicação por RS232 níveis TTL
- Ver folha de características em ANEXO 7 para mais detalhes



Figura 2.17 - Imagem de um modem GSM/GPRS da Comtech M2M [24].

## 2.3 – Conclusão do capítulo

Estes são, portanto, os periféricos utilizados para o desenvolvimento do sistema de ponto e acesso. O período de pesquisa e análise foi indispensável, pois foram identificados os dispositivos importantes para integração no sistema, assim como a sua compatibilidade e funcionalidade.

Relativamente ao leitor biométrico a ser utilizado, chegou-se à conclusão que o método de identificação por impressão digital seria o mais indicado para o novo sistema, e dentro deste método foram identificados dois leitores de impressão digital para integração.

Relativamente aos leitores de proximidade, foram identificados três leitores diferentes, dos quais dois são de alta frequência e um de baixa frequência.

Como periféricos adicionais foram identificados um teclado tipo matriz de 16 teclas, um leitor de banda magnética e três módulos de comunicação, sendo estes adaptadores para rede local, rede local sem fios e redes móveis GSM/GPRS.

O passo seguinte é a implementação de cada um destes separadamente, e posterior integração de todos no sistema final. O desenvolvimento e integração dos periféricos serão abordados no próximo capítulo.



## Capítulo 3

### Integração e desenvolvimento

Para o desenvolvimento deste dispositivo foi necessário estudar o método de ligação dos diferentes periféricos. Para isso, foi criado um esquema ilustrativo das ligações físicas entre os diversos componentes do dispositivo:

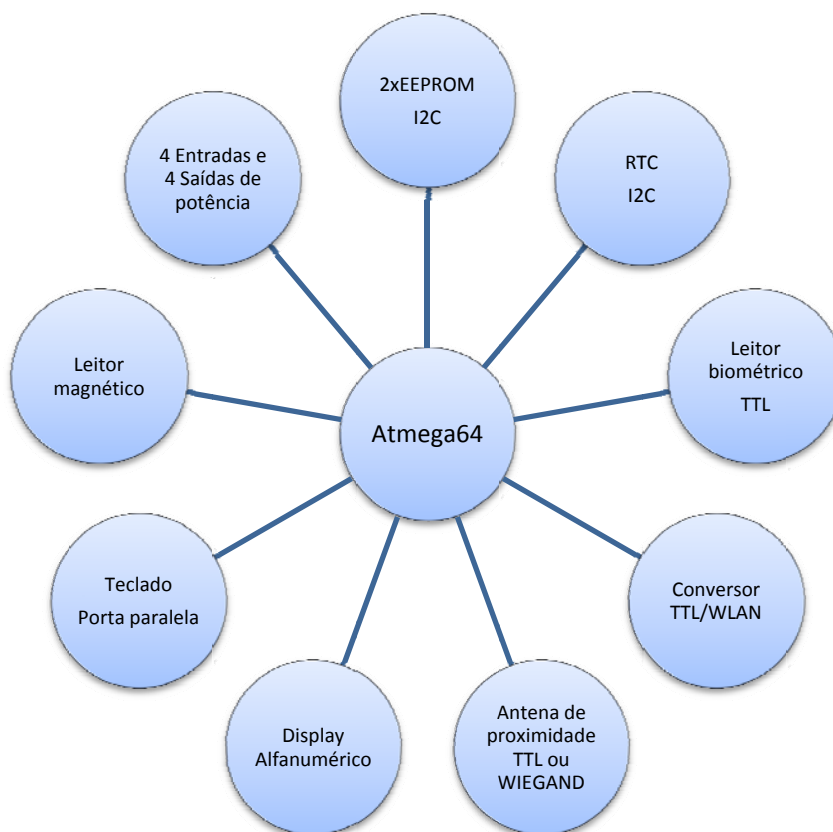


Figura 3.1 - Diagrama dos periféricos ligados ao microcontrolador ATmega64.

O Microcontrolador, como habitual, é o coração central deste sistema, e todos os periféricos serão controlados por ele.

Do ponto de vista de *firmware*, o trabalho foi feito de raiz utilizando a ferramenta de desenvolvimento já existente na empresa, BASCOM AVR em linguagem BASIC, e o programador tipo STK200 também já existente. Este assunto será tratado mais adiante neste documento.

### 3.1 - Identificação de funcionalidades

Pretende-se que o sistema tenha as seguintes funcionalidades:

- Controlo de data e hora das marcações nele efectuadas
- Identificação por impressão digital
- Identificação por cartão de proximidade
- Identificação por teclado (*PIN*)
- Identificação por dois métodos em simultâneo
- Possibilidade de algumas configurações por teclado
- *Feedback* luminoso e sonoro para o utilizador
- Possibilidade de comunicação com um *software* de gestão de acessos e assiduidades
- Gestão de acessos em modo *Offline*, isto é, com o *software* desligado
- Gestão de sensores e de dispositivos de bloqueio de portas
- Gestão de toques para sirene externa
- Possibilidade de funcionamento como pequena central de alarme activada por biometria, com sirene e sensores de intrusão externos

### 3.2 - Integração de Periféricos

Tendo em conta que a placa principal já existia antes de se efectuar este projecto, a parte de concepção de *hardware* mais crucial é a integração de periféricos. É esse o tema abordado nesta parte do relatório.

#### 3.2.1 - Leitor Biométrico

O leitor biométrico da *Suprema* é o melhor atributo deste novo sistema. Este, como já referido anteriormente, é ligado à placa principal por protocolo série com sinais de níveis TTL. Para a comunicação, o leitor utiliza um protocolo de comunicações proprietário da empresa coreana que o fabrica. O leitor biométrico não guarda as impressões digitais do utilizador, mas



sim um *template* gerado por um algoritmo proprietário do fabricante. Desta forma, não é possível utilizar engenharia reversa para obter a imagem da impressão digital. O sistema desenvolvido utiliza apenas as referidas *templates*, não havendo qualquer manipulação da informação biométrica do utilizador, excepto no interior do módulo da *Suprema*.

Depois de consultado o protocolo de comunicações do módulo, foi elaborada uma tabela com os comandos mais importantes para o funcionamento do sistema.

Tabela 3.1 - Comandos do leitor biométrico da Suprema utilizados no sistema.

Comando	Parâmetros	Funcionalidade
Registar biometria de utilizador	ID	Registar um novo utilizador no módulo, gerando uma nova <i>template</i> através da captura da impressão digital
Apagar utilizador	ID	Apaga todas as <i>templates</i> do utilizador
Identificar utilizador	-	Procura uma <i>template</i> idêntica à gerada e identifica o ID correspondente
Verificar utilizador	ID	Verifica se a <i>template</i> gerada coincide com a gravada com o respectivo ID
Comparar biometria	Template	Verifica se a <i>template</i> capturada coincide com a <i>template</i> passada por parâmetro, vinda de um cartão de proximidade <i>MIFARE</i>
Registar <i>template</i> enviada	Template; ID	Regista uma <i>template</i> enviada pelo <i>software</i> num certo ID
Apagar todos os utilizadores	-	Apaga todos os utilizadores da base de dados
Pedir <i>template</i> do utilizador	ID	Envia para o <i>software</i> a <i>template</i> do ID

Recorrendo a estas funcionalidades é possível fazer a gestão das *templates* registadas no sistema, assim como receber e enviar *templates* de e para o *software*, principalmente para partilha de informação com outros terminais. Desta forma, a gravação de uma *template* poderá ser feita apenas num terminal, e depois enviada a informação para todos os outros da instalação. Assim, o utilizador estará habilitado a utilizar qualquer dos terminais de identificação biométrica na instalação, pois as *templates* são compatíveis entre leitores do mesmo fabricante.

Fisicamente, este leitor é alimentado com os 3.3V disponíveis na ficha onde é ligado. Ao nível das comunicações, este leitor está ligado à porta série nº 2 do microcontrolador.

### 3.2.2 - Antena de Proximidade

A antena de proximidade i-class da HID foi facilmente integrada, pois a sua alimentação é de 5V DC e a comunicação é feita por porta série TTL. Visto o microcontrolador ATmega64 conter apenas 2 portas série físicas, foi necessário recorrer à configuração no *software* de programação de uma porta série virtual para comunicar através de outros pinos com as antenas de proximidade.

Relativamente às antenas de proximidade, as escolhidas para serem opção principal são as do tipo *MIFARE*. Esta tecnologia é propriedade da *Philips*, e tem os seus padrões largamente divulgados. No caso particular do projecto, o leitor utilizado foi o produzido pela STID, e possui um protocolo de comunicações específico. Também este leitor possui uma ligação série, e é emulada uma porta virtual no microcontrolador para que se faça a comunicação.

Finalmente, para integração da antena ISOPROX da STID é necessário recorrer ao protocolo *WIEGAND*. Este protocolo é facilmente descodificado utilizando dois *interrupts* externos do microcontrolador. Desta forma, um deles adiciona um bit como “um” lógico, enquanto o outro adicionará um “zero” lógico ao byte que estiver a ser recebido. Desta forma, pode-se montar um *array*, que no caso dos cartões ISOPROX mais vulgares, pode ter 26 ou 37 bits.

### 3.2.3 - Teclado

A estrutura electrónica do teclado não contém nenhum circuito integrado, ou seja, não tem qualquer processamento. Neste caso o teclado utilizado é de 16 teclas, estando divididas em 4 linhas e 4 colunas (4x4).

Para integração do teclado no sistema utilizou-se uma porta paralela do microcontrolador. Assim sendo, cada bit da porta fica ligado directamente a uma linha ou coluna do microcontrolador. Neste caso não existiam quaisquer resistências de *pull-up* para efeitos de referência nas linhas do teclado, por isso teve de se integrar na placa principal um *array* de resistências de 470Ω com essa finalidade.

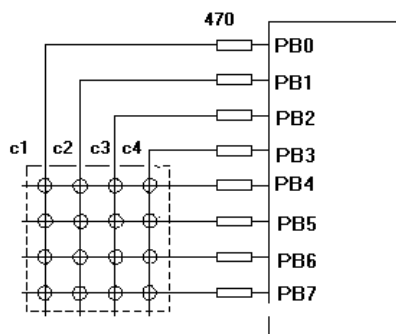


Figura 3.2 - Esquema de ligações do teclado à porta paralela do microcontrolador [25].

O teclado tem como objectivo criar uma maior interacção com o utilizador. Ao digitar o ID antes de inserir o dedo para recolha da impressão digital, o utilizador selecciona no sistema uma comparação 1:1, o que torna a validação biométrica muito mais rápida e fiável. As teclas numéricas também podem ser utilizadas para inserção de um *pin* pessoal, em casos especiais.

Para complementar as teclas numéricas existem quatro teclas de apoio. Essas têm as funções de Menu, Cima, Baixo e Funções especiais. Através destas teclas o utilizador pode fazer configurações no terminal, navegar pelo Menu ou utilizar as funções especiais.

### 3.2.4 - Leitor Magnético

A comunicação do leitor magnético é feita por três sinais eléctricos distintos. São eles o *Card Load Signal* (CLS), o *Read Data* (RDT) e o *Read Clock* (RCK). O CLS é o sinal que indica que um cartão está a ser lido no leitor e o RCK é o sinal de relógio que indica quando se deve ler o bit de dados no RDT. O seu funcionamento é demonstrado na figura 19.

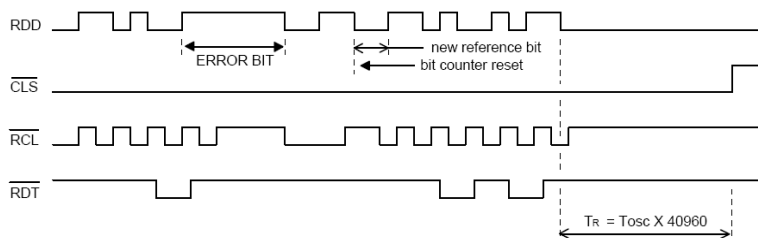


Figura 3.3 - Exemplo de uma leitura de um cartão magnético [26].

### 3.2.5 - Comunicações

Do ponto de vista das comunicações o processo de integração é bastante transparente. Visto que os módulos LAN e WLAN são conversores Série/TCP não é necessário fazer qualquer programação especial no *firmware*. Para o microcontrolador, escrever na rede LAN ou WLAN é como escrever numa porta série perfeitamente normal, sendo o conversor a tratar do encapsulamento e tratamento necessário dos dados.

Para integração do GPRS são necessários diversos comandos de configuração e ligação. Visto o GPRS ser taxado por volume de dados e não por tempo de ligação, o sistema ficará a funcionar em modo “*Always On*”, enviando os dados em tempo-real para o *software*. Para a configuração e conexão do modem são utilizados os comandos AT dos modems normais. O processo de ligação passa por identificar um *hostname* na internet, identificar o seu ip e ligar-se à porta correspondente, para depois ser redireccionado até ao *software*. Um exemplo de *hostname* é *betronic.dyndns.org*. Para se obter esta função pode-se utilizar o serviço gratuito da *dyndns.org* ou utilizar um *hostname* e/ou IP fixo.

## 3.3 - Firmware

Como já indicado anteriormente, a empresa New Betronic já possuía a licença de uma ferramenta de desenvolvimento para a família de microcontroladores AVR da Atmel, o Bascom AVR. A linguagem de programação deste *software* é o Basic, e o programador também já existente na empresa é o STK200, modelo que interage directamente com o *software*.

Um dos passos mais críticos deste projecto foi a necessidade de aprendizagem de uma nova linguagem de programação Basic. Esta não é habitualmente leccionada no decorrer do MIEEC, o que obrigou a um período de adaptação e aprendizagem da sintaxe da mesma.

Por razões de confidencialidade, e visto que este é um sistema de segurança, apenas serão reveladas algumas partes do código e do protocolo de comunicações.

O *firmware* é a essência funcional deste projecto, pois junta todas as peças para formar um único sistema. O seu desenvolvimento foi progressivo, sendo que cada periférico era integrado de cada vez. Assim, o código foi crescendo e ficando mais denso, à medida que se juntavam todos os diferentes periféricos. A versão final tem aproximadamente 6000 linhas de código em Basic.

O *firmware* está dividido em cinco diferentes partes, sendo elas:

- Inicializações e definições padrão
- Ciclo principal de comando
- Interrupção temporizada para controlo de tempo
- Funções de gestão e interacção com periféricos
- Outras funções

Para tornar o processo mais simples de se analisar concebeu-se um diagrama explicativo do funcionamento genérico do *firmware*.

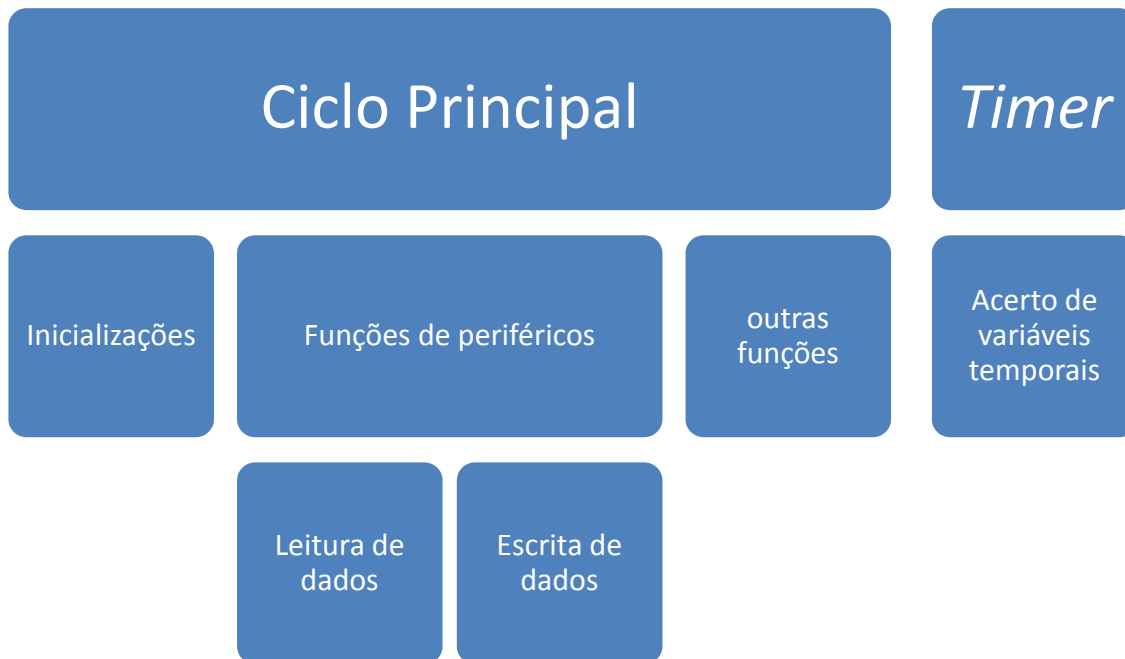


Figura 3.4 - Diagrama da arquitectura do *firmware* do sistema.

Como se pode ver no diagrama da figura 20, todas as funções estão dependentes do ciclo principal. O código do ciclo principal pode ser consultado no ANEXO 8.

Este ciclo é do tipo *Do While* e não tem qualquer parâmetro, sendo desta forma infinito. É através deste que são chamadas todas as funções ligadas com acções no terminal. Temos então as seguintes funções principais presentes:

- Call Keyboard – Verificação do estado do teclado
- Call Bio\_identify – Identificação de um utilizador por impressão digital
- Call Swuart\_read – Leitura de um cartão de proximidade
- Call Verifica\_toques – Activação de toques programados
- Call Data\_hora – Acerto da data e hora pelo RTC
- Reset Watchdog – Reinicialização do *Watchdog* de protecção
- Call Verifica\_inputs- Verificação do estado das entradas
- Call Verifica\_outputs – Alteração ou não do estado das saídas

No início de execução do programa são necessárias algumas inicializações de variáveis e de periféricos. Estas são executadas na primeira parte do *Main* do *firmware*, como mostra o excerto apresentado de seguida.

```

Main:
Terminal_type_temp = Terminal_type
If Terminal_type_temp <> "E" And Terminal_type_temp <> "S" And Terminal_type_temp <> "I" Then
Date$ = "01.01.08"          'DATA E HORA COM INICIO DO DIA/ANO
  
```

```

Time$ = "00:00:00"
Terminal_type = "I"
Config_in0 = "0"
Config_in1 = "0"
Config_in2 = "0"
Config_in3 = "0"
Config_out0 = "0"
Config_out1 = "0"
Config_out2 = "0"
Config_out3 = "0"
Offline_type = "0"
Card_serie = "AA"
Biometrico_activo = 1
Time_rele = 3
Biofree = 1
Bioprox = 1
Apontador_user = 0
Ponteiro_wr_log = 0
Biofree_number = 1
Timediff_eram = 0
Pin_menu = "0000"
Teclado_ligado = 0
Dual_finger = "0"
Tipo_picagem = "I"
Picagem_teclado_ram = 2
Bio_nivel_eram = &H34
Idterminal = "00"

' TERMINAL COM TIPO DE MOV INDIFERENTE
'TODAS AS ENTRADAS DESACTIVADAS

'TODAS AS SAIDAS EM NA

'DESACTIVADO OFFLINE
'SERIE AA
'BIOMETRICO ACTIVADO (para bioprox)
'Biofree desactivado

End If

Bio = Chr(32)
Prox = Chr(32)
Online = Chr(32)
Bio_presente = 0
Biofree_number_temp = Biofree_number
Online_str = Online
Prox_str = Prox
Configuracao = "0"
Caracter_bio = 1
Caracter_prox = 1
Bloquear_porta = 0
Onlinebefore = 0
Read_block = 0
Read_block2 = 0
Rw_en = 0
Flag_bio_match = 0
Flag_releon = 0
Waitok = 0
Offline_flag = 0
Time_offline_var = 0
Bio_caperror_flag = 0
Gravou = 0
Prox_time = 30 * 5
Timediff = Timediff_eram
Timediff_pointer = 1
Flag_tecla = 0
Pin_menu_temp = Pin_menu
Flag_menu = 0
Teclado_ligado_temp = Teclado_ligado
Dual_finger_temp = Dual_finger
Tipo_picagem_temp = Tipo_picagem
Picagem_teclado = Picagem_teclado_ram
Terminal_type_temp = Terminal_type
Reletempo = Time_rele
Flag_registro_auto = 0
Flag_mudanome = 0

Type_in0 = Config_in0
Type_in1 = Config_in1
Type_in2 = Config_in2
Type_in3 = Config_in3

Type_out0 = Config_out0
Type_out1 = Config_out1
Type_out2 = Config_out2
Type_out3 = Config_out3

```

'Carrega as definições dos ios e outros na memória

```

Offline_type_temp = Offline_type
Card_serie_temp = Card_serie

Biometrico_activo_temp = Biometrico_activo
Biofree_temp = Biofree
Bioprox_temp = Bioprox

Flag_alarme = 0
Flag_toca = 0
Flag_alarme_on = 0

Flag_pin = 0
Pin_valido = 0
Bio_keyboard = 0

Bio_nivel_var = Bio_nivel_eram
Flag_checkfinger = 1

Flag_readcard = 0

Mem_online = 0

Idterminal_temp = Idterminal

Prox_sector(1) = 1
Prox_sector(2) = 2
Prox_sector(3) = 4
Prox_sector(4) = 5
Prox_sector(5) = 6
Prox_sector(6) = 8
Prox_sector(7) = 9
Prox_sector(8) = 10
Prox_sector(9) = 12
Prox_sector(10) = 13
Prox_sector(11) = 14
Prox_sector(12) = 16
Prox_sector(13) = 17
Prox_sector(14) = 18
Prox_sector(15) = 20
Prox_sector(16) = 21
Prox_sector(17) = 22
Prox_sector(18) = 24
Prox_sector(19) = 25
Prox_sector(20) = 26
Prox_sector(21) = 28
Prox_sector(22) = 29
Prox_sector(23) = 30
Prox_sector(24) = 32
Prox_sector(25) = 33
Prox_sector(26) = 34
Prox_sector(27) = 36
Prox_sector(28) = 37
Prox_sector(29) = 38
Prox_sector(30) = 40
Prox_sector(31) = 41
Prox_sector(32) = 42
Prox_sector(33) = 44

Call Verifica_outputs          'Para que as saídas fiquem inicialmente abertas

Enable Interrupts             'activa as interrupções configuradas

Open "com1.:" For Random As #1      'Abre as portas com e respectivos canais
Open "com2.:" For Random As #2

Do
  Byteuart = Inkey(#1)
Loop Until Byteuart = 0
Buffertemp = ""

Cls                               'Limpa display
Cursor Off                       'desactiva cursor do display
Call Data_hora
Call Company_name                 ' Coloca no nome da empresa

```

```

Set Diag0                'coloca a OFF todos os Leds de Diagnostico e Outputs
Set Diag1
Set Diag2
Set Diag3

Wait 2

For A = 100 To 1000 Step 300      '"MUSICA" inicial
    Sound Buzz , 250 , A
Next A
Set Buzz

#if Dog                      'Arranca com watchdog
    Start Watchdog
#endif

Reset_rf = 0

Call Bio_reset              'Reset ao Leitor Biometrico
Call Swuart
Wait 1

Start Timer1                'Se todas as inicializações foram feitas, arranca com o timer

```

No bloco inicial (*If then*) são carregados os valores por defeito com que o terminal deve ficar depois de carregado o *firmware*. Graças ao bloco *If then* e à escrita na EEPROM do processador, os valores padrão apenas são carregados uma vez. Assim, mesmo que o terminal seja electricamente reiniciado, este não voltará a carregar as definições padrão. Pode-se ver, por exemplo, que a data por defeito é inicializada a dia 01-01-2008. Todas as configurações padrão podem ser configuradas por *software*. Os passos seguintes são inicializações de variáveis dinâmicas, periféricos e timer, assim como luzes e som de inicialização.

Para inicialização de periféricos, estão presentes as funções *Bio\_reset* e *Swuart* (ou *software* UART). Estas inicializam e detectam a presença do leitor biométrico e a antena de proximidade de alta-frequência, respectivamente. Assim sendo, pode afirmar-se que o terminal tem um comportamento tipo “*Plug-&-Play*” relativamente aos periféricos de interface série, pois consegue detectar a sua presença e activar as funções correspondentes ao periférico em questão.

A função de detecção do leitor biométrico é a seguinte:

```

Sub Bio_reset
,
    Biovec(1) = &H40          'start byte
    Biovec(2) = &H04          'command
    Biovec(3) = &H00          'low(numero_id)
    Biovec(4) = &H00          'Low2(numero_id)
    Biovec(5) = &H00          'high(numero_id)
    Biovec(6) = &H00          'high2(numero_id)
    Biovec(7) = &H00          'datasize low
    Biovec(8) = &H00          'datasize low2
    Biovec(9) = &H00          'datasize high
    Biovec(10) = &H00         'datasize high2
    Biovec(11) = &H00         'flag
    Biovec(12) = &H00         'checksum (resto de divisao por 256 da soma aritmética dos 11 bytes)
    Biovec(13) = &H0A         'stop byte
,

For A = 1 To 11
    Biovec(12) = Biovec(12) + Biovec(a)
Next A

```



```

,
  Biovec(12) = Biovec(12) Mod 256
  Print #2 , Chr(biovec(1)) ; Chr(biovec(2)) ; Chr(biovec(3)) ; Chr(biovec(4)) ; Chr(biovec(5)) ; Chr(biovec(6)) ;
  Chr(biovec(7)) ; Chr(biovec(8)) ; Chr(biovec(9)) ; Chr(biovec(10)) ; Chr(biovec(11)) ; Chr(biovec(12)) ; Chr(biovec(13));
,
  Esperasw = 0
  Do
    'buffer de input com "timeout" por contador
    Bytebio = Inkey(#2)
    Esperasw = Esperasw + 1
    Waitms 1
  Loop Until Esperasw = 2000 Or Bytebio = &H61 Or Bytebio = &H04 'espera por uma resposta do biometrico

  If Bytebio = &H61 Or Bytebio = &H04 Then
    Bio = Chr(3)
    Bio_presente = 1
  End If

  Waitms 20

  Do
    Bytebio = Inkey(#2)
    A = Ischarwaiting(#2)
  Loop Until A = 0

End Sub

```

Como se pode verificar, caso o leitor biométrico responda de maneira correcta ao comando enviado pela instrução *Print #2*, que envia o comando para a UART n.º 2, é colocado no *display* um carácter especial identificativo do leitor biométrico (Bio = Chr(3) ) e activada a variável que activa as funções relativas ao mesmo leitor ( Bio\_presente = 1 ). Os caracteres especiais para a presença do leitor de proximidade, da rede de comunicações e do leitor biométrico são definidos num editor de caracteres do *software* Bascom AVR como sendo os caracteres chr(1), chr(2) e chr(3), respectivamente.

Para detecção do leitor de proximidade criou-se a função *Swart*.

```

Sub Swuart
,
  Close #1
  Close #2
  Disable Interrupts
,
  'Cria a uart de software
  Open "comb.5:9600,8,n,2" For Output As #4 'No terminal rev1, este pino é o portb.4
  Open "comb.4:9600,8,n,2" For Input As #3 'No terminal rev1, este pino é o portb.5
,
  'comando MIF_closeSession
  Print #4 , Chr(&H80) ; Chr(&Hcc) ; Chr(&H02) ; Chr(&H00) ; Chr(&H00);

  Esperasw = 0
  Do
    Byteprox = Inkey(#3)
    Esperasw = Esperasw + 1
  Loop Until Esperasw = 1000 Or Byteprox > 0

  If Byteprox > 0 Then

    Waitms 200

  End If

'comando MIF_LoadKey
  Print #4 , Chr(&H80) ; Chr(&Hd0) ; Chr(&H80) ; Chr(&H00) ; Chr(&H06);

  Esperasw = 0
  Do
    Byteprox = Inkey(#3)
    Esperasw = Esperasw + 1
  Loop Until Esperasw = 1000 Or Byteprox > 0

```

```

If Byteprox = &HD0 Then
  Waitms 20
  Print #4 , Chr(&Hff) ; Chr(&Hff) ; Chr(&Hff) ; Chr(&Hff) ; Chr(&Hff) ; Chr(&Hff) ;

  Esperasw = 0
  Do
    Byteprox = Inkey(#3)
    Esperasw = Esperasw + 1
  Loop Until Esperasw = 10000 Or Byteprox > 0
  If Byteprox = &H90 Then
    Reset_rf = 1
    Prox = Chr(1)
  End If
End If

Close #3           'close sw uart
Close #4
Enable Interrupts

Open "com1:" For Random As #1           'abre hardware coms
Open "com2:" For Random As #2

End Sub

```

Esta função envia um comando de inicialização para o leitor de proximidade, recebendo ou não a sua resposta. Caso a resposta seja a esperada, o carácter de sinalização de leitor de proximidade presente será demonstrado no *display* ( *Prox = Chr(1)* ) e a variável que controla as funções relacionadas com este leitor é activada ( *Reset\_rf = 1* ). Um aspecto importante visível nesta função, assim como em todas as relacionadas com este periférico, é o fecho e abertura das duas portas série do processador ( *Close #1*, *Close #2*, *Open "com1"* e *Open "com2"* ). Este procedimento é necessário para que possam ser criadas portas virtuais de comunicação série de entrada ( *Open "comb.4:9600,8,n,2" For Input As #3* ) e de saída ( *Open "comb.5:9600,8,n,2" For Output As #4* ).

Para a contabilização de variáveis relacionadas com diferentes tempos utilizou-se o *Timer 1* do microcontrolador. A sua função é a seguinte:

```

Timer1_int:           'Rotina de Timer interrupt
,
  Stop Timer1         'para timer
,
  If Time_offline_var > 0 And Waitok = 1 Then
    Decr Time_offline_var
    Offline_flag = 0
  ElseIf Time_offline_var = 0 And Waitok = 1 Then
    'VALIDO
    Waitok = 0
    Offline_flag = 1
  End If
  If Time_online > 0 Then
    Decr Time_online
    Onlinebefore = 1
  ElseIf Time_online = 0 And Onlinebefore = 1 Then
    Online = Chr(32)
    Onlinebefore = 0
  End If
  If Reletime = 0 Then
    Flag_releon = 0
    Reset Ledval
  ElseIf Reletime > 0 Then
    Flag_releon = 1
    Decr Reletime
    Set Ledval

```

```

End If
If Toquetime = 0 Then
  Flag_toque = 0
Else
  Flag_toque = 1
  Decr Toquetime
End If
If Msgtime > 0 Then
  Decr Msgtime
End If
If Memtime > 0 Then
  Decr Memtime
End If
If Prox_time > 0 Then
  Decr Prox_time
End If
If Ledtemp = 0 Then
  Set Ledpow
  Reset Diag0
  Ledtemp = 29
Else
  Reset Ledpow
  Set Diag0
  Decr Ledtemp
End If
If Door_time > 0 Then
  Decr Door_time
End If
If Flag_alarm = 1 And Tempo_toca = 0 And Flag_alarm_on = 1 Then
  Flag_toca = 1
  Tempo_alarm = 30 * 120
Elseif Flag_alarm = 0 And Flag_alarm_on = 0 Then
  Flag_toca = 0
Elseif Flag_alarm_on = 0 Then
  Flag_toca = 0
End If

If Tempo_alarm > 0 Then
  Decr Tempo_alarm
Else
  Flag_alarm = 0

  Flag_toca = 0

End If
,
#if Dog
  Reset Watchdog
#endif
,
'Para maior rapidez na execução de comandos e abrir porta durante uma leitura
,
Load Timer1 , 100          'carrega timer
Start Timer1              'inicia timer
Return

```

Na rotina de interrupção do *Timer1* as variáveis que marcam os tempos são descontadas com uma frequência constante, o que permite um controlo aproximado de tempos. Algumas variáveis aqui utilizadas descontam o tempo de abertura das saídas (Reletime), o tempo de exibição das mensagens no *display* (Msgtime), o tempo dos toques (Toquetime), entre outros.

Para que o terminal interaja com o *software*, foi necessário criar um protocolo de comunicações específico, disponível em parte no ANEXO 9, por motivos de confidencialidade.

Assim, como estrutura de base temos:

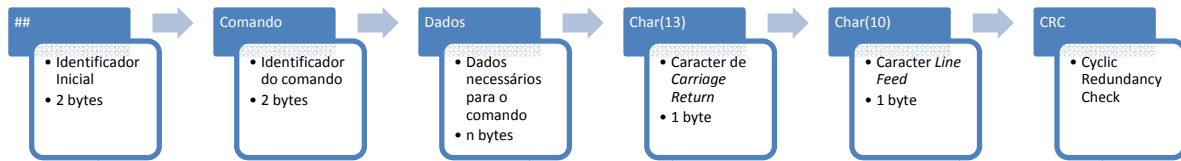


Figura 3.5 - Estrutura do protocolo de comunicações do sistema.

A figura 3.5 pretende demonstrar que os campos de identificador inicial, *carriage return*, *line feed* e CRC são comuns em todos os pacotes de comunicação. Assim sendo, os campos que variam são o campo identificador do comando em questão e os dados inerentes ao comando utilizado.

Como caracteres de início do comando são usados dois cardinais ##, identificando que o comando segue logo de seguida. Para término do comando, são enviados os caracteres de CR e LF, finalizando com o CRC.

O CRC tem como objectivo o controlo de erros, sendo que este é um *Exclusive Or* (XOR) lógico de todo o pacote. Desta forma, caso o CRC enviado não coincida com o CRC calculado, o pacote é descartado como sendo inválido.

Como se pode constatar, todos os comandos têm uma estrutura comum. Esta foi criada de forma a facilitar a interpretação e descodificação. De seguida é apresentado um excerto da função de comunicação do *firmware*.

Sub Cip

```

Algo = 0
Byteuart = 0
Flag_cip = 0
Flag_cip2 = 0
  
```

```

Buffertemp = ""
Do
  
```

```

    Byteuart = Inkey(#1)
    Esperasw = Esperasw + 1
    If Byteuart = "#" And Flag_cip = 0 Then
      Waitms 1
      Byte_array(1) = Byteuart
      Byteuart = Inkey(#1)
    
```

```

    If Byteuart = "#" And Flag_cip = 0 Then
      Flag_cip = 1
      Byte_array(2) = Byteuart
      Esperasw = 0
    
```

```

    Call Cip2
    Byte_array(3) = Inkey(#1)
    Call Cip2
    Byte_array(4) = Inkey(#1)
  
```

```

End If
Loop Until Esperasw = 50000 Or Flag_cip = 1
  
```

protocolo

'espera pelo ## de fim de inicio das instruções do

```

If Flag_cip = 1 Then
  Algo = 1
  Reset Diag1
End If
If Algo = 1 Then
  Okflag = 0
  
```

```

Koflag = 0
For Conta = 0 To 255

Comando_cf:                                     'Modo de configuração
If Byte_array(3) = "C" And Byte_array(4) = "F" Then
Call Cip2
Configuracao = Inkey(#1)
If Configuracao = "1" Then
Locate 3 , 3
Lcd Msg_configuracao
Sound Buzz , 400 , 500
'ENVIAR OK
Else
Call Company_name
Goto Reset_term
End If

Okflag = 1
Command_code = "CF"
Call Enviarokko
Exit For                                     'testado

Comando_ms:                                     'Envio de Mensagem (16 caracteres)
Elseif Byte_array(3) = "M" And Byte_array(4) = "S" Then
Locate 4 , 3
Vartemp = 0
Buffer_msg = ""
For B = 1 To 16
Call Cip2
Byteuart = Inkey(#1)
Buffer_msg = Buffer_msg + Chr(byteuart)
Next B
Lcd Buffer_msg
Msgtime = 30 * Time_msg
'ENVIAR OK
Okflag = 1
Command_code = "MS"
Call Enviarokko
Exit For

```

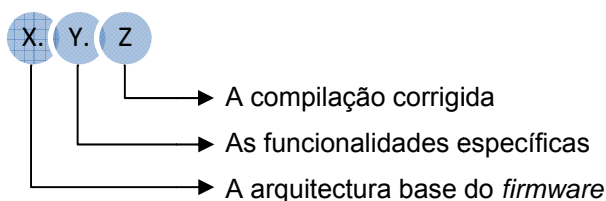
(...)

Neste pequeno excerto podem ver-se as respostas aos comandos CF e MS.

Em CF a função identifica as letras CF depois dos caracteres iniciais ## e recebe o parâmetro seguinte. Caso este parâmetro seja "1", é activado o modo de configurações do terminal e enviado um OK ao *software*. Caso seja diferente, o terminal é reiniciado.

Em MS a função identifica as letras MS depois dos caracteres iniciais ## e recebe a mensagem de 16 caracteres para a colocar no *display* do terminal ( *Lcd Buffer\_msg* ).

A nomenclatura das várias versões de *firmware* compiladas teve como regra o seguinte:



Os *firmwares* foram desenvolvidos a partir da versão base 4.1.1, e foram recompilados com funcionalidades específicas para diferentes aplicações. As especificações do *firmware* de base são:

- Ecrã de caracteres tipo 16x2 (colunas x linhas)
- Conversor de comunicação série para rede LAN com ou sem fios
- Funções de toques com 16 toques configuráveis
- Memória para 2000 marcações sem comunicação com o *software*
- Controlo de acesso de 4000 utilizadores
- Sinais de saída de 12 V para controlo de dispositivos externos, como por exemplo um trinco eléctrico ou uma buzina eléctrica.
- Entrada de sinais de sensores, como por exemplo botões de abertura manual de portas ou sensores de detecção de fumo e intrusão.
- Modo de alarme com impressões digitais de activação e desactivação.
- Gravação de impressões digitais directamente no terminal a partir do teclado.
- Função de *timediff*, que não permite duas marcações simultâneas do mesmo utilizador num espaço de n minutos.

Seguidamente é apresentada uma tabela com as versões compiladas:

Tabela 3.2 - Versões Compiladas do Firmware

<b>Versão</b>	<b>Funcionalidades Especiais</b>
4.1.1	Compatível com leitores de proximidade <i>MIFARE</i>
4.2.1	Compatível com leitores de proximidade <i>iClass</i>
4.3.1	Compatível com leitores de proximidade <i>ISOPROX</i>
4.4.1	Compatível com leitor de cartões magnéticos
4.5.1	Compatível com leitores de proximidade <i>MIFARE</i> e com modem GPRS

Desta forma, e devido à limitada memória de programa do ATmega64, é necessário proceder à instalação do *firmware* correcto para cada tipo de utilização, não sendo possível contemplar todos os periféricos disponíveis numa única versão configurável.

Existem ainda outras características importantes do sistema. Um dos elementos mais críticos é a memória de dados recolhidos, com os utilizadores e os horários de utilização correspondentes. Os dados são armazenados em duas EEPROMs externas ao microcontrolador, o que previne a perda de dados em caso de falha de energia.

Relativamente aos erros provocados pelo *firmware*, este tem um temporizador de *Watchdog*, que faz com que o microcontrolador reinicie em caso de bloqueio do *firmware*.

A programação do terminal é efectuada por uma aplicação de configuração, a mesma que define o método de autenticação a ser utilizado por cada utilizador. Assim, num mesmo terminal, podemos ter utilizadores a utilizar apenas impressão digital, outros a utilizar apenas cartão de proximidade, outros a utilizar PIN e ainda outros a utilizar qualquer conjugação destes. Também os periféricos podem ser activados ou desactivados, restringindo assim os métodos de autenticação para todos os utilizadores ao mesmo tempo.

Do ponto de vista do utilizador comum registado, o sistema é o mais simples e directo possível. Para o utilizar, o utilizador necessita apenas de apresentar o seu método de autenticação e esperar pela análise e resposta do sistema. Esta resposta é transmitida através de um sinal sonoro e através de uma mensagem no *display* e/ou uma luz verde ou vermelha, para o caso de válido ou inválido, respectivamente.

Estas e outras funções fazem parte do *firmware* que, como referido anteriormente, é bastante extenso e confidencial, sendo no entanto suficientes para demonstrar o tipo de programação desenvolvida.

### **3.4 – Conclusão do capítulo**

Depois da identificação dos periféricos a utilizar no sistema, foi necessária a sua efectiva integração. Neste capítulo foram identificados alguns aspectos importantes referentes à arquitectura do sistema.

Inicialmente foram identificadas as funcionalidades necessárias para que o sistema cumprisse os objectivos. De seguida foram caracterizados alguns aspectos importantes na integração dos diferentes periféricos. Por último é caracterizado o desenvolvimento do *firmware*, desde a estrutura geral até algumas funções em particular.

Assim, e após todo o processo de integração e desenvolvimento, foi possível obter um sistema piloto funcional que satisfazia os critérios inicialmente propostos. No capítulo seguinte será abordada a aplicação do sistema desenvolvido no mercado, e a sua característica multifacetada.





## Capítulo 4

### Aplicação e utilização

O sistema desenvolvido pode ser utilizado em diversas aplicações de controlo de ponto e acesso. A empresa utilizou-o para criar uma gama diferenciada de novos produtos, todos com o mesmo núcleo de processamento e periféricos variáveis com a aplicação pretendida. Estes divergem apenas na aparência exterior e em algumas funcionalidades, consoante os periféricos escolhidos. Todas elas estão preparadas para o controlo de ponto e de acesso do cliente, conforme o seu método de aquisição de dados.

Alguns dos produtos resultantes são neste momento comercializados pela empresa New Betronic e encontram-se instalados em clientes de referência, como por exemplo:

- Hospital Garcia da Horta – Almada (Sib Tower)
- Câmara Municipal da Amadora (Sib Zone)
- Hospital Geral de Santo António – Porto (Sib Zone e Sib Tower)
- Câmara Municipal de Estarreja (Sib Zone)
- Hospital José Maria Grande – Portalegre (Sib Enterprise)
- Hospital Santa Luzia – Elvas (Sib Enterprise)
- Instituto Piaget – Almada e V.N.Gaia (Sib Park)

Este sistema pode ser aplicado em qualquer cliente com necessidade de controlo de ponto e/ou acesso, podendo a autenticação ser efectuada por biometria, cartão de proximidade, cartão magnético, PIN de teclado ou mais que um em simultâneo.

Paralelamente ao terminal, foi desenvolvido pelo departamento de *software* da empresa uma aplicação para gestão dos dados recolhidos pelo terminal. Essa aplicação foi apelidada de SibCom, e serve de interface entre o terminal e o *software* de controlo de ponto. O SibCom

também está habilitado para configurar e parametrizar o terminal desenvolvido, mediante um Protocolo de Comunicações criado no decorrer do projecto.

## 4.1 - Terminais

A arquitectura SIB3000 permitiu criar uma grande variedade de terminais de controlo de ponto e acesso. Aqui são apresentados alguns dos terminais criados a partir deste sistema, cada um com a sua especificidade e aplicabilidade, mas todos com as mesmas características internas de placa principal e periféricos.

### 4.1.1 – Terminal SibZone

Terminal de fácil instalação e utilização, pode utilizar autenticação por impressão digital, cartão de proximidade ou ambos. Para feedback com o utilizador, possui um *display* alfanumérico tipo 16x2, um besouro interno, leds de status e de válido ou inválido. (ANEXO 10)



Figura 4.1 - Imagem do terminal SibZone.

Este sistema permite a utilização com biometria e antena de proximidade. Cabe ao cliente decidir o método de autenticação a utilizar por cada utilizador. Neste caso, os métodos possíveis são:

- Cartão de proximidade
- Cartão de proximidade mais impressão digital (comparação biométrica 1:1)
- Impressão digital (comparação biométrica 1:N)

Este é o terminal base da solução, pois é o mais simples e fácil de instalar.

#### 4.1.2 – Terminal SibTower

Terminal com um aspecto mais consistente, não necessita de parede para ser instalado. Pode ser utilizada a autenticação por impressão digital, cartão de proximidade ou ambos. Como o Sibzone, este também possui para feedback com o utilizador um display alfanumérico tipo 16x2 e um besouro interno. (ANEXO 11)



Figura 4.2 - Imagem do terminal SibTower.

Este sistema permite a utilização com biometria e antena de proximidade. Cabe ao cliente decidir o método de autenticação a utilizar por cada utilizador. Neste caso, os métodos possíveis são:

- Cartão de proximidade
- Cartão de proximidade mais impressão digital (comparação biométrica 1:1)
- Impressão digital (comparação biométrica 1:N)

As vantagens deste terminal face ao SibZone são o facto de possuir um *display* de caracteres de maiores dimensões e de não ser necessária uma parede para o fixar, podendo ser aplicado directamente no chão.

#### 4.1.3 – Terminal MiniSib

Terminal de encastrar, anti-vandalismo, com autenticação por impressão digital e feedback para o utilizador por besouro e leds de válido ou inválido. (ANEXO 12)



Figura 4.3 - Imagem do terminal MiniSib.

Este sistema permite a utilização apenas com biometria. Neste caso, a única hipótese para o utilizador será a de utilizar a sua impressão digital para o reconhecimento.

A grande vantagem deste terminal é o facto de este ficar embutido na parede e não ter *display*, sendo um terminal anti-vandalismo extremamente robusto.

#### 4.1.4 – Terminal SibStrong

Terminal completamente em aço inoxidável, destaca-se pela sua robustez. Este é voltado para o exterior e o anti-vandalismo. (ANEXO 13)



Figura 4.4 - Imagem do terminal SibStrong.

Este sistema permite a utilização com biometria e antena de proximidade. Cabe ao cliente decidir o método de autenticação a utilizar por cada utilizador. Neste caso, os métodos possíveis são:

- Cartão de proximidade

- Cartão de proximidade mais impressão digital (comparação biométrica 1:1)
- Impressão digital (comparação biométrica 1:N)

As vantagens deste terminal face ao SibZone são o facto de possuir um *display* de caracteres de maiores dimensões e ser feito em alumínio, o que o torna bastante resistente.

#### 4.1.5 – Terminal SibPark

Terminal vocacionado para o controlo de acesso a parques de estacionamento automóvel, é montado dentro de uma torre para fácil acesso a partir de uma viatura, e controla uma cancela motorizada para permitir ou negar o acesso ao utilizador. (ANEXO 14)



Figura 4.5 - Imagem do sistema SibPark.

Este sistema permite a utilização cartão magnético e antena de proximidade. Cabe ao cliente decidir qual o método que pretende utilizar para a entrada das viaturas.

A grande vantagem deste terminal é o seu desenho especialmente concebido para fácil utilização a partir de um automóvel, necessitando o utilizador apenas de baixar o vidro e apresentar o cartão para que se faça a autenticação.

#### 4.1.6 – Terminal SibZone Enterprise

Terminal multifuncional que, para além de todas as características do SibZone, tem um teclado. Este pode ser utilizado para autenticação no sistema ou para configurar o próprio terminal (ANEXO 14)



Figura 4.6 Imagem do sistema SibZone Enterprise.

Este sistema permite a utilização com biometria, antena de proximidade e teclado. Cabe ao cliente decidir o método de autenticação a utilizar por cada utilizador. Neste caso, os métodos possíveis são:

- Cartão de proximidade
- Impressão digital (comparação biométrica 1:N)
- Teclado mais impressão digital (comparação biométrica 1:1)
- PIN numérico por teclado
- Qualquer combinação dos três anteriores.

As vantagens deste terminal face ao SibZone são o facto de ser possível alterar configurações do terminal sem *software*, apenas utilizando o teclado, e a possibilidade de um utilizador ser reconhecido através de um PIN numérico.

Os periféricos de todos os terminais podem ser alterados pelo cliente no momento da compra. Por exemplo, se um utilizador pretender comprar um SibZone apenas para uso de cartão de proximidade, pode adquirir o terminal sem o custo adicional do leitor biométrico, ficando assim mais barato. Portanto, as configurações aqui apresentadas são as mais completas possíveis do respectivo terminal.

Relativamente às comunicações, cada um destes terminais poderá ser montado com adaptador para rede local LAN, redes sem fios WLAN ou redes móveis GPRS, sendo do cliente essa decisão.

O projecto trouxe a base para que a empresa pudesse desenvolver todos estes diferentes terminais, sendo portanto uma mais-valia para o crescimento económico da mesma.

## Capítulo 5

# Conclusões e Perspectivas de Desenvolvimento

Este projecto foi extremamente importante para o conhecimento e manuseamento de ferramentas de identificação pessoal. As perspectivas de desenvolvimento são grandes, principalmente na interacção com o utilizador.

Relativamente à arquitectura utilizada, esta pode ser evoluída para uma arquitectura tipo PC, com um visual mais gráfico e moderno. Com uma arquitectura deste tipo, como por exemplo a PC104, é possível a gestão de uma muito maior quantidade de informação e interacção do utilizador com o sistema. Poder-se-ia, por exemplo, com um ecrã gráfico colorido e sensível ao toque fazer consultas à base de dados, de forma a actualizar informações pessoais, aceder a saldos de contas, planeamento de férias, entre outros.

Relativamente aos métodos de reconhecimento biométrico, estes estão a evoluir rapidamente para métodos cada vez mais fiáveis e difíceis de falsificar.

Um dos métodos mais promissores é o de reconhecimento do padrão das veias. Começam a existir no mercado novos leitores que se baseiam em frequências de luz não visível para obter o traçado das veias, quer do dedo, quer da mão.

Um exemplo de um sistema de reconhecimento biométrico que utiliza o dedo é o VeinID da Hitachi. Um exemplo de um sistema de reconhecimento biométrico que utiliza a palma da mão é o PalmSecure da Fujitsu. Ambos os sistemas emitem luz e recolhem o reflexo das ondas de infra-vermelhos originado nas veias da mão humana [29].

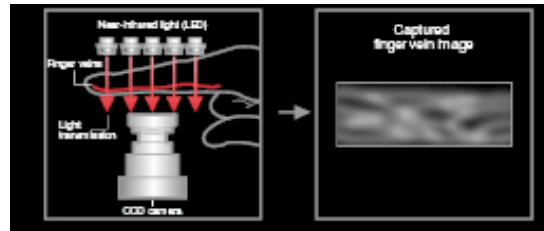


Figura 5.1 - Ilustração do método de autenticação por reconhecimento das veias [27].

Este projecto teve como objectivo o desenvolvimento de um sistema de controlo de ponto e acesso para a empresa New Betronic, que foi plenamente alcançado.

Inicialmente, foi feito um estudo de mercado, de modo a compreender qual seria a melhor tecnologia biométrica a ser explorada no novo sistema. O método que mais se adequou ao sistema desenvolvido foi o de reconhecimento de impressão digital. Foi feita uma análise a vários periféricos, de modo a identificar quais seriam mais vantajosos de serem integrados no sistema. Foi utilizado um leitor biométrico de impressão digital da marca Suprema,

A fase de integração foi a mais demorada, pois foi necessário juntar todos os periféricos e desenvolver um *firmware* para o controlo do sistema. Uma das grandes dificuldades iniciais da fase de integração foi a linguagem de programação BASIC, pelo simples facto de que esta nunca tinha sido utilizada pelo aluno. Depois de superada a etapa da aprendizagem da sintaxe, foi um processo demorado de integração de periféricos um por um, e de construção de funções de *firmware* para objectivos especiais.

O projecto não desenvolveu apenas um terminal, mas um sistema flexível, o que permitiu a criação de vários terminais com características distintas. Este é um factor importante, pois permite uma rentabilização do esforço dispendido no decorrer do projecto, assim como dos módulos que o constituem. Assim, para a empresa fabricar qualquer um dos terminais apresentados, utiliza sempre a mesma placa principal, e um *firmware* ligeiramente alterado para o terminal em questão.

O mercado do controlo de ponto e acesso é um mercado em constante evolução, o que levará este sistema a ter uma evolução a nível tecnológico no futuro. No momento em que este relatório foi escrito já tinha sido feito na empresa um relatório de pesquisa e análise das tecnologias PC104, e já tinham sido feitos os contactos com a Hitachi, de forma a obter mais informações sobre o seu VeinID.

Assim, pode concluir-se que este projecto foi um sucesso para a empresa, pois permitiu a criação de uma nova gama de produtos já instalados em diversos clientes de referência.



## Referências

- [1] Wikipédia. “Biometria”. Disponível em <http://pt.wikipedia.org/wiki/Biometria>. Acesso em 15/Maio/2008.
- [2] John D. Woodward, Jr., Katharine W. Webb et al, “Army Biometric Applications: Identifying and Addressing Sociocultural Concerns”, Proceeding of RAND, ISBN: 0-8330-2985-1, pp. 185, 2001.
- [3] S.A.R. Zaidi, S.M.H. Zaidi, K. Samad, Ahmad Ali Iqbal, “Simplified Static Image Face Detection Algorithm”, Proceedings of First International Conference on Information & Communication Technology (ICICT 2005), Pakistan, August 2005.
- [4] “Security Technical Implementation Guide”, Report by DISA Field Security Operations, V1 R 2, August 2004.
- [5] Roland Piquepaille’s Technology Trends. “3D Biometric Facial Recognition Comes to UK”. Disponível em <http://www.primidi.com/2004/11/26.html>. Acesso em 16/Maio/2008
- [6] Burleson Consulting. “Using fingerprints as tables primary keys”. Disponível em [http://www.dba-oracle.com/t\\_fingerprint\\_primary\\_keys.htm](http://www.dba-oracle.com/t_fingerprint_primary_keys.htm). Acesso em 16/Maio/2008.
- [7] Fidis. “A study on PKI and biometrics”. Disponível em <http://www.fidis.net/resources/deliverables/hightechid/int-d32000/doc/20/>. Acesso em 15/Maio/2008.
- [8] Mitsubishi Electric Research Laboratories. “Íris Recognition from 1-2 Meters”. Disponível em <http://www.merl.com/projects/irisrecognition/>. Acesso em 15/Maio/2008.
- [9] Roland Piquepaille’s Technology Trends. Disponível em [http://www.primidi.com/images/sign\\_and\\_go.jpg](http://www.primidi.com/images/sign_and_go.jpg). Acesso em 16/Maio/2008.
- [10] K. P. Khushk, A. A. Iqbal, “An Overview of leading biometrics Technologies used for human identity”, IEEE Student Conference on Engineering Sciences and Technology, 2005; 27 August 2005.
- [11] Biometrics. “Speaker Recognition”. Disponível em <http://www.biometrics.gov/MediaRoom/speaker.aspx>. Acesso em 15/Maio/2008.
- [12] Nacional Center for State Courts. “Biometrics Comparison Chart”. Disponível em <http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html>. Acesso em 15/Maio/2008.

- [13] Chinastars. "Fingerprint Module". Disponível em <http://chinastars.hisupplier.com/product-32052-fingerprint-module.html> Acesso em 16/Maio/2008.
- [14] Griaule Biometrics. "Frequent Questions and Answers". Disponível em <http://www.griaulebiometrics.com/page/en-us/FVCFAQ> Acesso em 19/Maio/2008.
- [15] Suprema Inc. "SFM-3000 Series". Disponível em [http://www.supremainc.com/eng/product/em\\_15.php?mark=215](http://www.supremainc.com/eng/product/em_15.php?mark=215). Acesso em 20/Maio/2008
- [16] Wikipédia. "RFID". Disponível em <http://pt.wikipedia.org/wiki/RFID>. Acesso em 20/Maio/2008
- [17] HID Corporation. "iClass". Disponível em [http://www.hidcorp.com/prod\\_detail.php?prod\\_id=62](http://www.hidcorp.com/prod_detail.php?prod_id=62). Acesso em 20/Maio/2008.
- [18] STID. "13.56 MHZ RFID Module". Disponível em [http://www.stid.com/produits.php?gamme\\_commerciale\\_id=22&famille\\_id=3&modele\\_id=51&version\\_id=143](http://www.stid.com/produits.php?gamme_commerciale_id=22&famille_id=3&modele_id=51&version_id=143). Acesso em 20/Maio/2008.
- [19] HID Corporation. "HID Proximity". Disponível em [http://www.hidcorp.com/prod\\_detail.php?prod\\_id=63](http://www.hidcorp.com/prod_detail.php?prod_id=63). Acesso em 20/Maio/2008.
- [20] Farnell. "Keypads". Disponível em <http://pt.farnell.com/1130806/electrical-circuit-protection/product.us0?sku=eao-eco16250-06>. Acesso em 16/Maio/2008.
- [21] CardCom. "Manual Swipe Type Magnetic Card Reader". Disponível em <http://www.cardcom.com/CARDCOMWEB/kdr1000.html>. Acesso em 20/Maio/2008.
- [22] Lantronix. "Embedded Networking". Disponível em <http://www.lantronix.com/device-networking/embedded-device-servers/>. Acesso em 20/Maio/2008.
- [23] Wikipédia. "GPRS". Disponível em <http://pt.wikipedia.org/wiki/Gprs> . Acesso em 20/Maio/2008
- [24] ComTech M2M. "GSM modem module – OEM-GPRS2E". Disponível em <http://www.comtechm2m.com/embedded-modem/embedded-modem-gsm-gprs.htm>. Acesso em 20/Maio/2008.
- [25] Bascom AVR. Manual de utilização da ferramenta de desenvolvimento.
- [26] Arihav. Datasheet do leitor de cartões magnéticos modelo KDR-1932. 2002.
- [27] Hitachi. "Finger Vein Authentication". Disponível em <http://www.hitachi-eu.com/veinid/Technical%20Facts/How%20FV%20works.html>. Acesso em 20/Maio/2008
- [28] Rice, J. Goodwin, B. "Biometric Access and Use Systems", IEEE Colloquium on Vehicle Security, 25 October 1990.
- [29] Cross, J.M. Smith, C.L. "Thermigrafic imaging of subcutaneous vascular network of the back of the hand for biometric identification", IEEE International Carnahan Conference on Security Technology, 20 October 1995.

## **Anexos**



# **Anexo 1**

*Waterproof Standalone Fingerprint Module for Outdoor*

# SFM3030-OD



SFM3030-OD is a standalone fingerprint identification module for outdoor applications. The front side of optical sensor is designed to be IP65 rated against rain and dust. Combined with a wide temperature range and solid sensor surface, SFM3030-OD is an ideal solution for rugged and durable biometric products.

## Features

- Rugged optical fingerprint sensor
  - IP65 rated waterproof front side
  - Solid and scratch-free sensor surface
  - High quality fingerprint image for both dry and wet fingers
- Award winning fingerprint algorithm (No 1 in FVC2004)
- Industry's fastest 1:1 and 1:N matching speed
- Low power consumption and fast power-on time
- Serial interface with simple protocol
- User-configurable 8 port digital I/O
- Easy template distribution for network applications



**SUPREMA**

## Specifications

CPU	400 MHz DSP
Flash memory	1 MB / 4 MB (extendible up to 4 MB upon request)
EER	< 0.1%
Enrollment time	800 msec
1:1 Verification time	800 msec
1:1000 identification time *	970 msec
Template size	256 ~ 384 Bytes (configurable, 384 Bytes default)
Template capacity	1,900 at 1 MB flash (9,500 at 4 MB flash)
Host communication	Asynchronous serial, CMOS level (3.3V) 9600/19200/38400/57600/115200 bps
External I/O	8 ports, configurable digital I/O. Easy to configure I/O events and signal patterns. 26bit wiegand output is supported in 3.3V level.
Encryption	256 bit AES (fingerprint data protection)
Supply voltage	3.3 Vdc regulated
Operating temperature	-20 ~ 70°C
Sensor type	Optical
Resolution	500 (dpi)
Sensing area	15.9 x 17.9 (mm)
Image size	288 x 288 (pixel)
IP rating **	IP65
Dimension (Main board)	55mm x 40mm x 8mm (WxLxH)
Dimension (Sensor)	21mm x 23mm x 54mm (WxLxH)

\* average 1:1000 genuine identification time including feature extraction time

\*\* apply to the top front side of optical sensor

## Functions

- Enrollment / 1:1 verification / 1:N identification
- User data management
- System parameter configuration

## Applications

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>• Access control</li> <li>• Door lock</li> <li>• Safes &amp; Vaults</li> </ul> | <ul style="list-style-type: none"> <li>• Time and attendance</li> <li>• POS</li> <li>• ATM</li> </ul> |
|---|---|

## Evaluation Kit

SFM3030-OD evaluation kit allows a user to evaluate the module's functionality quickly and easily. The evaluation kit also provides software tools, SDK and technical documents to help customers in application development.

Contents:

- SFM3030-OD
- SFM evaluation board
- SFM SDK
- PC interface program with source code
- Technical documents

For sales and inquiries, please contact:

## Suprema Inc.

16F Parkview Office Tower, Jeongja-dong, Bundang  
Seongnam, Gyeonggi, 463-863 Korea  
Tel: +82-31-783-4502, Fax: +82-31-783-4503  
E-mail: sales@supremainc.com  
Homepage: <http://www.supremainc.com>

## **Anexo 2**



# iCLASS<sup>®</sup> OEM50 Module

Contactless Smart Card Module • Read/Write • Wiegand/TTL Interface • 3131



## ACCESS flexibility.

Designed for embedding into OEM equipment as a component in upper level assemblies, the iCLASS<sup>®</sup> OEM50 Module is a 13.56 MHz contactless smart card reader/writer in an extremely compact printed circuit board form factor.

The OEM50 enables iCLASS technology to be used for multiple applications including cashless vending, biometrics, time and attendance, alarm system control, HVAC control, process control, and point-of-sale terminals.

With only a two-wire serial interface and a regulated power supply, an OEM has the power of iCLASS at their fingertips.

The OEM50 is designed to operate with a wide variety of antenna configurations. HID offers optional antenna PCBs in 3.15" x 3.15" (80 mm x 80 mm) and 1.34" x 1.89" (34 mm x 48 mm) sizes, and also provides a comprehensive antenna design guide for OEMs. Separating the antenna from the module allows the OEM to make the most efficient use of available space, and allows the module to be installed in a metal enclosure while the antenna is remotely located behind a non-conductive bezel.

Inputs and outputs are all TTL level logic. Transient suppression, voltage regulation, and output drivers will be provided by the Host device. A user guide (Part Number 3131-901) provides complete interface specifications.

When used with iCLASS cards, the OEM50 offers security features such as RF data encryption and mutual authentication using 64-bit keys for each application area and optional DES or Triple DES data encryption for the HID application area. HID provides key management for access control and other data stored in the HID application area.

For access control applications, the OEM50 can read either iCLASS credentials (transmitting the Wiegand formatted data as encoded), MIFARE<sup>®</sup> Standard, Ultralight, or DESFire<sup>®</sup> credentials (transmitting Wiegand data based on the card serial number in 26-, 32-, 34-, 40-, or 56-bit formats). For non-access control applications, the OEM50 module can read or write to any application area on the iCLASS credential, with all reader functions controlled by an external Host processor via the TTL port using the iCLASS Serial Protocol.

The OEM50 has a logic level control output which can be operated by serial commands via the TTL port. This can be used to control external devices or audiovisual indicators with the appropriate driver circuitry.

When the configurable Hold Control Line is asserted, either all card reading is disabled or the module will buffer one card read and ignore subsequent reads until the line is released.

## Features

### Card Compatibility

The iCLASS® OEM50 Module is compatible with all iCLASS credentials. The module's versatility allows it to read credentials meeting several ISO standards:

- 15693 – read/write (2k bit and 16k bit iCLASS credentials)
- 14443A - read only (MIFARE® card serial number)
- 14443B - read/write (16k bit iCLASS credential)

### Application Support

HID offers Certification Training, as well as a Software Developer's Kit (available separately; consult factory for details). See HID Application Note 28 for details.

### Mounting

The module can be mounted on standoffs, using the four slots located at each corner of the PCB, sized for a #2-56 screw (maximum screw head or standoff diameter is 0.20" or 5.0 mm). The module can also be mounted by installing PCB mount pin headers and installing compatible sockets on the host device.

Metal components located near the antenna may reduce the card reading distance of the module. The antenna will NOT read cards or tags if completely enclosed in a metal enclosure. (If a metal enclosure is required, the antenna can be remotely located behind a non-metallic bezel.)

### Environmental

If used in outdoor environments, the module must be epoxy potted or installed in a watertight enclosure.

### Warranty

Warranted against defects in materials and workmanship for one year. (See complete warranty policy for details.)

### Part Numbers

Base Part Number: 3131  
Antennae: Consult Factory

### Options:

Key Management - Standard or Custom  
Selectable Output Type (for MIFARE Cards)  
Standard Termination: none; solder pads and vias provided  
Programmable Control Output Operation (logic level)

## Specifications

### Typical Maximum Read Range

Dependent upon antenna design, enclosure design, exciter voltage, materials used, and proximity of metal components.

### Dimensions

PCB: 1.10" x 1.20" (27.94 mm x 30.48 mm)  
Large Antenna: 3.15" x 3.15" (80 mm x 80 mm)  
Small Antenna: 1.35" x 1.90" (34 mm x 48 mm)

### Component Height

Top: 0.10" (2.5 mm) max  
Bottom: 0.10" (2.5 mm) max

### Material

FR-4 Fiberglass laminate

### Power Requirements

Nominal input: 5VDC +/- 15%  
Regulated DC power required

### Input Voltage Range

Processor: 5VDC +/- 0.250 V  
Exciter: 4.75 - 8.0 VDC

### Current Requirements

Peak current (based on exciter input)  
93 mAmp at 5VDC; 121 mAmps at 8 VDC  
Average current: Consult Factory

### Operating Temperature

-35° to 65° C (-31° to 150° F)

### Operating Humidity

5% to 95% relative humidity non-condensing

### Weight

Consult Factory

### Transmit Frequency

13.56 MHz

### Pending Certifications

cURus - UL Recognized for electrical safety  
(US and Canada) OEM or integrator must secure regulatory approvals for the entire integrated device, consisting of the module and OEM components.  
IP55

### Cable Distance

I/O and power connections – 1' (30 cm)  
Wiegand/Serial TTL Interface – 1' (30 cm)  
Antenna Cable  
50-Ohm MCX Coax – Consult Factory  
24 AWG twisted pair – up to 3.0" (76 mm)

© 2007 HID Global. All rights reserved. HID, the HID logo, and iCLASS are trademarks or registered trademarks of HID Global in the U.S. and/or other countries. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners. Rev. 3/2007



For best results, please  
print on recycled paper.

MKT-OEM50\_DS\_EN



**ACCESS** experience.

[hidcorp.com](http://hidcorp.com)

#### HID Global Offices:

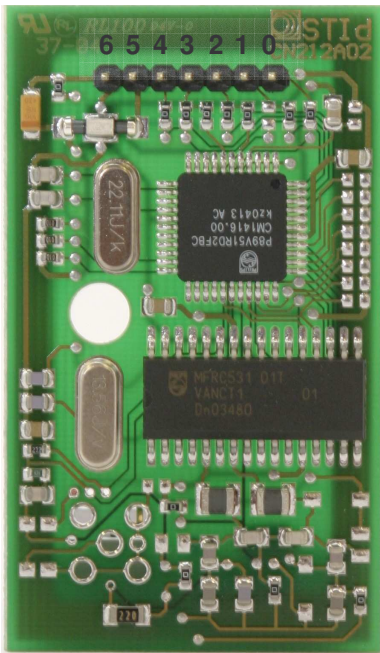
**Corporate**  
**North America**  
9292 Jeronimo Road  
Irvine, CA 92618-1905  
U.S.A.  
Phone: (800) 237-7769  
Phone: (949) 598-1600  
Fax: (949) 598-1690

**Asia Pacific**  
19/F 625 King's Road  
North Point  
Island East  
Hong Kong  
Phone: +852 3160-9800  
Fax: +852 3160-4809

**Latin America**  
Circunvalacion Ote. #201 B  
Despacho 2  
Col. Jardines del Moral  
Leon 37160, Gto.  
Mexico  
Phone: +52 477 779 1492  
Fax: +52 477 779 1493

**Europe, Middle East & Africa**  
Homefield Road  
Haverhill, Suffolk  
CB9 8QP  
England  
Phone: +44 (0) 1440 714 850  
Fax: +44 (0) 1440 714 840

## **Anexo 3**



### Usage recommendations

- **Important:** Max. distance between the module and the controller board: **0,5 m**
- Power supply tension at the reader's connector should be strictly comprised between **4.5V and 5.5V**. Filtered regulated power supply is highly recommended.
- Keep the reader away from computer or power cables as much as possible. They can generate an electrical perturbation that is function of their proximity and radiation level.
- Distance to respect between two modules:  
parallel plan: 30 cm – Same plan: 40 cm – Perpendicular: 25 cm.

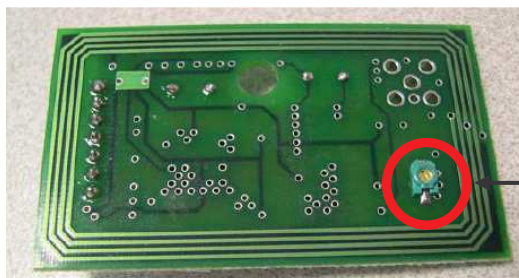
Pin number		6	5	4	3	2	1	0
ISO 2 (2x)	Description	0 V	+ 5 V	code	data	clock	Mode	Nc
	Type of signal	input	input	output	output	output	Input	-
Wiegand(3x)	Description	0 V	+ 5 V	data0	data1	clock	Mode	Nc
	Type of signal	input	input	output	output	output	Input	-
RS232 TTL (5X)	Description	0 V	+ 5 V	Setup	Tx	Rx	Read	Nc
	Type of signal	input	input	input	output	input	Input	-

- Pin 0 (nc) must remains unconnected
- Data signal are TTL compliant

**Caution:** RS232 TTL modules must not be directly connected to a RS232 COM port. You have to use a RS232 ⇔ RS232 TTL converter.

### Antenna tuning:

If the reading distances are reduced after the module has been fitted to its final place, you can adjust the antenna. Use a thin screwdriver to modify the capacitor value.



Adjustable capacitor

## **Anexo 4**

# MCAK1604NBWB



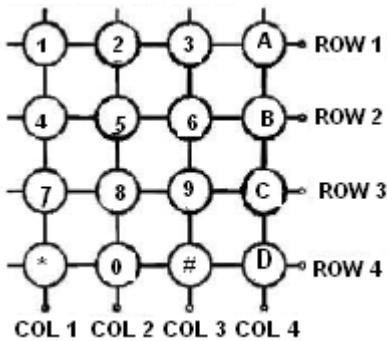
## Keypads



### Specifications:

Contact Rating	: 20mA, 24V dc.
Maximum Contact Resistance	: 200Ω.
Life	: 1,000,000 cycles per key.
Operating Temperature	: -20°C to +60°C.
Storage Temperature	: -40°C to +65°C.

### Standard Matrix Circuit Diagram:

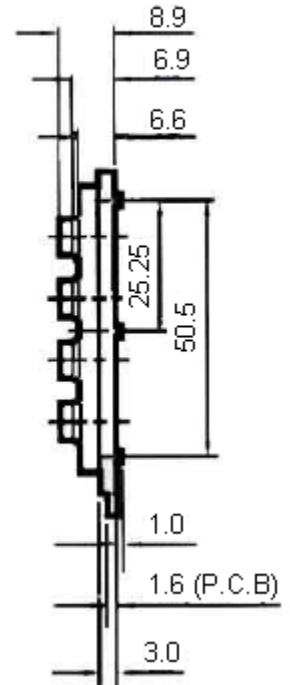
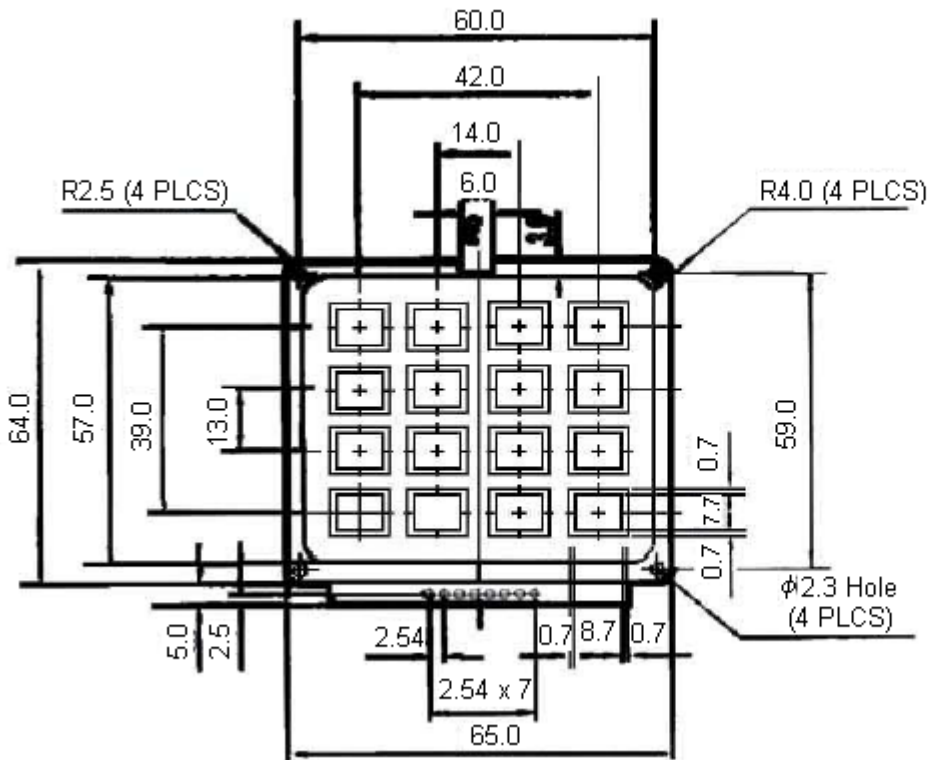


Output Arrangement	
Output Pin Number	Symbol
1	COL 1
2	COL 2
3	COL 3
4	COL 4
5	ROW 1
6	ROW 2
7	ROW 3
8	ROW 4



# MCAK1604NBWB

## Keypads



Actuating Force : 100 ±30 grams.  
Stroke : 1.5 ±0.5mm

Dimensions : Millimetres

### Part Number Table

Description	Part Number
Keypad, 4 x 4 Plastic	MCAK1604NBWB



### Notes:

### International Sales Offices:



**AUSTRALIA – Farnell InOne**  
Tel No: ++ 61 2 9645 8888  
Fax No: ++ 61 2 9644 7898



**FINLAND – Farnell InOne**  
Tel No: ++ 358 9 560 7780  
Fax No: ++ 358 9 345 5411



**NETHERLANDS – Farnell InOne**  
Tel No: ++ 31 30 241 7373  
Fax No: ++ 31 30 241 7333



**SWITZERLAND – Farnell InOne**  
Tel No: ++ 41 1 204 64 64  
Fax No: ++ 41 1 204 64 54



**AUSTRIA – Farnell InOne**  
Tel No: ++ 43 662 2180 680  
Fax No: ++ 43 662 2180 670



**FRANCE – Farnell InOne**  
Tel No: ++ 33 474 68 99 99  
Fax No: ++ 33 474 68 99 90



**NEW ZEALAND – Farnell InOne**  
Tel No: ++ 64 9 357 0646  
Fax No: ++ 64 9 357 0656



**UK – Farnell InOne**  
Tel No: ++ 44 8701 200 200  
Fax No: ++ 44 8701 200 201



**BELGIUM – Farnell InOne**  
Tel No: ++ 32 3 475 2810  
Fax No: ++ 32 3 227 3648



**GERMANY – Farnell InOne**  
Tel No: ++ 49 89 61 39 39 39  
Fax No: ++ 49 89 613 59 01



**NORWAY – Farnell InOne**  
Tel No: ++ 45 44 53 66 66  
Fax No: ++ 45 44 53 66 02



**UK – BuckHickman InOne**  
++ 44 8450 510 150  
++ 44 8450 510 130



**BRAZIL – Farnell-Newark InOne**  
Tel No: ++ 55 11 4066 9400  
Fax No: ++ 55 11 4066 9410



**HONG KONG – Farnell-Newark InOne**  
Tel No: ++ 852 2268 9888  
Fax No: ++ 852 2268 9899



**PORTUGAL – Farnell InOne**  
Tel No: ++ 34 93 475 8804  
Fax No: ++ 34 93 474 5288



**UK – CPC**  
++ 44 8701 202 530  
++ 44 8701 202 531



**CHINA – Farnell-Newark InOne**  
Tel No: ++86 10 6238 5152  
Fax No: ++86 10 6238 5022



**IRELAND – Farnell InOne**  
Tel No: ++ 353 1 830 9277  
Fax No: ++ 353 1 830 9016



**SINGAPORE – Farnell-Newark InOne**  
Tel No: ++ 65 6788 0200  
Fax No: ++ 65 6788 0300



**EXPORT – Farnell InOne**  
Tel No: ++ 44 8701 200 208  
Fax No: ++ 44 8701 200 209

For enquiries from all other markets



**DENMARK – Farnell InOne**  
Tel No: ++ 45 44 53 66 44  
Fax No: ++ 45 44 53 66 06



**ITALY – Farnell InOne**  
Tel No: ++ 39 02 93 995 200  
Fax No: ++ 39 02 93 995 300



**SPAIN – Farnell InOne**  
Tel No: ++ 34 93 475 8805  
Fax No: ++ 34 93 474 5107



**ESTONIA – Farnell InOne**  
Tel No: ++ 358 9 560 7780  
Fax No: ++ 358 9 345 5411



**MALAYSIA – Farnell-Newark InOne**  
Tel No: ++ 60 3 7873 8000  
Fax No: ++ 60 3 7873 7000



**SWEDEN – Farnell InOne**  
Tel No: ++ 46 8 730 50 00  
Fax No: ++ 46 8 83 52 62

<http://www.farnellinone.com>

<http://www.buckhickmaninone.com>

<http://www.cpc.co.uk>

**Disclaimer** This data sheet and its contents (the "Information") belong to the Premier Farnell Group (the "Group") or are licensed to it. No licence is granted for the use of it other than for information purposes in connection with the products to which it relates. No licence of any intellectual property rights is granted. The Information is subject to change without notice and replaces all data sheets previously supplied. The Information supplied is believed to be accurate but the Group assumes no responsibility for its accuracy or completeness, any error in or omission from it or for any use made of it. Users of this data sheet should check for themselves the Information and the suitability of the products for their purpose and not make any assumptions based on information included or omitted. Liability for loss or damage resulting from any reliance on the Information or use of it (including liability resulting from negligence or where the Group was aware of the possibility of such loss or damage arising) is excluded. This will not operate to limit or restrict the Group's liability for death or personal injury resulting from its negligence. Multicomp is the registered trademark of the Group. © Premier Farnell plc 2004.



## **Anexo 5**



## XPort Embedded Device Server

- ▶ Minimal engineering effort required to web-enable virtually any electronic device
- ▶ Remote command and control of edge devices
- ▶ Real-time edge device status via e-mail alerts
- ▶ 256-bit AES encryption for secure communications
- ▶ EMC/EMI-compliant; RoHS-compliant
- ▶ Everything you need – all in a single RJ45 package



## Build Network Connectivity into Your Products, Quickly and Simply

XPort® is a compact, integrated solution to web-enable any device with serial capability. By incorporating XPort to a product design, manufacturers can offer network connectivity as a standard feature within weeks — so they can be accessed and controlled over the Internet.

### Full Networking in a Tiny Package

XPort removes the complexity – of designing network connectivity into a product by incorporating all of the required hardware and software inside a single embedded solution. Smaller than your thumb, it includes all essential networking features, including a 10Base-T/100Base-TX Ethernet connection, proven operating system, an embedded web server, e-mail alerts, a full TCP/IP protocol stack, and 256-bit AES encryption for secure communications. This easy-to-embed networking processor module enables engineers to focus on their core competency while reducing development time and cost and increasing product value.

### Integrated Network Communications Module

XPort is powered by our DSTni™ network processor SoC, which includes a 10/100 MAC/PHY and 256 KB of SRAM. It features a built-in web server for communications with a device via a standard Internet browser. Web capability can be used for remote configuration, real-time monitoring or troubleshooting. XPort has 512 KB of on-module Flash for web pages and software upgrades. It acts as a dedicated co-processor that optimizes network activities permitting the host microprocessor to function at maximum efficiency.

### Building Intelligent Devices

With XPort you can embed intelligence into any electronic product for applications such as:

- Remote diagnostics and upgrades
- Asset tracking and replenishment
- Automation and control
- Power management
- Remote collaboration
- Personalized content delivery

### Robust, Feature-Rich Software Suite

Eliminating the need to negotiate the intricacies of Transmission Control Protocol (TCP) or Internet Protocol (IP), XPort incorporates:

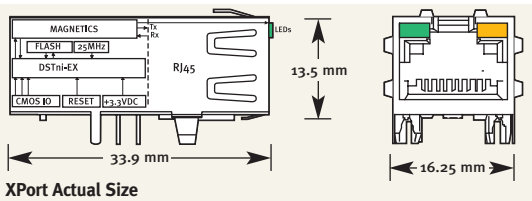
- Robust Real Time Operating System (RTOS)
- Full-featured network protocol stack
- Proven, ready-to-use serial-to-wireless application
- Built-in web server for device communication and configuration via a standard browser

The Windows-based DeviceInstaller™ makes configuring one or more XPorts in a subnet quick and easy.

- Install and configure XPort and load firmware
- Assign IP & other network specific addresses
- Set wireless parameters
- Load custom web pages and view specific device data
- Enable web-based configuration of the device
- Ping or query the attached device(s) over the network
- Allow Telnet communication with the device(s)



## XPort Hardware and Software



XPort Actual Size



### Features and Specifications

#### Serial Interface

- Interface: CMOS (Asynchronous, 5V tolerant)
- Data Rates: 300 bps to 921,600 bps
- Characters: 7 or 8 data bits
- Parity: odd, even, none
- Stop Bits: 1 or 2
- Control Signals: DTR/DCD, CTS, RTS
- Flow Control: XON/XOFF, RTS/CTS
- Programmable I/O: 3 PIO pins (software selectable)

#### Network Interface

- Interface: Ethernet 10Base-T or 100Base-TX (Auto-Sensing)
- Connector: RJ45
- Protocols: TCP/IP, UDP/IP, ARP, ICMP, SNMP, TFTP, Telnet, DHCP, BOOTP, HTTP and AutoIP

#### Indicators (LED)

- 10Base-T connection
- 100Base-TX connection
- Link & activity indicator - Full/half duplex

#### Management

- SNMP, Telnet, serial, internal Web server, and Microsoft Windows<sup>®</sup>-based utility for configuration

#### Security

- Password protection
- Optional 256-bit AES Rijndael encryption

#### Internal Web Server

- Storage capacity: 384 KB for web pages

#### Architecture

- CPU: Based on the DSTni-EX enhanced 16-bit, 48MHz or 88MHz x86 architecture
- Memory: 256 KB SRAM and 512 KB Flash
- Firmware: upgradeable via TFTP and serially

#### Power

- Input voltage: 3.3 VDC

#### Environmental

- Extended Temp: -40° to 85°C (-40° to 185°F)
- Commercial Temp: 0° to 70°C (32° to 158°F)
- Storage: -40° to 85°C (-40° to 185°F)

#### Packaging

- Dimensions: 33.9 x 16.25 x 13.5 mm (1.33 x .64 x .53 in)
- Weight: 9.6 g (0.34 oz)

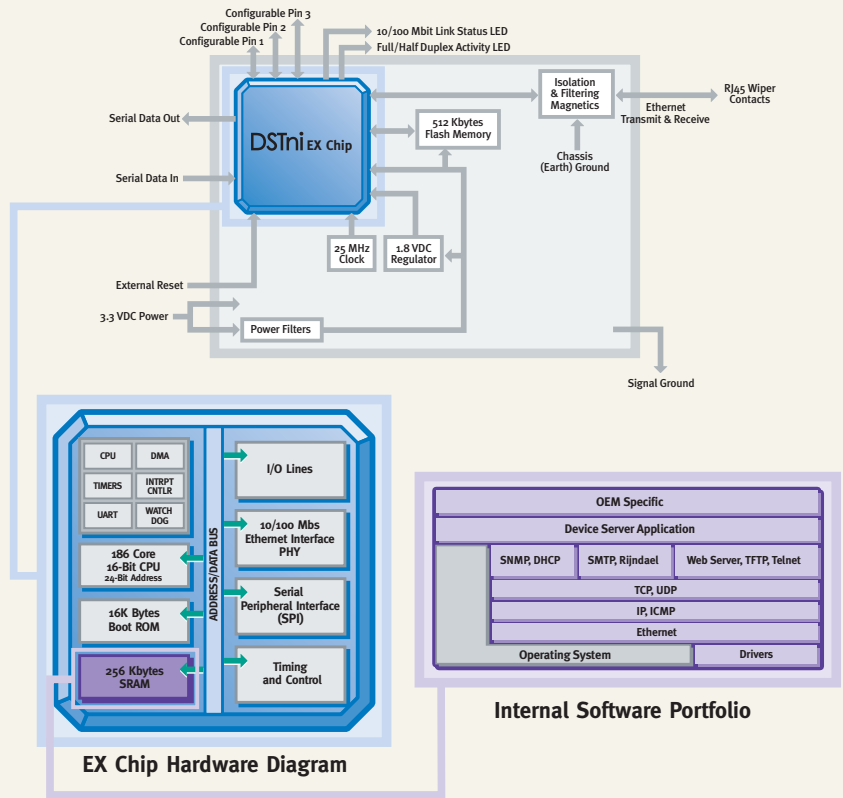
#### Warranty

- 2-year limited warranty

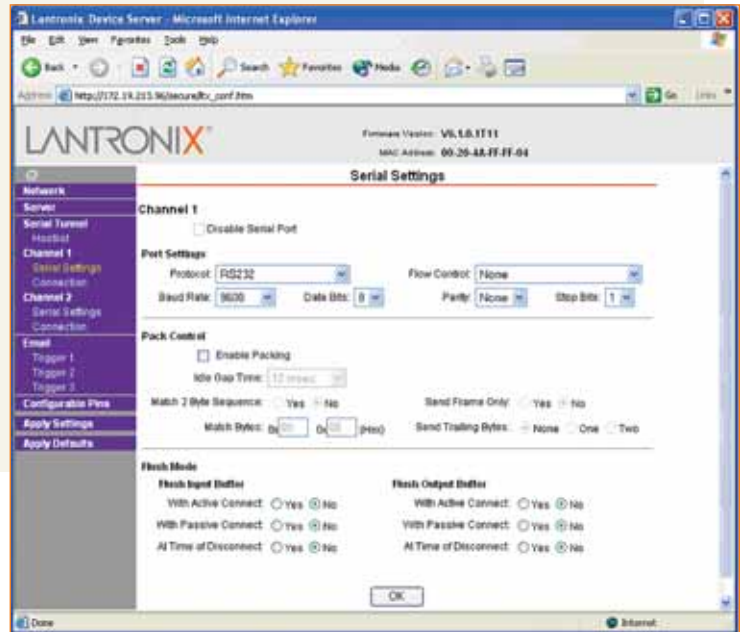
#### Included Software

- MS Windows-based DeviceInstaller software and MS Windows-based Com Port Redirector

Model	Part Number	Description
XPort XE	XP1001000-03R	XPort RoHS Extended Temperature
Min. Quantity: 50 Units	XP1001001-03R	XPort RoHS Commercial Temperature
	XP1001000M-03R	XPort XE RoHS Extended Temperature, with MODBUS
XPort SE	XP1002000-03R	XPort RoHS Extended Temperature, with Encryption
Min. Quantity: 50 Units	XP1002001-03R	XPort RoHS Commercial Temperature, with Encryption
XPort SE SMPL	XP1002005-03R	XPort RoHS Extended Temperature, with Encryption - Sample
XPort 485	XP1004000-03R	XPort RS-485 RoHS Extended Temperature, with Encryption
XPort 485 SMPL	XP1004005-03R	XPort RS-485 RoHS Extended Temperature, with Encryption - Sample
XPort Evaluation Kit	XP100200K-03	XPort Evaluation Kit, with Encryption



The included DeviceInstaller software makes configuring XPort quick and easy!



### XPort Evaluation Kit

The XPort Evaluation Kit includes everything you need to integrate the XPort into your next product design, including:

- An XPort Evaluation Board and reference design including CAD PCB files and complete BOM
- Universal AC power adapter
- Network (CAT5) and serial cable
- Connector adapter
- Data sheet
- Lantronix utilities CD containing new Com Port Redirector, DeviceInstaller
- Sample code and application notes
- Complete user manual



## **Anexo 6**



## Embedded Device Server - MatchPort AR

- ▶ Application-ready, secure SSL/SSH networking module for high-volume applications
- ▶ Low cost, high-performance, 32-bit, 166Mhz 159 MIPS platform
- ▶ Built-in CGI and AJAX web server
- ▶ Pin compatible family includes 802.11 b/g wireless
- ▶ Ethernet MAC/PHY; add only RJ45 jack and magnetics to device's PCB
- ▶ SNMP V2c ready, MIB II support
- ▶ "Cisco-like" CLI, XML, serial and Telnet management capability

## Secure, Powerful, Application-Ready Networking with Advanced Web Server Capability

MatchPort™ Architect (AR) delivers SSL/SSH ready Ethernet networking capability to virtually any product with a serial interface on the host microcontroller. This flexible product provides affordable connectivity in the same compact, single-socket form factor as its wireless cousin, the MatchPort b/g. With MatchPort, OEMs can design wired Ethernet or WiFi networking into their products using a single PCB design.

MatchPort AR is a powerful networking co-processor module. Without burdening the device's main processor, it sends and receives serial data in packets over Ethernet. It incorporates state-of-the-art CGI and AJAX web server capabilities for remote data acquisition, device monitoring and configuration, and virtually no programming is required.

With a simple connection between the device microcontroller's serial port and one of MatchPort AR's two serial ports, it enables OEMs to create feature-rich applications for medical, security, retail/POS, industrial/building automation, metering, gaming and more.

### Pin-Compatible Wired Module Family

The MatchPort family lets you "future proof" your designs with a choice of flexible, media-independent 802.11 b/g or Ethernet networking modules. It takes the complexity out of RF design and embedded Ethernet networking so you can focus on designing your products. And it minimizes engineering risk, reduces cost and shortens development time.

### Bullet-Proof Security

The MatchPort award-winning operating system, Evolution OS™, offers a variety of robust data encryption and authentication options, including secure SSH v2.0, SSL v3.0 protocol

support with a choice of AES or 3DES encryption coupled with SHA-1 or MD5 authentication. *Evolution OS supports both public and private key infrastructures and provides the flexibility to use any key size up to 1024-bit.*

Evolution OS is designed to survive hostile Internet attacks such as denial of service (DoS) and port mapping. It also ensures that MatchPort cannot be used to bring down other devices on the network.

### Advanced Web Server Technologies

MatchPort's advanced, integrated CGI-capable web server transforms a standalone device into a fully functioning networked product that can be configured and managed remotely via a standard web browser. Users can remotely monitor and collect information from the device in real-time using the CGI (Common Gateway Interface)-capable server and send the information to dynamic web pages. MatchPort AR incorporates AJAX technology to ensure smooth browsing of dynamic content served from the edge device. Additionally, it supports open standards such as "Cisco-like" CLI, XML and serial and Telnet management options.

XML and RSS support provide a useful way to transfer information for machine-to-machine communication. An RSS aggregator can collect readings from various machines and push them to a supervisory program for monitoring and control. In a security system, XML data sent to an application can provide enough information to decide whether to call the police or fire department. Similarly, facilities managers could use an aggregator to collect RSS feeds from remote locations to check for open or closed doors, for example.

### Processing Power and Flexibility

MatchPort AR effortlessly handles the most computationally demanding applications with a 32-bit, 159 MIPS (Dhrystone 2.1) 166 MHz processor. With 8 MB SDRAM and 4 MB Flash, it provides enough memory capacity for OEM customization, loading web pages and data 'store-and-forward' applications. Seven control pins (CP/GPIO) are available to enable customizable, pre-programmed responses such as email notifications, SNMP traps or I/O control of peripherals.

LANTRONIX®  
EVOLUTION OS™





## Features and Specifications

### Serial Interface

CMOS 3.3V signals. Speed software selectable and customizable from 300bps to 230,400bps  
 Serial Line Formats: 7 or 8 data bits, 1-2 Stop bits  
 Parity: odd, even, none  
 Modem Control: DTR,DCD  
 Flow Control: XON/XOFF (software), CTS/RTS (hardware), none

### Network Protocols

Protocols Supported: ARP,UDP,TCP,Telnet, ICMP,SNMP, DHCP,BOOTP, Auto IP,HTTP,SMTP,FTP, HTTPS, SSH, SSI, FTP, PPP

### Network Interface

Ethernet 10/100 base TX with Auto Negotiation, and HP Auto MDIX

### Management (of MatchPort AR)

Internal WebManager (SSL Option for secure login)  
 Cisco-like CLI (over Serial Ports, Telnet or SSH)  
 XML Configuration Records via CLI or FTP  
 DeviceInstaller software  
 Firmware: Upgradeable via TFTP, FTP, Web, Serial Port  
 Flash wear leveling and erase cycle statistics

### Security

SSL Client & Server, Selectable 128/256/512/1024 Bit Certificates  
 SSH Client, 8 Server Selectable 128/256/512/1024 Bit Public/Private Key support  
 ENCRYPTION: AES, 3DES and RC4 Encryption for SSH & SSL  
 Lantronix end-to-end AES 128 Bit Encryption  
 AUTHENTICATION: SHA-1, MD5, Base-64  
 User Access Lists  
 Security hardened OS and Protocol Stacks

### Internal Web Server

CGI with AJAX support  
 Storage capacity: 1 MB with factory default firmware loaded

### Architecture

Lantronix DSTni-FX 32-bit processor, 166Mhz (159 MIPS - Dhystone 2.1),  
 7 GPIO  
 Memory: 8 MB SDRAM, 4 MB Flash (Factory default).  
 Contact Lantronix for larger memory configuration.

### Power Consumption

Average Power Consumption:0.67W (210mA) at 3.3V.

### Environmental

Operating Temperature range -40° to 70°C (-40° to 158°F)  
 Storage range: -40°C to +85°C (-40°F to 185°F)

### Packaging

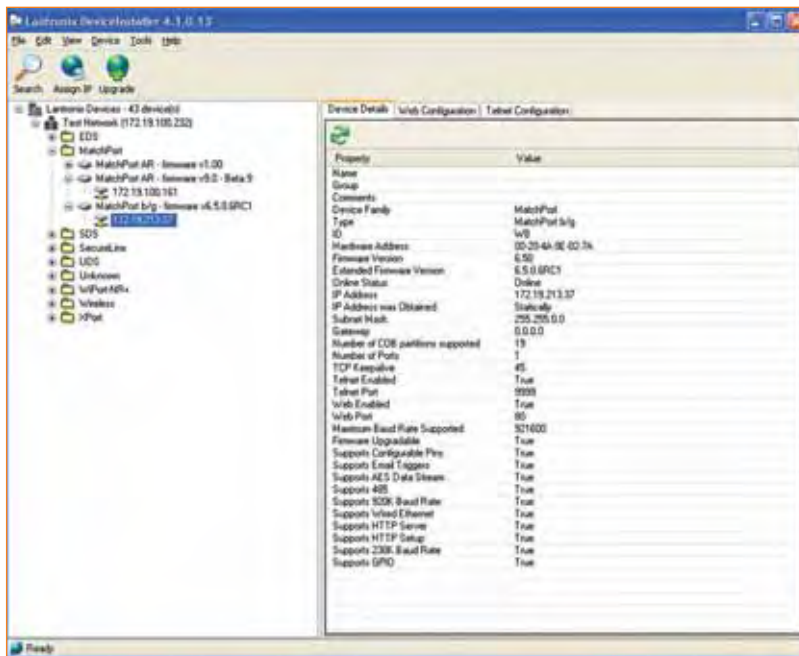
Dimensions: 44.4 x 44.4 x 10.4 mm (1.75 x 1.75 x .41 in)  
 Weight: 29g  
 Material: Plastic shell, 260°C tolerant

### Warranty

2-year limited warranty

### Included Software

Windows® 98/NT/2000/XP/Vista based  
 DeviceInstaller configuration software and  
 Com Port Redirector, Web-Manager



The included DeviceInstaller software makes configuration quick and easy!

## MatchPort AR Demonstration Kit

The demonstration kit contains the key accessories to evaluate a MatchPort AR product:

- MatchPort demonstration board
- RS-232 cable, DB9F, null modem
- Cat5e UTP RJ45M/M Ethernet cable
- 3.3V power supply
- Antenna

**Note: MatchPort sample must be purchased separately.**

## Ordering Information

### Part Number

MPR3002000-01

### Description

- MatchPort AR AES bulk pack
  - Minimum order quantity 50 units
- 
- MPR300200S-01
- MatchPort AR sample case
  - One MatchPort AR enclosed
  - Free 30-day Secure Com Port Redirector™ evaluation license
  - Order quantities of up to 10
- 
- MP10010NMK-01
- MatchPort AR Demonstration Kit

# LANTRONIX®

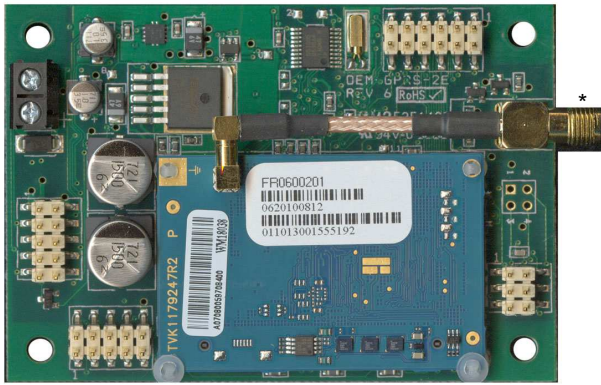
15353 Barranca Parkway | Irvine | CA 92618 | USA | Tel: 949.453.3990 | Fax: 949.453.3995 | [www.lantronix.com](http://www.lantronix.com)

©2007 Lantronix, Inc. Lantronix is a registered trademark, and MatchPort, Evolution OS, DeviceLinX and DeviceInstaller are trademarks of Lantronix, Inc. All other trademarks are the property of their respective owners. Specifications subject to change without notice. All rights reserved. 910-522 09/07 DGS2500

## **Anexo 7**

# OEM-GPRS2E

## Intelligent GSM/GPRS monitoring solution



\*CABLE-004 - SMA female connector cable (optional extra)



### Applications

**Battery Powered Applications**  
**Security Systems**  
**Remote Utility Metering**  
**Vending Machines**  
**Remote Data Collection**  
**Mobile Communications**  
**Environmental Control**  
**Automated Signs**

In general – any equipment that requires remote monitoring and communication over GPRS or GSM networks.

OEM-GPRS2E enable's legacy equipment with simple I/O or serial protocols to communicate over GSM and GPRS networks. Ideal for standalone applications where there is no external microcontroller.

Part Number	Variant
FR06000200	OEM-GPRS2E TTL
FR06000201	OEM-GPRS2E RS232

OEM-GPRS2E enables host equipment to communicate over the GSM and GPRS networks. It includes an on-board TCP/IP stack with listening and client sockets enabling legacy protocols to be transported via IP networks such as GPRS and the Internet. Two variants are available, which allow connection to TTL or RS232 compatible equipment interfaces. The OEM-GPRS2E supports extended AT-Commands for establishing and controlling connections. Where the host equipment is unable to control the connection, it supports auto-dial and auto-answer features.

OEM-GPRS2E is able to remain in low power sleep mode until a wakeup event occurs. Once awake, the module can perform a number of automated operations before re-entering low power sleep and standby modes. This includes start / monitor timer sequences, SMS and data autodial features. It can wake from an on-board real-time clock (RTC) and host signals (data, DTR).

Integration has been made simple by maintaining Comtech's standard module footprint and connectors.

### Benefits

- Automatic monitoring and reporting of simple I/O without requiring communication knowledge.
- Fast time to market with minimal risk

### Features

- **GSM/GPRS Modem**
  - GSM (CSD, SMS, voice)
  - GPRS (Class B 4+2 Class 10)
  - GPRS 57.6 Kbps (down), 28.8 Kbps (up)
  - Quad Band (900/1800 Mhz, 850/1900Mhz)
  - Integrated TCP/IP stack, listening and client sockets
  - ROHS Compliant
  - On-board SIM Holder
  - Extended AT Command
  - Sleep and Standby modes
  - Programmable event timers
  - Real-time-Clock with external battery support
  - Wake events (Data, RTC, DTR)
  - Automated operation (Autodial, SMS, timers)
  - FR06000200 TTL interface - 5-9V power supply
  - FR06000200 RS232 interface - 5-15v power supply
  - MMCX RF connector, with SMA option (CABLE-004)
  - Audio and LED connector
  - -20°C to 70°C operating temperature
  - Small mechanical size approx 59x89mm
- **Automated modes for standalone operation**
  - No external microcontroller required
  - Configurable power down & wake event modes
  - Programmable event timers and Real time clock
  - Autoanswer & autodial
  - Autosend SMS or dial upon alarm/event for reporting status or establishing calls

**COMTECH M2M**  
inspiring innovation

machine 2 machine connectivity

Copyright © 2007 Comtech M2M Ltd. All brand or product names are trademarks or registered trademarks of Comtech M2M Ltd. The specifications and information herein are subject to change without notice. For the latest data revision visit our website detailed below.

Revision	4	Issue Date	14/11/07	Filename	OEMGPRS2E	Page Number	1
----------	---	------------	----------	----------	-----------	-------------	---

Web: [www.comtechm2m.com](http://www.comtechm2m.com) Email: [sales@comtechm2m.com](mailto:sales@comtechm2m.com) Tel: +44 (0) 1204 664333 Fax: +44(0) 1204 664334

Comtech M2M Ltd, Comtech House, Paragon Business Park, Horwich, Bolton, Lancashire, BL6 6HG, UK



## **Anexo 8**

```

'
'*****
*
' ** Ciclo Principal do Firmware
**
'*****
*
      Do

          If Teclado_ligado_temp = 1 Then

              Call Keyboard

              Config Pinf.0 = Input           'Teclado
              Config Pinf.1 = Input           'Teclado
              Config Pinf.2 = Input           'Teclado
              Config Pinf.3 = Input           'Teclado
              Config Pinf.4 = Input           'Teclado
              Config Pinf.5 = Input           'Teclado
              Config Pinf.6 = Input           'Teclado
              Config Pinf.7 = Input           'Teclado

          End If

          If _hour = 1 And Flag_timerequest = 0 And Configuracao = "0"
Then
              Flag_timerequest = 1
              Bufferteste = ""
              Bufferteste = Startcode + "TR" + Chr(13) + Chr(10)
              Vartemp = Crc8(bufferteste , 6)
              Print #1 , Bufferteste ; Chr(vartemp) ; Chr(4); 'enviar
time-request
          End If
          '
          If _hour > 1 And Flag_timerequest = 1 And Configuracao = "0"
Then
              Flag_timerequest = 0           'caso
tenha sido enviado time-request às 3h, volta flag a 0
              Start Timer1
              Start Watchdog
              Locate 2 , 1
              Lcd Msg_reiniciar
              Idle
          End If

          If Flag_mudanome = 1 Then
              Flag_mudanome = 0
              Empresa = Empresa_temp
          End If
          '
          If Sensor = 1 And Biofree_temp = 1 And Configuracao = "0" And
Bio_presente = 1 And Buzz_valido = 0 And Mem_online = 0 Then
'caso esteja um dedo no biométrico. Falta juntar rotinas de gravação
              Locate 2 , 1
              Lcd Msg_identificar
              Sound Buzz , 1000 , 200
              Waitok = 1
              Do
                  Byteuart = Inkey(#2)
                  Buffer_ok = Ischarwaiting(#2)
              Loop Until Buffer_ok = 0

```

```

        Call Bio_identify
    End If

    If Prox_time = 0 And Configuracao = "0" And Bioprox_temp = 1
    And Prox = Chr(1) And Mem_online = 0 Then
        Call Bio_reset

        Call Swuart_read                                'rotina de
comunicação com prox
        Call Swuart
        Prox_time = 30 * 1
    End If

    If Rw_en = 1 Then                                    'foi lido
um cartão com sucesso
        Sound Buzz , 400 , 700
        Rw_en = 0
        If Biometrico_activo_temp = 1 And Bio_presente = 1 Then
'Só pede dedo se a biometria estiver activa
            Flag_bio_match = 0
            If Array_prox(8) = "0" Then
                Locate Ybio_pordedo , Xbio_pordedo
                Lcd Bio_pordedo
                Call Bio_matchfeature
            Elseif Array_prox(8) = "1" Then
                Flag_bio_match = 1
            End If
            Elseif Biometrico_activo_temp = 0 Or Bio_presente = 0 Then
                Flag_bio_match = 1
            End If

            If Flag_bio_match = 1 Then                    'foi
encontrado um match finger, envia o cmd online
                'Bufferout = ""
                Bufferout = Startcode
                Bufferout = Bufferout + "OL"
                Bufferout = Bufferout + Tipo_picagem_temp
                Bufferout = Bufferout + Terminal_type_temp
                'Testestr = Chr(array_prox(6))            'envia
serie
                'Bufferout = Bufferout + Testestr
                'Testestr = Chr(array_prox(7))            'envia
serie
                'Bufferout = Bufferout + Testestr
                '
                Call Escreve_tempo
                Bufferout = Bufferout + Movimento_hora +
Movimento_minuto + Movimento_segundo + Movimento_dia + Movimento_mes +
Movimento_ano

                Testestr = Chr(array_prox(1))            'envia num
                Bufferout = Bufferout + Testestr
                Testestr = Chr(array_prox(2))            'envia num
                Bufferout = Bufferout + Testestr
                Testestr = Chr(array_prox(3))            'envia num
                Bufferout = Bufferout + Testestr
                Testestr = Chr(array_prox(4))            'envia num
                Bufferout = Bufferout + Testestr
                Testestr = Chr(array_prox(5))            'envia num
                Bufferout = Bufferout + Testestr

```

```

Bufferout = Bufferout + Chr(13) + Chr(10)
Check = Crc8(bufferout , 27)

Serie = Chr(array_prox(6)) + Chr(array_prox(7))

If Serie = Card_serie_temp Then

    For A = 1 To 5
        Array_temp2(a) = Array_prox(a)
        Array_temp(a) = Chr(array_temp2(a))
        Array_id(a) = Array_prox(a)
    Next A
    Array_id(6) = Tipo_picagem_temp

    If Flag_alarme_on = 1 Then
        Locate 2 , 1
        Lcd " ALARME ACTIVO  "
        Msgtime = 30 * 5
        Buzz_valido = 2
        Goto Continua_main
    End If

    Call Time_diff_sub

    If Timediff_ok = 1 Then

        Print #1 , Bufferout ; Chr(check) ; Chr(4);
        Flag_bio_match = 0
        Time_offline_var = 45 * Time_offline
        Waitok = 1
        Locate Ymsg_avalidar , Xmsg_avalidar
        Lcd Msg_avalidar

        Reset Ledval

        Esperasw = 0
        Do
            Waitms 1
            Incr Esperasw
        Loop Until Ischarwaiting(#1) = 1 Or

Esperasw = 200

        Call Cip
        If Okreceived = 0 Then
            Call Valida_offline
            If Valido_offline = 1 Then
                Mem_online = 1
                Memtime = 30 * 3
                Waitok = 0
            Else
                Buzz_valido = 2
                Locate 2 , 1
                Lcd Ko_defaultmsg
                Call Time_diff_sub_del
            End If
        Elseif Okreceived = 1 Then
            Locate 2 , 1
            Lcd " "
            Locate 2 , 1

```

```

                                Lcd Msg_validoid ; Chr(array_prox(1))
; Chr(array_prox(2)) ; Chr(array_prox(3)) ; Chr(array_prox(4)) ;
Chr(array_prox(5)) ;

                                Msgtime = 30 * Time_ok_defaultmsg
                                Reletime = 30 * Time_rele 'Faz abrir
a porta

                                Flag_releon = 1
                                Elseif Okreceived = 2 Then
                                    Locate 2 , 1
                                    Lcd Ko_defaultmsg
                                    Msgtime = 30 * Time_ok_defaultmsg
                                    Call Time_diff_sub_del
                                End If
                                Okreceived = 0
                                Waitok = 0
                                Elseif Timediff_ok = 0 Then

                                    Sound Buzz , 400 , 700
                                    Locate 2 , 1
                                    Lcd "PICAGEM REPETIDA"
                                    Msgtime = 30 * 2

                                End If
                                Else
                                    Buzz_valido = 2
                                    Locate 2 , 1
                                    Lcd Msg_serieinvalida
                                    Msgtime = 30 * 2
                                    Bufferokko = "" 'envia SS
para PC
                                    Bufferokko = Startcode + "NG" + Tipo_picagem_temp +
Terminal_type_temp + "00000" + Chr(13) + Chr(10)
                                    Varcrc8 = Crc8(bufferokko , 15)
                                    Print #1 , Bufferokko ; Chr(varcrc8) ; Chr(4);
                                End If
                                End If
                                Flag_bio_match = 0

                                End If
,
Continua_main:
    Call Verifica_hora_toques
    Call Verifica_toques
    Call Data_hora 'Atualiza
data/hora no display

    If Ischarwaiting(#1) = 1 Then
        Call Cip
    End If

    #if Dog
        Reset Watchdog
    #endif

    If Flag_toque = 0 Then
        Call Verifica_inputs 'Verifica
estado dos inputs e toma as decisões
        Call Verifica_outputs 'Verifica
estado e decide
    End If

```

```

        If Buzz_valido = 1 Then
            Buzz_valido = 0
            For A = 1000 To 100 Step -100
                Sound Buzz , 300 , A
            Next A
            Waitok = 0
            Wait 1
        Elseif Buzz_valido = 2 Then
            Buzz_valido = 0
            Set Ledinv
            For A = 100 To 1500 Step 200
                Sound Buzz , 300 , A
            Next A
            Waitok = 0
            Reset Ledinv
        End If

        If Memtime = 0 And Mem_online = 1 Then
            If Okreceived = 0 Then
                Call Write_log
            End If

            Okreceived = 0
            Mem_online = 0
        End If

    Loop

```

## **Anexo 9**

## PROTOCOLO DE COMUNICAÇÃO SIBZONE 2008

---

**Data:** 11 de Fevereiro de 2008

### Departamento de Investigação e Desenvolvimento

Equipa de Hardware

Tiago Ferreira

Fevereiro de 2008

**Lisboa**

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

**Porto (Unidade de produção)**

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)



## Índice

DEFINIÇÕES BÁSICAS.....	4
<i>Introdução</i> .....	4
<i>Particularidades</i> .....	4
<i>Definições Padrão</i> .....	5
CONFIGURAÇÕES.....	6
<i>Modo de Configurações</i> .....	6
<i>Configuração de Entrada/Saída/Indiferenciado</i> .....	6
<i>Configuração de Data/Hora</i> .....	6
<i>Configuração de Nome do Terminal</i> .....	7
<i>Configuração de INPUTS</i> .....	7
<i>Configuração de OUTPUTS</i> .....	7
<i>Configuração de Tipo de Modo Offline</i> .....	8
<i>Configuração da Série dos Cartões do Terminal</i> .....	8
<i>Configuração do Modo de Autenticação</i> .....	8
<i>Configuração do Tempo e Saída de Toque</i> .....	9
<i>Configuração do horário de toques</i> .....	9
<i>Configuração do Número de Impressões Digitais por Utilizador</i> .....	9
<i>Configuração do ID do Terminal</i> .....	10
<i>Activação de Teclado</i> .....	10
<i>Configuração do TimeDif (tempo mínimo entre picagens para o mesmo ID)</i> .....	10
<i>Activação do modo Dual Function</i> .....	11
<i>Configuração do Tipo de Picagem</i> .....	11
<i>Pedido de Configurações do Terminal</i> .....	12
INTERACÇÃO .....	13
<i>Movimento Online</i> .....	13
<i>Envio de Mensagem para o Display</i> .....	13
<i>Gravar ID com uma Impressão Digital Codificada</i> .....	14
<i>Abertura Remota de Porta</i> .....	14
<i>Bloquear porta</i> .....	14
<i>Desbloquear porta</i> .....	15
<i>Time-Request (todas as 03h##m, pede o acerto de horário)</i> .....	15
<i>Apagar todas as Impressões Digitais do Terminal</i> .....	15
<i>Apagar uma Impressão Digital</i> .....	16
<i>Pedido de envio de uma Impressão Digital Codificada já gravada</i> .....	16
<i>Registar uma impressão digital com envio da mesma (2 pacotes)</i> .....	17
<i>Receber Número de Templates de um ID</i> .....	17
<i>Reset do Terminal</i> .....	17
<i>Diagnóstico de ligação "KEEP-ALIVE"</i> .....	18
<i>Versão do terminal</i> .....	18

### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
 Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
 Tlm. (+351) 96 173 06 52

### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
 ■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
 Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

<i>Pedido de Nº de biometrias de um ID.....</i>	18
<i>Registo de biometrias no Cartão .....</i>	19

**BASE DE DADOS ..... Erro! Marcador não definido.**

<i>Número de Movimentos na Base de Dados .....</i>	<b>Erro! Marcador não definido.</b>
<i>Download dos Movimentos guardados na Memória do Terminal .....</i>	<b>Erro! Marcador não definido.</b>
<i>Registar Utilizador na Base de Dados.....</i>	<b>Erro! Marcador não definido.</b>
<i>Apagar Movimentos da Base de Dados .....</i>	<b>Erro! Marcador não definido.</b>
<i>Apagar Base de Dados.....</i>	<b>Erro! Marcador não definido.</b>
<i>Número de Utilizadores na Base de Dados.....</i>	<b>Erro! Marcador não definido.</b>
<i>Enviar Plano de Acesso para a Base de Dados.....</i>	<b>Erro! Marcador não definido.</b>

## DEFINIÇÕES BÁSICAS

### Introdução

Este documento destina-se ao desenvolvimento de soluções de software para o equipamento *SIBzone*<sup>®</sup> 2007, com leitor biométrico da *Suprema – SFM3000 series* e com a versão 3.4 do firmware.

O documento encontra-se dividido por instruções, estando estas agrupadas nas seguintes categorias:

- CONFIGURAÇÕES
- INTERACÇÃO
- BASE DE DADOS

Cada instrução é descrita com toda a informação necessária para ser utilizada, incluindo um exemplo.

O Protocolo de comunicação deverá ser implementado através de uma string de caracteres enviada num pacote TCP/IP para o terminal. A resposta será feita da mesma forma.

**NOTA:** CR -> Carácter 13 ou HEX= 0D    LF -> carácter 10 ou HEX=0A    CRC8 -> XOR lógico de toda a *string* de dados

### Particularidades

Às 03:## é enviado um comando “Time-Request”. Este serve para, se a aplicação estiver preparada, acertar as horas do terminal.

Caso o “Time-Request” tiver sido executado pelo terminal (não é necessário que tenha tido resposta), o terminal fará um *RESET* automático às 05h00.

As Séries Pré-definidas para o envio de picagens são:

- SI – Série Inválida (Tentativa de autenticação com impressão digital inválida)
- SB – Série Biométrica (Autenticação com impressão digital válida)
- KB – Série Teclado (Autenticação via Teclado)

## Definições Padrão

Tipo de Terminal	I – Indiferenciado
Data/Hora	00:00 ##/##/2007
Nome do Terminal	SIBZONE 2007
Inputs	Todas Desabilitadas
Outputs	Todas Normalmente Abertas
Modo Offline	Não autenticar Offline
Série dos Cartões	AA
Modo de Autenticação	Prox
Número de Biometrias por ID	1 Biometrias/ID
Activação do Teclado	Desactivado
Modo <i>TimeDif</i>	Desactivado
Modo <i>Dual Function</i>	Desactivado
Tipo de Picagem	Indiferenciado
Tempo de Abertura do Relé	1 segundo

### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)

## CONFIGURAÇÕES

### Modo de Configurações

PC -> Terminal      ##CFx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Modo de Configurações  
0 – Desligado  
1 – Ligado

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

nota: Quando em modo de configurações, não é possível fazer autenticações no terminal

Exemplo: ##CF1+CR+LF+CRC8

Activa o modo de configurações do terminal

---

### Configuração de Entrada/Saída/Indiferenciado

PC -> Terminal      ##ESx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Tipo de Movimento  
E – Entrada  
S – Saída  
I - Indiferenciado

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##ESE+CR+LF+CRC8

Configuração do terminal para o tipo Entrada

---

### Configuração de Data/Hora

PC -> Terminal      ##CSssmmhhyDDMMAAAA+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

ss – Segundos  
mm – Minutos  
hh – Horas  
y – Dia da semana  
1-Domingo; 2-Segunda...  
DD – Dia  
MM – Mês  
AAAA - Ano

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##CS001516205042007+CR+LF+CRC8

Hora/Data:      16:15 05/04/2007

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

### Configuração de Nome do Terminal

PC -> Terminal      ##NExxxxxxxxxxxx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

xxxxxxxxxx – Nome do terminal  
(12 caracteres)

yy – Confirmação de Recepção  
OK – Confirmado  
KO – Falhado

Exemplo: ##NENOMETERMINAL+CR+LF+CRC8

“NOMETERMINAL”

### Configuração de INPUTS

PC -> Terminal      ##CIxz+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Identificação da entrada  
(0,1,2 ou 3)

z – Modo:

- 0 – Desabilitado
- 1 – Abertura Manual
- 2 – Alarme Low
- 3 – Alarme High
- 4 – Fire Low
- 5 – Fire High
- 6 – Sensor de Porta Aberta

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##CI01+CR+LF+CRC8

Abertura Manual na entrada 0

### Configuração de OUTPUTS

PC -> Terminal      ##COxz+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Identificação da saída  
(0,1,2 ou 3)

z – Modo:

- 0 – Normalmente Aberto
- 1 – Normalmente Fechado

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##CO21+CR+LF+CRC8

Saída 2 em modo NORMALMENTE FECHADO

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

### Configuração de Tipo de Modo Offline

PC -> Terminal      ##MOx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Modo *Offline*

0 – Não autentica Offline (aceita todos os utilizadores)

1 – Autentica Offline (Apenas deixa passar os utilizadores com plano válido no momento de autenticação)

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##MO1+CR+LF+CRC8

Modo de autenticação Offline activa

### Configuração da Série dos Cartões do Terminal

PC -> Terminal      ##SRxx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

xx – Série dos cartões aceites no terminal (valor alfanumérico)

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##SRBE+CR+LF+CRC8

Série de cartões BE

### Configuração do Modo de Autenticação

PC -> Terminal      ##MBx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Modo de Biometria

0 – Prox (Só cartão)

1 – BioProx (Cartão e Biometria)

2 – Todos

3 – Só Biofree (Só Biometria)

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##MB1+CR+LF+CRC8

Modo BioProx (Cartão e biometria)

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

### Configuração do Tempo e Saída de Toque

PC -> Terminal      ##BZxz+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Tempo de toque (1 a 9 segundos)  
z – Saída onde irão actuar os toques (0 a 3).  
Caso se envie 4, desactiva todos os toques.

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##BZ72+CR+LF+CRC8      Toques com duração de 7 segundos na saída 2

### Configuração do horário de toques

PC -> Terminal      ##TQxxhh:mm+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

xx – Número do toque (de 0 a 15)  
hh – Hora do toque  
mm – Minuto do toque  
(Caso se envie a hora 25, o toque fica desactivado)

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##TQ1216:30+CR+LF+CRC8 Toque número 12 às 16:30

### Configuração do Número de Impressões Digitais por Utilizador

PC -> Terminal      ##NIx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Número de Impressões  
Digitais/Utilizador (1 ou 2), ficando os  
ID's entre 0 e 99999

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##NI2+CR+LF+CRC8      Número de Impressões Digitais definido para 2



### Configuração do ID do Terminal

PC -> Terminal      ##IDxx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

xx – ID do terminal  
(2 algarismos)

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##ID05+CR+LF+CRC8

As picagens Biofree passam a ser 05xxx

### Activação de Teclado

PC -> Terminal      ##KBx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Activar/Desactivar Teclado  
0 – Desligado  
1 – Ligado

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##CF1+CR+LF+CRC8

Activa o teclado

### Configuração do TimeDif (tempo mínimo entre picagens para o mesmo ID)

PC -> Terminal      ##TDx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – ID do terminal  
0 – desactivado  
2 a 9 – tempo em minutos

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Nota: 1 é assumido como 2 minutos

Exemplo: ##TD3+CR+LF+CRC8

Define um tempo mínimo de 3 minutos

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

### Activação do modo Dual Function

PC -> Terminal      ##DFx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – valor

0 – desactivado

1 – activado

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Nota: implementa as funções de ponto e acesso no mesmo terminal, sendo que a ordem das biometrias gravadas corresponde a uma ordem predefinida das funções (1 – ponto; 2 – acesso; 3 - emergência)

Exemplo: ##DF1+CR+LF+CRC8

Activa o modo *Dual Function*

### Configuração do Tipo de Picagem

PC -> Terminal      ##TPx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

x – Tipo de Picagem

P – Ponto

A – Acesso

I – Indiferenciado

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##TPA+CR+LF+CRC8

Configuração do tipo de picagem para Acesso

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

### Pedido de Configurações do Terminal

PC -> Terminal      ##RC+CR+LF+CRC8

Terminal -> PC      ##yy1[pacote]+CR+LF+CRC8

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Descrição do Pacote	
Campo	Bytes
Tipo Terminal	1
Inputs	4
Outputs	4
Modo Offline	1
Série Cartão	2
Modo de Autenticação	1
Tempo de Relé	1
Nº Biometrias por ID	1
<i>TimeDif</i>	1
Keyboard	1
Modo <i>Dual Function</i>	1
Tipo de Picagem	1

Exemplo: ##RC+CR+LF+CRC8

Pedido de envio de pacote com as configurações correntes do terminal

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)

## INTERACÇÃO

### Movimento Online

Terminal -> PC            ??????????????????????????????  
 PC -> Terminal         ??????????????????????????????

xxxxx – Número de utilizador  
 ss – Série do cartão  
 (caso seja apenas biometria, a série será SB  
 “Série Bio”, e em caso de tentativa inválida, SI  
 “Série Inválida”)  
 z – Tipo de Acesso  
 E – Entrada  
 S – Saída  
 P – Indiferenciado  
 t – Tipo de Picagem  
     P – Ponto  
     A – Acesso  
     I – Indiferenciado

?? – Confirmação de Recepção  
 ?? – Confirmado  
 ??- Falhado

Exemplo: ??????????????????????      Cartão 145 série BT, Terminal de Entrada

### Envio de Mensagem para o Display

PC -> Terminal         ##MSxxxxxxxxxxxxxxxx+CR+LF+CRC8  
 Terminal -> PC        ##yy1+CR+LF+CRC8

xxxxxxxxxxxxxxxx – Mensagem de 16  
 caracteres

yy – Confirmação de Recepção  
 OK – Confirmado  
 KO - Falhado

Exemplo: ##MSG PARABENS MARIA +CR+LF+CRC8      “ PARABENS MARIA ”

### Gravar ID com uma Impressão Digital Codificada

PC -> Terminal      ##SIzxxxxx+CR+LF+CRC8

Terminal -> PC      ##yy3+CR+LF+CRC8

xxxxx – Número de Utilizador

z – Nível de segurança

0 – BioProx

1 – Prox

2 – Biofree

3 - Captura

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##SI562311+CR+LF+CRC8

Utilizador nº 562311 com modo Prox

### Abertura Remota de Porta

PC -> Terminal      ##AP+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##AP+CR+LF+CRC8

As saídas invertem o seu estado durante n seg

### Bloquear porta

PC -> Terminal      ##BP+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##BP+CR+LF+CRC8

As saídas ficam bloqueadas, excepto a de toques

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

---

### Desbloquear porta

PC -> Terminal      ##DP+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##DP+CR+LF+CRC8      Todas as saídas ficam desbloqueadas

---

### Time-Request (todas as 03h##m, pede o acerto de horário)

Terminal -> Pc      ##TR+CR+LF+CRC8

Pc -> Terminal      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##TR+CR+LF+CRC8      Pedido de acerto de horas

---

### Apagar todas as Impressões Digitais do Terminal

PC -> Terminal      ##AT+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##AT+CR+LF+CRC8      As impressões digitais do terminal são apagadas

### Apagar uma Impressão Digital

PC -> Terminal      ##AUxxxxx+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

xxxxx – Número de Utilizador  
(entre 0 e 99999)

yy – Confirmação de Recepção  
OK – Confirmado  
KO - Falhado

Exemplo: ##AU12345+CR+LF+CRC8

Apagar utilizador nº 12345 no Leitor Biométrico

### Pedido de envio de uma Impressão Digital Codificada já gravada

PC -> Terminal      ##GSxxxxx+CR+LF+CRC8

Terminal -> PC      ##z+CR+LF+CRC8

Terminal -> PC      ##yywt+CR+LF+CRC8

xxxxx – Número de Utilizador  
(entre 0 e 99999)

z – Nº biometrias  
0 – nenhuma biometria  
1 – uma biometria  
2 – duas biometrias  
yy – Confirmação de Recepção  
OK – Confirmado  
KO – Falhado  
w – nº de ordem da biometria  
t – biometria codificada (256 bytes)

Exemplo: Envio de 2ª biometria referente ao User ID 40000

##GS40000+CR+LF+CRC8

Pedir envio da impressão digital nº 40000

##2+CR+LF+CRC8

Pacote recebido com indicação de duas biometrias

##OK1[...]+CR+LF+CRC8

Pacote recebido com mensagem de confirmação e biometria codificada nº1

##OK2[...]+CR+LF+CRC8

Pacote recebido com mensagem de confirmação e biometria codificada nº2

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

www.betronic.com ■ www.sibaccess.com ■ international@betronic.com ■ apoio.clientes@betronic.com

---

### Registar uma impressão digital com envio da mesma (2 pacotes)

PC -> Terminal      ##ETwxxxxxz+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

w – Número do pacote (1 ou 2)

xxxxx – Número de Utilizador  
(entre 0 e 99999)

z – biometria codificada (128 bytes)

yy – Confirmação de Recepção

OK – Confirmado

KO – Falhado

Exemplo: ##ET812345(...)+CR+LF+CRC8

Pacote 8 da Impressão Digital nº 110

---

### Receber Número de Templates de um ID

PC -> Terminal      ##CKxxxxx+CR+LF+CRC8

Terminal -> PC      ##y+CR+LF+CRC8

xxxxx – Número de ID  
(entre 0 e 99999)

y – Número de Templates

Exemplo: ##CK12345+CR+LF+CRC8

Receber o número de templates do User ID12345

---

### Reset do Terminal

PC -> Terminal      ##RB+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

yy – Confirmação de Recepção

OK – Confirmado

KO - Falhado

Exemplo: ##RB+CR+LF+CRC8

Terminal reinicia passados 2 segundos

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)



---

### Diagnóstico de ligação "KEEP-ALIVE"

PC -> Terminal      **##IO+CR+LF+CRC8**

Terminal -> PC      **##IA+CR+LF+CRC8**

Nota: Este comando deve ser enviado de 2 em 2 minutos, de modo a ser possível identificar que o terminal está ligado ao Software, através do ícone que aparece no display do terminal

Exemplo: **##IO+CR+LF+CRC8**

Aparece um ícone no display do terminal

---

### Versão do terminal

PC -> Terminal      **##TE+CR+LF+CRC8**

Terminal -> PC      **##z+CR+LF+CRC8**

z – Mensagem de 16 bytes contendo a versão de firmware do terminal

Exemplo: **##TE+CR+LF+CRC8**

Pedido de versão de firmware do terminal

---

### Pedido de N° de biometrias de um ID

PC -> Terminal      **##CKxxxxx+CR+LF+CRC8**

Terminal -> PC      **##z+CR+LF+CRC8**

xxxxx – Número de Utilizador  
(entre 0 e 99999)

z – N° biometrias  
0 – nenhuma biometria  
1 – uma biometria  
2 – duas biometrias

Exemplo: Envio de 2ª biometria referente ao User ID 40000

**##GS40000+CR+LF+CRC8**

Pedir envio da impressão digital nº 40000

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)

### Registo de biometrias no Cartão

PC -> Terminal      ##SCwxxxxxz+CR+LF+CRC8

Terminal -> PC      ##yy1+CR+LF+CRC8

w – Número do pacote

Nota: 2 primeiros pacotes → 1ª biometria  
2 últimos pacotes → 2ª biometria

xxxxx – Número de Utilizador  
(entre 0 e 99999)

z – biometria codificada (128 bytes)

yy – Confirmação de Recepção

OK – Confirmado

KO – Falhado

Exemplo: ##SC112345(...)+CR+LF+CRC8

Pacote 1 da Impressão Digital nº1 do ID nº 12345

#### Lisboa

Av. do forte nº3, Edifício Suécia I/II, Piso 1 ■ 2794-038 Carnaxide, Portugal  
Tel. (+351) 21 412 32 41 / (+351) 21 410 60 67 ■ Fax. (+351) 21 413 11 27  
Tlm. (+351) 96 173 06 52

#### Porto (Unidade de produção)

Av. Central de S. Fins, nº 581, S. Pedro de Fins ■ 4425-514 Maia, Portugal  
■ Tel. (+351) 22 944 68 75 ■ Fax. (+351) 22 960 60 60  
Tlm. (+351) 96 170 09 79

[www.betronic.com](http://www.betronic.com) ■ [www.sibaccess.com](http://www.sibaccess.com) ■ [international@betronic.com](mailto:international@betronic.com) ■ [apoio.clientes@betronic.com](mailto:apoio.clientes@betronic.com)

## **Anexo 10**

# SIBZone

SISTEMA INTEGRADO BETRONIC



## A SIMPLICIDADE DE UM TOQUE SEGURO

Uma tecnologia de leitura biométrica premiada no evento internacional FVC, em 2004 e 2006, pela demonstração de excelência quer em qualidade, quer em velocidade.



A leitura biométrica por impressão digital é hoje o método de eleição na autenticação de indivíduos que alia segurança, eficácia e univocidade a uma forma de utilização inata, natural e ergonómica.



# SIBzone

SISTEMA INTEGRADO BETRONIC

**SIBZONE ACCESS,**  
idealizado para um melhor controlo e rigor na gestão de acessos.



## BIOFree



Terminal com leitura exclusivamente biométrica, por impressão digital, com capacidade até 5 biometrias por utilizador.

## BIOPROX



Terminal com leitura biométrica, activada por cartão de proximidade (Prox-RF).

## PROX3000



Terminal com leitura (Prox-RF), activada por cartão de aproximação, com opção de leitor de proximidade adicional.



Tecnologia de reconhecimento por biometria premiada nos eventos FVC2004 e FVC2006 pela exibição de elevados níveis de velocidade e segurança no processo de autenticação.

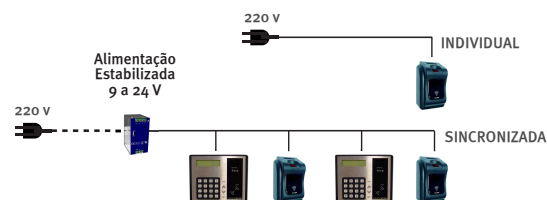


Tecnologias 13,56 MHz Contactless Smart Card / 125 KHz Proximity Access Card em conjugação com uso de cartões com capacidade de memória até 2K bytes e funcionalidade de leitura/escrita asseguram robustez, durabilidade e fiabilidade.

## Características

### Eléctricas

Alimentação: 220 V Individual / 9V - 24V estabilizada  
Protecções: Contra Curto-Circuitos e Sobre tensões  
Autonomia (UPS): Bateria interna recarregável, com capacidade para 2 a 5 h. em caso de quebra de energia



### Hardware

Display: Tipo LCD 16x2 / 24 x 4 opcional  
Controlo: Visual com base em 2 leds e Sonoro com base em Buzzer interno  
Processador: Risc 16 MHz  
Memória: 512 Kb expansível até 1 Mb  
RTCC: Real Time Clock interno  
Comunicações: TCP/IP ou RS485  
Saídas Externas: 4 saídas externas com capacidade de accionar 4 cargas de 1A  
Entradas: 4 entradas com capacidades para aquisição de dados de sensores  
Autonomia Off-line: Capacidade para 5000 utilizadores registados  
Autonomia On-line: Memória para 5000 autenticações  
Autonomia Off-line de armazenamento de templates: 0 a 9500 biometrias  
Normas: IP65, CE, ROHS

### Leitores Biométricos:

#### Tipo: Óptico ou Capacitivo

CPU: 400Mhz DSP  
Memória Flash: 1 Mb extensível a 4 Mb  
Resolução: 500 dpi  
Tempo de identificação: < 1 segundo  
Encriptação: 256bits AES  
Tamanho template: 256 bytes  
Equal error Rate: < 0,1%  
Rotação máxima do dedo: 90º  
Superfície contacto: sólida, anti-arranhão, qualidade assegurada mesmo para dedo húmido  
Algoritmo de autenticação de impressão digital premiado por duas vezes consecutivas (FVC2004 e FVC2006)



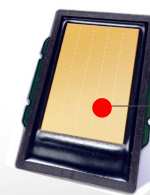
Óptico



COMPARATIVO



Capacitivo



- Sem necessidades especiais manutenção/limpeza
- Degradação da superfície de contacto diminui performance
- Maior robustez face a condições adversas (humidade)
- Menor custo

- Necessidade de protecção contra ESD
- Maior fiabilidade e robustez do processo de autenticação
- Maior portabilidade
- Resolução idêntica ao Óptico

## Funcionalidades

User ID: um ou mais templates associados

Cada template associado a uma dada função: ponto, acesso, emergência, outros.

## R/F Proximidade:

13,56 Mhz com 16 Kb de memória, possibilidade de ser re-escrito indefinidamente

125 Khz com 26 bts de memória, numero de identificação definido de fábrica.

## ■ Firmware

### Configuração:

Firmware totalmente configurável através do PC, com recurso a Software de Configuração. Validação:

Cada movimento poderá ser submetido a um conjunto de parâmetros de validação configuráveis de forma a trabalharem individualmente ou em conjunto.

## ■ Mecânicas

Temperatura de funcionamento: -10°C a 55°C / 14°F a 131°F

Humidade: 99% não condensada

Dimensões: 148mm x 85mm x 75mm

## ■ Requisitos mínimos para a instalação de um terminal SIBZONE

Ponto de alimentação 220V, Ponto de rede 10/100 TCP/IP, ou cabo de comunicações RS485

Fixação do terminal em parede lisa com montagem vertical e inclinação a 0° ou montagem em coluna vertical com posição horizontal e inclinação entre 10° a 20°.

## ■ Aplicações

Captura de dados gerais (produção, obras, outros)

Controlo de acessos

Controlo e gestão de assiduidade

Controlo e gestão de bilhética

Outras

## **Anexo 11**



# SIBTOWER

SISTEMA INTEGRADO BETRONIC



O SIBTOWER é um sistema integrado, com SIB Access Monitor, o qual permite efectuar a gestão de acesso de utentes a determinados espaços condicionados.

Uma solução totalmente informatizada e com autenticação e com equipamentos sem bloqueio físico (SIB Tower).  
Uma solução testada e desenvolvida com a certificação do Hospital de S. António do Porto.

# SIBTOWER

SISTEMA INTEGRADO BETRONIC

O SIBTOWER, idealizado para o controlo e gestão de acessos, integrado com a tecnologia de Biometria "FingerPrint Recognition Algorithm", faz a comparação da impressão digital do utilizador com uma template presente no cartão de proximidade negando ou não o seu acesso. A combinação da leitura de proximidade com um leitor de impressões digitais incrementa ao controlo de acessos um nível de segurança com uma eficácia assegurada.

## Protecção de Dados Pessoais

Todas as entidades públicas ou privadas que procedam ou pretendam proceder ao tratamento de dados pessoais, por meios total ou parcialmente automatizados, como é o caso das soluções Betronic para Controlo de Assiduidade, Gestão de Recursos Humanos, Segurança, Identificação e Controlo de Acessos nos termos previstos no art. 4.º da Lei 67/98, de 26 de Outubro, deverão contactar a CNPD para efeitos de autorização ou registo, sendo que como neste caso do SIBTOWER, a impressão digital está indexada no interior do cartão deixa de existir a necessidade de uma base de dados com detalhes do utilizador, eliminado a obrigatoriedade de registar na CNPD.



## Configurações possíveis

### BIOFree



Terminal com leitura exclusivamente biométrica, por impressão digital. Capacidade para 1900 utilizadores (expansível a 9600) FAR: 0,0001%

### PROX3000



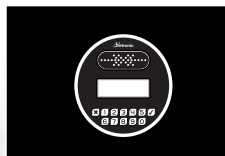
Terminal com leitura (Prox-RF), activada por cartão de aproximação.

### BIOPROX



Terminal com leitura biométrica (impressão digital), activada por cartão de proximidade e leitor de proximidade adicional.

### TECLADO



identificação e administração local do sistema via teclado.

# SIBTOWER

SISTEMA INTEGRADO BETRONIC

## Características

### Eléctricas

Alimentação: 9V - 24V  
Protecções: Contra Curto-Circuitos e Sobre tensões  
Alimentação de Reserva (opcional): UPS

### Hardware

Display: Tipo LCD 2 linhas (16x2)  
Controlo: Visual com base em 2 leds e Sonoro com base em Besouro interno  
Processadores: Processador Risc 16 MHz  
Memória: 64 Kbytes expansível até 256 kbytes  
RTCC: Real Time Clock interno  
Comunicações: TCP/IP ou RS485  
Saídas Externas: 4 saídas externas com capacidade de accionar 3 cargas de 1A e uma até 0,5A  
Entradas: 4 entradas com capacidades para aquisição de dados de sensores  
Capacidade para 4000 utilizadores Off-line  
Memória para 2000 autenticações Off-line

### Firmware

Configuração: Firmware totalmente configurável através do PC, com recurso a Software de Configuração.  
Validação: Cada movimento poderá ser submetido a um conjunto de parâmetros de validação configuráveis de forma a trabalharem individualmente ou em conjunto.

### Mecânicas

Temperatura de funcionamento: -10°C a 55°C / 14°F a 131°F  
Humidade: 99% não condensada

Dimensões:  
Altura: 1100mm  
Diâmetro: 150mm

### Requisitos mínimos

Os requisitos mínimos para a instalação de um terminal SIBTOWER são:  
Ponto de alimentação 9V - 24V, Ponto de rede 10/100 TCP/IP, ou cabo de comunicações.  
Base de fixação ao solo

### Comunicações

A comunicação TCP/IP permite que um terminal de ponto seja interligado a uma vulgar rede Ethernet, assim através da qual os terminais podem ser ligados e endereçados a partir de uma rede local, ou mesmo, através da Internet.

## **Anexo 12**

# SIBzone

SISTEMA INTEGRADO BETRONIC



## A SIMPLICIDADE DE UM TOQUE SEGURO



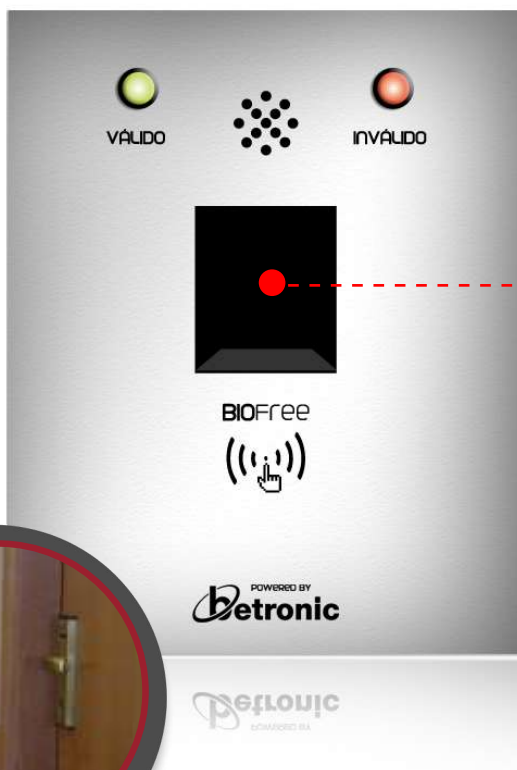
Uma tecnologia de leitura biométrica premiada no evento internacional FVC, em 2004 e 2006, pela demonstração de excelência quer em qualidade, quer em velocidade.

A leitura biométrica por impressão digital é hoje o método de eleição na autenticação de indivíduos que alia segurança, eficácia e univocidade a uma forma de utilização inata, natural e ergonómica.

# SIBzone

SISTEMA INTEGRADO BETRONIC

**MINISIBZONE ACCESS,**  
idealizado para um melhor controlo e rigor na gestão de acessos.



## BIOfree



Terminal com leitura exclusivamente biométrica, por impressão digital, com capacidade até 5 biometrias por utilizador.



## Características

### Eléctricas

Alimentação: 220 V Individual / 9V - 24V estabilizada  
Protecções: Contra Curto-Circuitos e Sobre tensões  
Autonomia (UPS): Bateria interna recarregável, com capacidade para 2 a 5 h. em caso de quebra de energia

### Hardware

Controlo: Visual com base em 2 leds e Sonoro com base em Besouro interno  
Processador: Risc 16 MHz  
Memória: 512 Kb expansível até 1 Mb  
RTCC: Real Time Clock interno  
Comunicações: TCP/IP ou Wireless  
Saídas Externas: 4 saídas externas com capacidade de accionar 4 cargas de 1A  
Entradas: 4 entradas com capacidades para aquisição de dados de sensores  
Autonomia Off-line: Capacidade para 4000 utilizadores registados  
Autonomia On-line: Memória para 10.000 autenticações  
Autonomia Off-line de armazenamento de templates: 0 a 10.000 biometrias  
Normas: IP65, CE, ROHS

### Leitores Biométricos:

#### Tipo: Óptico ou Capacitivo

CPU: 400Mhz DSP  
Memória Flash: 1 Mb extensível a 4 Mb  
Resolução: 500 dpi  
Tempo de identificação: < 1 segundo  
Encriptação: 256bits AES  
Tamanho template: 256 bytes  
Equal error Rate: < 0,1%  
Rotação máxima do dedo: 90º  
Superfície contacto: sólida, anti-arranhão, qualidade assegurada mesmo para dedo húmido  
Algoritmo de autenticação de impressão digital premiado por duas vezes consecutivas (FVC2004 e FVC2006)

#### Funcionalidades



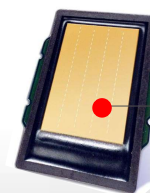
Óptico



COMPARATIVO



Capacitivo



- Sem necessidades especiais manutenção/limpeza
- Degradação da superfície de contacto diminui performance
- Maior robustez face a condições adversas (humidade)
- Menor custo

- Necessidade de protecção contra ESD
- Maior fiabilidade e robustez do processo de autenticação
- Maior portabilidade
- Resolução idêntica ao Óptico

# SIBzone

SISTEMA INTEGRADO BETRONIC

User ID: um ou mais templates associados  
Cada template associado a uma dada função: ponto, acesso, emergência, outros.

## ■ Firmware

### **Configuração:**

Firmware totalmente configurável através do PC, com recurso a Software de Configuração. Validação: Cada movimento poderá ser submetido a um conjunto de parâmetros de validação configuráveis de forma a trabalharem individualmente ou em conjunto.

## ■ Mecânicas

Temperatura de funcionamento: -10°C a 55°C / 14°F a 131°F  
Humidade: 99% não condensada  
Dimensões: 148mm x 85mm x 75mm

## ■ Requisitos mínimos para a instalação de um terminal SIBZONE

Ponto de alimentação 220V, Ponto de rede 10/100 TCP/IP, ou rede Wireless  
Fixação do terminal embutido em parede lisa com montagem vertical e inclinação a 0°

## ■ Aplicações

Captura de dados gerais (produção, obras, outros)  
Controlo de acessos  
Controlo e gestão de assiduidade  
Outras



## **Anexo 13**

# SIBzone

SISTEMA INTEGRADO BETRONIC



## A SIMPLICIDADE DE UM TOQUE SEGURO



Uma tecnologia de leitura biométrica premiada no evento internacional FVC, em 2004 e 2006, pela demonstração de excelência quer em qualidade, quer em velocidade.



A leitura biométrica por impressão digital é hoje o método de eleição na autenticação de indivíduos que alia segurança, eficácia e univocidade a uma forma de utilização inata, natural e ergonómica.



# SIBzone

SISTEMA INTEGRADO BETRONIC

**SIBZONE STRONG ACCESS,**  
idealizado para um melhor controlo e rigor na gestão de acessos.



## PROX3000



Terminal com leitura (Prox-RF), activada por cartão de aproximação, com opção de leitor de proximidade adicional.

## BIOPROX



Terminal com leitura biométrica, activada por cartão de proximidade (Prox-RF).

## BIOFree



Terminal com leitura exclusivamente biométrica, por impressão digital, com capacidade até 9600 utilizadores.



Tecnologia de reconhecimento por biometria premiada nos eventos FVC2004 e FVC2006 pela exibição de elevados níveis de velocidade e segurança no processo de autenticação.



Tecnologia 125 KHz Proximity Access Card e funcionalidade de leitura encriptada de 26 Bits, assegurando robustez, durabilidade e fiabilidade.

## Características

### Eléctricas

Alimentação: 220 V Individual / 9V - 24V estabilizada  
Protecções: Contra Curto-Circuitos e Sobre tensões  
Alimentação de Reserva: Constituída por bateria recarregável de 9V permitindo autonomia para várias horas em funcionamento normal independentemente do leitor usado.



### Hardware

Display: Tipo LCD 4x20 com backlight  
Controlo: Visual com base em 3 leds ( Vermelho, Amarelo e Verde ) e sonoro com base num besouro interno  
Processador: 2 processadores de 8 bits e alta performance  
Memória: 32KB de memória de dados não volátil ( expansível para 128KB )  
RTCC: Real Time Clock interno  
Comunicações: Standard a 9600 bits/S tipo: RS232 (1 terminal até 15m) RS485 (31 terminais até 1200m)  
Multi-RS485 (124 terminais até 1200m) Modem TCP/IP Canal Rx/Tx extra para usos gerais  
Saídas Externas: 2 relés com contacto normalmente aberto ( 7A 250V a.c. / 7A 30V d.c.), totalmente configuráveis quer em termos de actividade quer em termos de accionamento  
Autonomia Off-line: Capacidade para 4000 utilizadores registados  
Autonomia On-line: Memória para 2000 autenticações  
Autonomia Off-line de armazenamento de templates: 0 a 9600 biometrias  
Normas: IP65, CE

### Leitor Biométrico:

#### Tipo: Óptico ou Capacitivo

CPU: 32 Bit RISC (66Mhz)  
Memória : 150 biometrias  
Resolução: 506 dpi  
Tempo de identificação: < 1 segundo  
Encriptação: 256bits  
Tamanho template: 256 bytes  
Equal error Rate: < 0,1%  
Superfície contacto: sólida, anti-arranhão, qualidade assegurada mesmo para dedo húmido



Óptico



- Sem necessidades especiais manutenção/limpeza
- Degradação da superfície de contacto diminui performance
- Maior robustez face a condições adversas (humidade)
- Menor custo

**R/F Proximidade:**

125 Khz com 26 Bits de memória, numero de identificação definido de fábrica.

■ **Firmware**

**Configuração:**

Firmware totalmente configurável através do PC, com recurso a Software de Configuração.

Validação: Cada movimento poderá ser submetido a um conjunto de parâmetros de validação configuráveis de forma a trabalharem individualmente ou em conjunto.

■ **Mecânicas**

Temperatura de funcionamento: -10°C a 55°C / 14°F a 131°F

Humidade: 99% não condensada

Dimensões: 220mm x 165mm x 45mm

■ **Requisitos mínimos para a instalação de um terminal SIBZONE**

Ponto de alimentação 220V, Ponto de rede 10/100 TCP/IP, ou cabo de comunicações RS485

Fixação do terminal em parede lisa com montagem vertical e inclinação a 0° ou montagem em coluna vertical com posição horizontal com inclinação entre 10° a 20°.

■ **Aplicações**

Captura de dados gerais (produção, obras, outros)

Controlo de acessos

Controlo e gestão de assiduidade

Controlo e gestão de bilhética

Outras

## **Anexo 14**

# SIBPARK BARRIER

SISTEMA INTEGRADO BETRONIC



UMA BARREIRA FÁCIL E ECONÓMICA



No sector privado, comercial ou industrial, há a necessidade de gerir o acesso a pessoas autorizadas. Existem várias tecnologias para este efeito, mas a Barreira automática é, ainda, a solução mais simples e económica. A linha **SIBPARK** oferece uma gama completa de produtos fiáveis e seguros.

Qualquer modelo **SIBPARK** pode ser activado por comando à distância, chave magnética, cartão magnético embutido no chão, chave personalizada ou botoneira instalada na portaria.

Além da própria detecção de obstáculo das barreiras, não podemos prescindir das fotocélulas de segurança, que fazem parte integrante de um bom funcionamento do sistema.

# SIBPARK BARRIER

SISTEMA INTEGRADO BETRONIC

**SIBPARKBARRIER**, constituído por uma barreira automática para uso intensivo, composto por um motor electrohidráulico monofásico de 220V. com desencravamento manual (caso falte a corrente eléctrica), com aste até 7 metros, em alumínio com pintura termolacada a branco, com reflectores. Quadro electrónico em caixa P.V.C. protegido por fusíveis e por acopladores ópticos nas entradas contra descargas eléctricas até 2500 de pico.

Quadro com 3 sistemas de funcionamento: Automático normal, Temporizado e Parque.

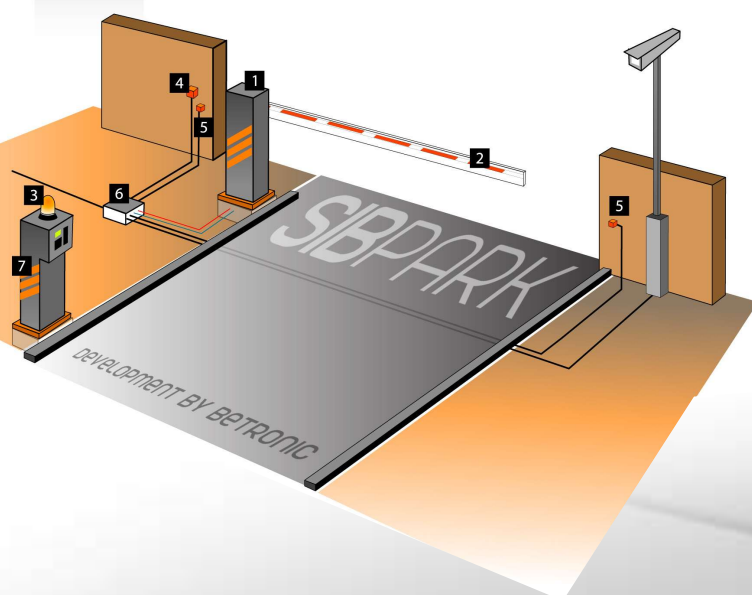
Tem ainda 4 sistemas de funcionamento suplementares de segurança do motor por fins de curso, válvulas de By-Pass, temporização de trabalho e ampola térmica.

## Características

	RÁPIDA		STANDART	
	2 / 2,5 / 3	4	4 / 5	4 / 5 / 7
Comprimento máximo de haste (m)	2 / 2,5 / 3	4	4 / 5	4 / 5 / 7
Tempo máximo de abertura (s)	2	3	3,5	4,5
Tipo de haste	NORMAL / SAIA / ARTICULADA			
Alimentação	230V - (-6+10%) 50 Hz			
Térmico do motor	120°C			
Sistema de anti-esmagamento	REGULAÇÃO POR VÁLVULAS DE BY-PASS			
Temperatura de funcionamento	-20°C +55°C			
Acabamento	Personalizado			
Grau de protecção	IP44			

### CARACTERÍSTICAS TÉCNICAS DO MOTOR

Velocidade (rpm)		
Potência (w)	2800	1400
Corrente absorvida (a)	200	200
Alimentação	230V - (-6+10%) 50 Hz	



- 1 Barreira
- 2 Haste
- 3 Lâmpada Sinalizadora
- 4 Chave de Contacto
- 5 Células fotoeléctricas
- 6 Caixa de Controle/Derivação
- 7 Torre de Comando  
Chave magnética, cartão magnético, chave personalizada ou botoneira instalada na portaria
- 8 Câmara de Vigilância



## **Anexo 15**

# SIBzone

SISTEMA INTEGRADO BETRONIC



## A SIMPLICIDADE DE UM TOQUE SEGURO

VERSÃO ENTERPRISE

Uma tecnologia de leitura biométrica premiada no evento internacional FVC, em 2004 e 2006, pela demonstração de excelência quer em qualidade, quer em velocidade.



A leitura biométrica por impressão digital é hoje o método de eleição na autenticação de indivíduos que alia segurança, eficácia e univocidade a uma forma de utilização inata, natural e ergonómica.



# SIBzone

SISTEMA INTEGRADO BETRONIC

**SIBZONE ENTERPRISE,**  
idealizado para um melhor controlo e rigor na gestão de assiduidade.



## BIOFree

Terminal com leitura exclusivamente biométrica, por impressão digital, com capacidade até 5 biometrias por utilizador.



## BIOPROX

Terminal com leitura biométrica, activada por cartão de proximidade (Prox-RF).



## PROX3000

Terminal com leitura (Prox-RF), activada por cartão de aproximação, com opção de leitor de proximidade adicional.



## TECLADO

identificação e administração local do sistema via teclado.



Tecnologia de reconhecimento por biometria premiada nos eventos FVC2004 e FVC2006 pela exibição de elevados níveis de velocidade e segurança no processo de autenticação.

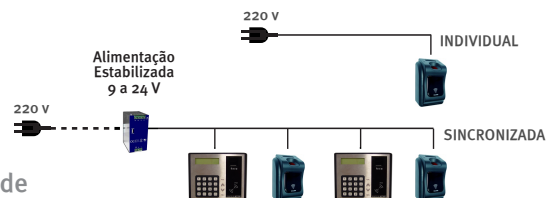


Tecnologias 13,56 MHz Contactless Smart Card / 125 KHz Proximity Access Card em conjugação com uso de cartões com capacidade de memória até 2K bytes e funcionalidade de leitura/escrita asseguram robustez, durabilidade e fiabilidade.

## Características

### Eléctricas

Alimentação: 220 V Individual / 9V - 24V estabilizada  
Protecções: Contra Curto-Circuitos e Sobre tensões  
Autonomia (UPS): Bateria interna recarregável, com capacidade para 2 a 5 h. em caso de quebra de energia



### Hardware

Display: Tipo LCD 16x2 / 24 x 4 opcional  
Controlo: Visual com base em 2 leds e Sonoro com base em Buzzer interno  
Processador: Risc 16 MHz  
Memória: 512 Kb expansível até 1 Mb  
RTCC: Real Time Clock interno  
Comunicações: TCP/IP ou RS485  
Saídas Externas: 4 saídas externas com capacidade de accionar 4 cargas de 1A  
Entradas: 4 entradas com capacidades para aquisição de dados de sensores  
Autonomia Off-line: Capacidade para 5000 utilizadores registados  
Autonomia On-line: Memória para 5000 autenticações  
Autonomia Off-line de armazenamento de templates: 0 a 9500 biometrias  
Normas: IP65, CE, ROHS

### Leitores Biométricos:

#### Tipo: Óptico ou Capacitivo

CPU: 400Mhz DSP  
Memória Flash: 1 Mb extensível a 4 Mb  
Resolução: 500 dpi  
Tempo de identificação: < 1 segundo  
Encriptação: 256bits AES  
Tamanho template: 256 bytes  
Equal error Rate: < 0,1%  
Rotação máxima do dedo: 90º  
Superfície contacto: sólida, anti-arranhão, qualidade assegurada mesmo para dedo húmido  
Algoritmo de autenticação de impressão digital premiado por duas vezes consecutivas (FVC2004 e FVC2006)



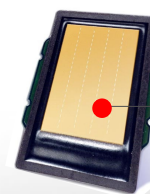
Óptico



COMPARATIVO



Capacitivo



- Sem necessidades especiais manutenção/limpeza
- Degradação da superfície de contacto diminui performance
- Maior robustez face a condições adversas (humidade)
- Menor custo

- Necessidade de protecção contra ESD
- Maior fiabilidade e robustez do processo de autenticação
- Maior portabilidade
- Resolução idêntica ao Óptico

## Funcionalidades

User ID: um ou mais templates associados

Cada template associado a uma dada função: ponto, acesso, emergência, outros.

## R/F Proximidade:

13,56 Mhz com 16 Kb de memória, possibilidade de ser re-escrito indefinidamente

125 Khz com 26 bts de memória, numero de identificação definido de fábrica.

## ■ Teclado

Teclado alfanumérico com teclas de apoio para identificação e administração local, teclas de navegação para selecção de menu.

## ■ Firmware

### Configuração:

Firmware totalmente configurável através do PC, com recurso a Software de Configuração. Validação:

Cada movimento poderá ser submetido a um conjunto de parâmetros de validação configuráveis de forma a trabalharem individualmente ou em conjunto.

## ■ Mecânicas

Temperatura de funcionamento: -10°C a 55°C / 14°F a 131°F

Humidade: 99% não condensada

Dimensões: 148mm x 128mm x 38mm

## ■ Requisitos mínimos para a instalação de um terminal SIBZONE

Ponto de alimentação 220V, Ponto de rede 10/100 TCP/IP, ou cabo de comunicações RS485

Fixação do terminal em parede lisa com montagem vertical e inclinação a 0° ou montagem em coluna vertical com posição horizontal e inclinação entre 10° a 20°.

## ■ Aplicações

Captura de dados gerais (produção, obras, outros)

Controlo de acessos

Controlo e gestão de assiduidade

Controlo e gestão de bilhética

Outras