Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica

Trabalho de Conclusão de Curso – TCC

Projeto e Implementação de um Sistema de Segurança Eletrônica Bluetooth.

Juliano Rodrigues Fernandes de Oliveira
jrfo@cpqd.com.br

Orientador:
Dr. Antonio Marcus Nogueira Lima

Campina Grande, Janeiro de 2006.

Biblioteca Setorial do CDSA. Fevereiro de 2021.

Sumé - PB

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Departamento de Engenharia Elétrica

Trabalho de Conclusão de Curso – TCC

Projeto e Implementação de um Sistema de Segurança Eletrônica Bluetooth.

Juliano Rodrigues Fernandes de Oliveira
(Aluno)

Dr. Antonio Marcus Nogueira Lima
(Orientador)

Sumário

Lista de Figuras

Lista de Tabelas

1. Introdução

Para acesso a ambientes, sistemas de segurança mecânica são amplamente utilizados (fechaduras mecânicas), porém atualmente os sistemas de segurança puramente mecânico são facilmente burlados.

Necessitando de uma maior segurança para acesso a determinados ambientes, a eletrônica embarcada associou-se à segurança mecânica, com o objetivo de aumentar o nível de confiabilidade dos sistemas de segurança utilizando para acesso aos ambientes.

Códigos identificam o usuário que está acessando um determinado ambiente através de diversos métodos, entre estes estão os cartões magnéticos, teclados para digitação manual da senha, entre outros.

O Brasil possui aproximadamente 86 milhões de usuários de telefonia móvel celular. A rápida difusão do celular deixou clara a importância da mobilidade no dia-a-dia das pessoas e abriu caminho para a propagação de outras tecnologias que têm como grande apelo livrar o mundo dos fios. Usuários cada vez mais interessados em soluções sem fio aos poucos descobrem os benefícios do Bluetooth, arquitetura que vem ampliando seu potencial e promete movimentar o mercado nos próximos anos.

Bluetooth é uma tecnologia de rádio de curto-alcance criada pela Ericsson em meados da década de 90 e desenvolvida hoje por diversas companhias [13]. Esta tecnologia sem fio elimina os cabos usados para conectar os dispositivos digitais. Baseada em um link de rádio de curto alcance e baixo custo, essa tecnologia pode conectar vários tipos de dispositivos sem a necessidade de cabos, proporcionando uma maior liberdade de movimento.

É desejável um sistema de segurança que possua mobilidade e utilize os atuais recursos disponíveis pelo usuário. Dada estas condições temos que uma ótima opção está em torno da utilização do telefones inteligentes (smartphone) com comunicação Bluetooth embarcada como a ferramenta de autenticação de um sistema de segurança.

Neste trabalho de conclusão de curso, trataremos das etapas de projeto e desenvolvimento da ferramenta de segurança eletrônica para acesso seguro a ambientes através da comunicação Bluetooth, e desenvolvimento do software embarcado do telefone inteligente que realiza a autenticação com o dispositivo eletrônico desenvolvido.

2. Objetivos

2.1. Objetivos Gerais

Desenvolver um sistema de segurança para acesso a determinado ambiente, onde a autenticação de acesso seja realizada por conexão 'sem fio' Bluetooth através de um telefone inteligente (smartphone).

2.2. Objetivos Específicos

Objetivamos agregar eletrônica de acionamento e comunicação sem fio Bluetooth a um microcontrolador que compõe o núcleo de processamento do sistema de segurança de tal maneira que seja possível através de comunicação conforme os devidos protocolos de comunicação conectar um dispositivo Bluetooth remoto ao circuito eletrônico desenvolvido, visando recepção de comandos que serão processados no sistema de segurança para permitir o acesso do portador do dispositivo ao ambiente sob segurança.

3.WBTV42-D-SPP Módulo de comunicação Bluetooth [1]

Os fatores determinantes na escolha pelo módulo de comunicação Bluetooth como componente do sistema de segurança foram basicamente: Custo (próximo a 30 dólares), disponibilidade em laboratório e suporte ao perfil de porta serial, este fator facilitador na realização da comunicação entre o microcontrolador núcleo do sistema de segurança e o módulo Bluetooth através de uma conexão serial RS232.

3.1 Características

- Bluetooth compatível com versão 1.2;
- Antena interna;
- 8Mb memória Flash externa;
- Máxima taxa da UART: 921.6kbps;
- BT classe 2, alcance nominal 30 metros;
- Alimentação única de 3.3V;
- Firmware embarcado implementa perfil de comunicação através de comandos AT;
- Rápida integração a tecnologia wireless;
- 34-ball BGA Package: 1.33" x .58" (33.0 x 14.7mm);
- 24-pin DIP Package: 1.40" x .90" (35.0 x 25.0mm).

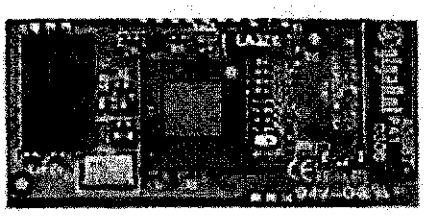

Figura 1A

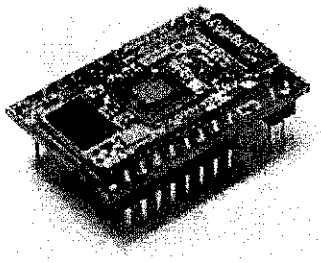

Figura 1B

Figura 1 – WBTV42-D-SPP. A) 34-Ball BGA. B) 24-pin DIP

3.2 Descrição Geral

O módulo Wintec WBTV42 integra o controlador de banda base Bluetooth com o componente de radio freqüência (RF), memória Flash, cristal oscilador e antena embutida (ilustrado pela Figura 2), provendo uma solução de tecnologia sem fio de baixo custo para aplicações embarcadas.

A Figura 2 ilustra o diagrama de blocos e a interface de entrada e saída do módulo WBTV42.

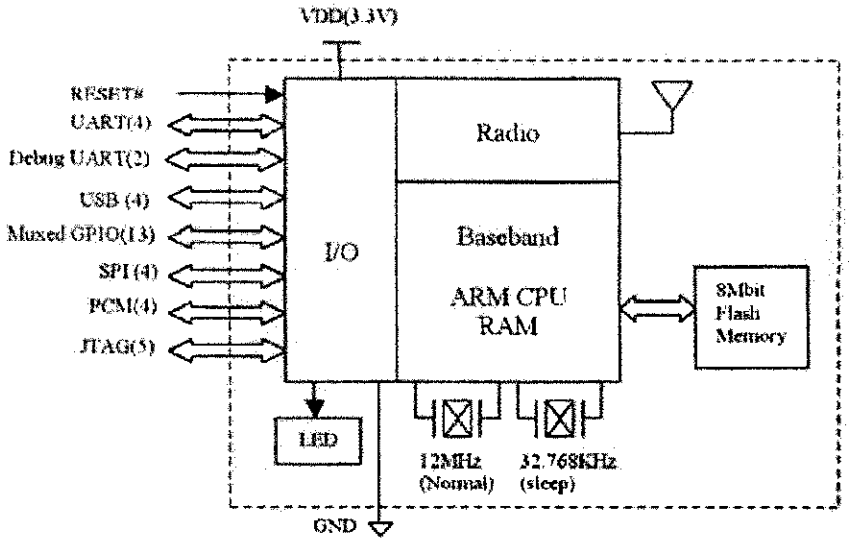

Figura 2 – Diagrama de blocos do módulo WBTV42

O módulo WBTV42 é compatível com a especificação Bluetooth v1.2. O controlador da banda base contém um microcontrolador RISC de 32-bit com núcleo composto por um microprocessador ARM7TDMI que executa o software que contém a pilha Bluetooth. O ARM7TDMI permite instruções ARM de 32-bit misturadas com instruções ARM de 16-bit para prover melhorias no tempo de execução. Os cristais osciladores são utilizados como fonte de relógio do módulo de acordo com o modo de operação, 12MHz para operação normal e 32,768kHz no modo de espera. O módulo requer alimentação através de uma fonte de 3,3 Volts DC. Na próxima seção serão descritos com mais detalhes as interfaces de entrada e saída do módulo WBTV42.

3.3 Descrição Funcional

O rádio Bluetooth opera na região não licenciada, na banda ISM 2,4GHz. O esquema de distribuição do espectro divide a banda em 79 freqüências começando de 2,402GHz (incrementos de 1MHz), para combater o efeito de interferências e desvanecimento. O desvio de freqüência a partir da freqüência portadora é de +/- 140 até +/-175kHz, para representação dos "0" e "1" e a técnica de modulação usada consiste na técnica de modulação binária Gaussiana de deslocamento de freqüência (FSK – Frequency-shift keying). A taxa de varredura por freqüências é de 1600 buscas/seg, ou 625μseg por freqüência. A busca por freqüências é determinada por uma seqüência de busca pseudo-randômica, que é única para cada piconet, e pode suportar um mestre e no máximo 7 escravos.

A banda base recebe através do radio o sinal, converte para forma digital, realiza a descompressão, extrai as informações dos pacotes, e checa os códigos de detecção de erro (ECC). Na transmissão, envia os dados em pacotes, determina os identificadores, gera o ECC, e converte o dado digital para forma a qual possa ser transmitida utilizando o transmissor de RF (ou seja, modula o sinal digital).

Os dados são transferidos a uma taxa máxima de aproximadamente 1Mbps. O cabeçalho do protocolo limita o bluetooth a taxas entre 723,2kbps e 57,6kbps por um link sem conexão assíncrono (ACL), ou no máximo 433,9kbps para cada caminho de um link sem conexão síncrono.

O módulo WBTV42 possui uma antena embutida, mas não utiliza um amplificador de potência para poder economizar energia. A sensibilidade do receptor é de aproximadamente –86dBm típico. A faixa nominal de comunicação está limitada em 30 metros (a 0 dBm).

O módulo Bluetooth WBTV42 foi desenvolvido para suportar uma variedade interfaces padrões de hardware, descritos abaixo.

1. Interface UART de comunicação com o microprocessador host: 9600, 19,2k, 38,4k, 57,6k, 115,2k, 230,4k, 460,8k e 921,6kbps. Juntamente com os pinos

de TX e RX, a interface UART suporta os sinais de controle de fluxo por hardware CTS e RTS. Dois pinos adicionais DUART_TX e DUAR_RX são providos para debug via UART. Um LED integrado ao modulo sinaliza a atividade de recepção da UART.

2. Interface USB: A interface USB embutida é compatível com a versão 1.1, com taxa de transmissão de dados de 12Mbps na velocidade máxima e 1,5Mbps a velocidade baixa. É capaz de transmitir dados ao modulo Bluetooth a uma taxa maior que a necessária, e por padrão a interface USB é desativada na configuração padrão do módulo.
3. porta GPIO: 13 pinos individuais programáveis como entrada ou saída, multiplexados com outros sinais são providos para uso geral.
4. SPI: Interface serial de 4-fios e alta velocidade, operando a 12MHz na operação como escravo e 6MHz na operação como mestre.
5. Interface PCM para aplicações de áudio com suporte de acesso direto à memória (DMA). Na interface PCM, o pino de entrada PCM_IN possui um resistor de pull-up interno. O usuário pode deixar os pinos da interface PCM desconectados, caso a mesma não seja utilizada.
6. Interface JTAG. Todas as entradas JTAG, tais como TDI, TCK, TMS e TRSTN, possuem resistores de pull-up e pull-down internos. O usuário pode deixar os pinos da interface JTAG desconectados, caso a mesma não seja utilizada.

3.4 Pilha de Software Bluetooth

A pilha de software Bluetooth é composta pela parte alta residente na memória flash juntamente com parte baixa que opera no hardware da banda base. A mesma é ilustrada pela Figura 3.

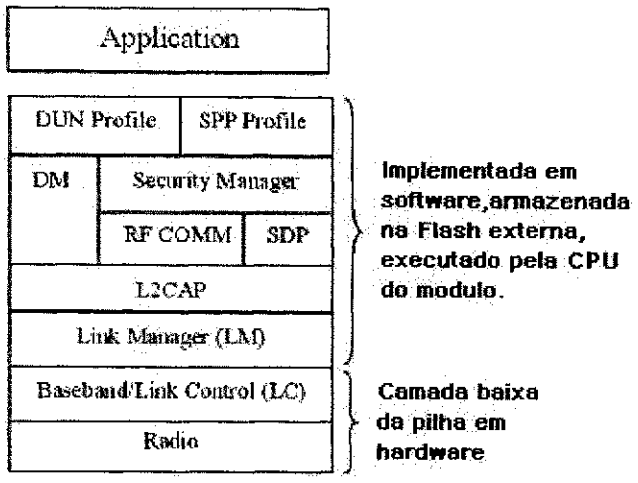

Figura 3 – Pilha Bluetooth típica

A camada alta da pilha inclui o L2CAP (Protocolo de adaptação e controle do link lógico), RFCOMM (Comunicação por Rádio Freqüência), SPP (perfil de porta serial) e DUN (Rede dial-up). O L2CAP realiza a tarefa de multiplexação para suporte a vários protocolos, tais como SDP (Protocolo para Descoberta de Serviços) e RFCOMM, executados sobre a L2CAP, as tarefas de segmentação e reconstrução para as transmissões de pacotes com comprimento de até 64kB e o agrupamento de dispositivos Bluetooth em uma piconet.

A camada SDP disponibiliza meios para as aplicações descobrirem quais serviços estão disponíveis. Isto consiste no serviço de banco de dados de descoberta para os dispositivos com as interfaces: servidor e cliente. A interface cliente local permite que uma aplicação procure por serviços disponíveis no dispositivo remoto. O modulo WBTV42 suporta comunicação para rede scatternet com no máximo 4 piconets.

O gerenciamento de link (link manager) é executado pela CPU embarcada no módulo WBTV42 e gerência a comunicação entre os dispositivos Bluetooth. Cada dispositivo Bluetooth possui seu próprio gerenciador de link que descobre gerenciadores de link's provenientes de dispositivos remotos e comunica-se com os mesmos para manusear a instalação do link entre eles, negociando as características, autenticando a qualidade do serviço (QoS), criptografia e ajuste da taxa de dados no link de forma dinâmica.

A camada RFCOMM é um protocolo de transporte para emulação da porta serial. É emulado o controle da RS232 e os sinais de dados, tais como CTS. Suporta até 60 conexões simultâneas entre dois dispositivos Bluetooth permitindo transmissão e recepção de pacote de dados de até 32kB de tamanho.

Os perfis SPP/DUN habilitam o uso da sintaxe de comandos AT no processador hospedeiro. O conjunto de comandos AT é enviado sob a forma de string de caracteres pelo dispositivo Bluetooth.

A pilha de protocolos bluetooth do módulo WBTV42 possui diferentes configurações, porém, em todos os casos a camada baixa da pilha, incluindo o rádio, banda base e o gerenciador de link, é incorporada ao módulo WBTV42.

O perfil de porta serial (SPP) define como configurar e conectar a porta serial virtual entre dois dispositivos sem fio que possuem a tecnologia Bluetooth. O perfil de porta serial emula uma conexão RS232 utilizando os sinais de controle de fluxo RS232. O perfil assegura o uso de taxas de comunicação de até 128kbps. Este perfil é comumente escolhido para aplicações embarcadas como a definida por este trabalho de conclusão de curso, assim justificando a preferência pelo uso da mesma.

A opção SPP do modulo WBTV42 contém completamente a camada superior e inferior da pilha de protocolos Bluetooth juntamente com a aplicação suporte para o perfil SPP. A camada superior da pilha de protocolos associado com o perfil SPP é armazenada na memória Flash e executada pelo núcleo ARM no modulo. O sistema host (neste caso o microcontrolador PIC) comunica-se com o modulo Bluetooth através da sintaxe de comandos AT. A taxa de comunicação padrão é 115kbps.

3.5 Aplicação

Três comandos do tipo AT são requeridos para estabelecimento de uma conexão Bluetooth com outro dispositivo SPP Bluetooth, são eles: DISCOVERY, BOND e CONNECT. O módulo pode ser utilizado em conexões ponto-a-ponto, ponto-multiponto e scatternet com a taxa de comunicação de dados Bluetooth variando entre 57,6kbps e 723,2kbps.

Quando um link Bluetooth é estabelecido com outro dispositivo SPP Bluetooth, uma piconet é configurada. Um dos dispositivos Bluetooth age como mestre, tomando o controle para propósitos de sincronização. Na conexão do tipo ponto-a-ponto, existem somente a presença de um dispositivo mestre e um dispositivo escravo que comunica somente entre si. Uma conexão multi-ponto consiste em um dispositivo mestre e até no máximo 7 dispositivos escravos compartilhando dados entre os dispositivos da mesma piconet. Na conexão entre dispositivos de diferente piconets é conhecido como scatternet. Isto é quando dois ou mais piconets comunicam entre si, estas piconets não precisam estar sincronizadas e o dispositivo mestre em uma piconet pode ser um dispositivo escravo em outra piconet. A Figura 4 ilustra graficamente os modos de configuração das redes sem fio Bluetooth. O módulo Wintec Bluetooth suporta todos estes modos descritos anteriormente.

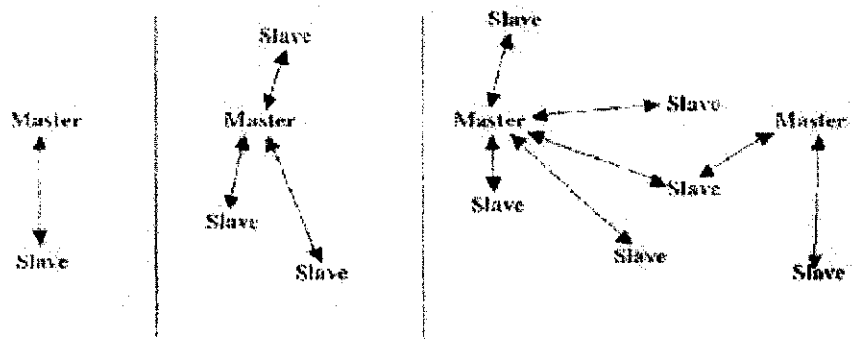

Figura 4 – rede ponto-a-ponto, ponto-multiponto e scatternet

3.6 Operação SPP

Quando o host envia comando ao módulo WBTV42, uma resposta é retornada ao host sob a forma de comando AT (string ASCII) para o host processar a resposta e tomar alguma ação sobre a mesma. Se o comando CONNECT for enviado para o módulo com sucesso, o módulo entra em modo bypass, similarmente ao modem em modo de dados, e os dados podem ser trocados entre os dispositivos Bluetooth host e o dispositivo remoto. Uma seqüência de escape deve ser enviada pelo host ao módulo para que o mesmo retorne ao modo de comando.

Em aplicações embarcadas, os usuários são livres para desenvolver toda a parte superior da pilha e os perfis, assim como o programa aplicativo. Software/Firmware pode ser atualizado pela porta UART do modulo WBTV42.

Para conectar o modulo WBTV42 a porta UART do dispositivo host devem ser ligados de forma invertida os pinos de TX e RX, e RTS e CTS como ilustrado pela Figura 5.

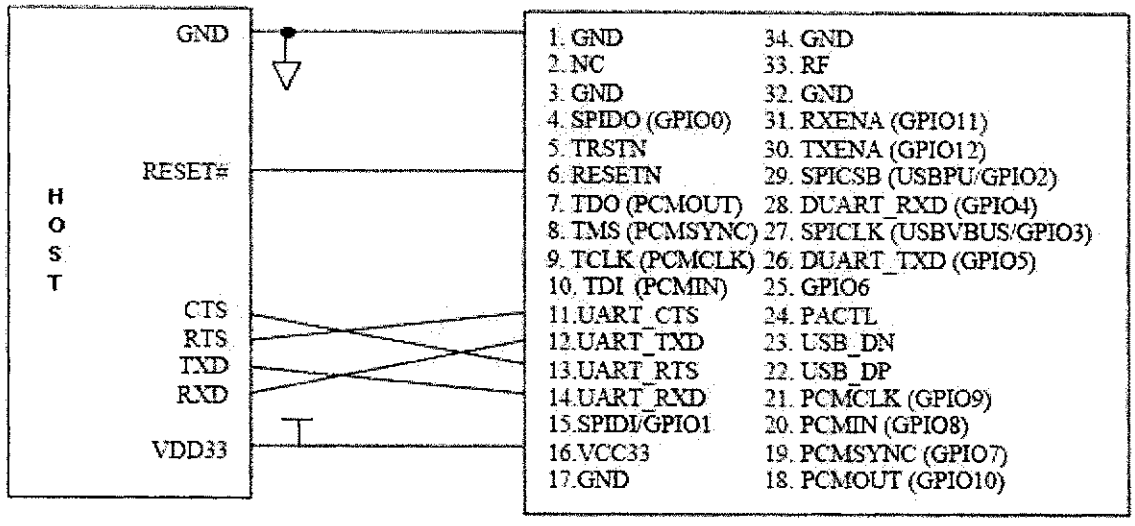

Figura 5 – Interface entre o modulo WBTV42 e o processador host

Na seção 4 serão explicadas em maiores detalhes as interfaces dos comandos entre o host e WBTV42-D-SPP.

3.7 Definição de pinos WBTV42-D-SPP

A Tabela 1 identifica e descreve os pinos do modulo Wintec WBTV42-D-SPP.

Nome	DIP Pin #	Descrição	Interface
RESETN	13	Reset Input (active low for 5 ms)	
UART_CTS	14	Clear To Send (pull-down, active low)	UART
UART_TXD	15	Transmit Data	UART
UART_RTS	9	Request to Send (active low)	UART
UART_RXD	16	Receive Data (pull-down)	UART
SPIDO (GPIO0)	1	SPI DataOut (weak internal pull-down)	SPI
SPIDI (GPIO1)	2	SPI Data In (weak internal pull-down)	SPI
SPICLK (GPIO3,USBVBUS)	10	SPI Clock (weak pull-down, active high)	SPI, USB
SPICSN (GPIO2, USBPU)	8	SPI Chip Select (weak internal pull-down)	SPI, USB
PCMOU T (GPIO10)	17	PCM Out	PCM
PCMIN (GPIO8)	18	PCM Input	PCM
PCMCLK (GPIO9)		PCM Clock	PCM
DUART_TXD (GPIO5)	19	Debug UART Transmit Data	Debug
DUART_RXD (GPIO4)	20	Debug Receive Data (Baseband activity LED)	Debug
NC		No Connect	
VCC33	12	Power 3.3V input	Power
GND	11	Ground	Ground

Tabela 1 –Descrição dos pinos WBTV42-D-SPP

3.8 Características Elétricas

A Tabela 2 define as características elétricas do modulo Wintec WBTV42-D-SPP.

Descrição	Min	Typ	Max	Unit
Storage Temperature	-40	-	+105	°C
Operating Temperature	0	25	70	°C
Supply Voltage VDD	3.0	3.3	3.6	V
RF Frequency	2400	-	2483.3	MHz
Low Level Input Voltage V_{IL}	-	-	0.8	V
High Level Input Voltage V_{IH}	2.0	-	-	V
Low Level Output Voltage V_{OL}	-	-	0.4	V
High Level Output Voltage V_{OH}	2.4	-	-	V
Low Level Output Current I_{OL}	-	-	-2.2	mA
High Level Output Current I_{OH}	-	-	3.1	mA
Input Leakage Current I_L	-1	-	+1	µA
Schmitt Trigger to High Threshold V_{T+}	1.47	-	1.50	V
Schmitt Trigger to Low Threshold V_{T-}	0.89	-	0.95	V
Pull-up Resistor R_{PU}	50	-	100	KΩ
Pull-down Resistor R_{PD}	40	-	100	KΩ
Input Capacitance C_I	-	-	7.5	pF
USB Differential Input Sensitivity V_{DI}	0.2	-	-	V
USB Differential Common Mode Range V_{CM}	0.8	-	2.5	V
USB Pull-up Resistor R_{PU}	1.425	1.5	1.575	KΩ
USB Pull-down Resistor R_{PD}	14.25	15	15.75	KΩ

Tabela 2 –Características elétricas (VDD=3,3V)

4. Interface de Comandos Wintec Bluetooth SPP

Nesta seção serão introduzidos os comandos básicos que permitem ao módulo Wintec Bluetooth SPP conectar-se com outro dispositivo que suporte o perfil de porta serial (SPP).

A vantagem da utilização do módulo Wintec Bluetooth é sua simples operação, basta o desenvolvedor conhecer a estrutura dos comandos AT para controle das operações que a mesma sintaxe é adotada para o modulo Wintec Bluetooth, com algumas diferenças que serão vistas no decorrer desta seção.

Em um PC, o software de comunicação Hyperterminal [2] é utilizado como ferramenta para envio de comandos AT, que serão convertidos em um conjunto de bits e enviados ao módulo por meio de uma porta serial.

O módulo Bluetooth responde ao comando AT enviado com um evento composto por uma string ASCII. Baseando neste evento de resposta, o host determina se a conexão com o Bluetooth remoto foi realizada com sucesso ou não.

Para estabelecimento de uma conexão Bluetooth com um outro dispositivo Bluetooth SPP, três comandos básicos são necessários: DISCOVERY, BOND e CONNECT.

4.1 Convenções de comandos e respostas [3]

Cada comando enviado para o módulo Bluetooth deve iniciar com a string "AT+ZV", e toda resposta do módulo ao host começará com a string "AT-ZV".

Comando: Determinado pela string ASCII enviada do host para o módulo. A mesma deverá ser terminada por um caractere de retorno de carro (0x0D).

Resposta: Determinado pela string ASCII enviada do módulo para o host. A mesma são terminadas por caracteres retorno de carro (0x0D) e nova linha (0x0A).

O usuário não precisa se preocupar se as strings enviadas devem ser com letras maiúsculas ou minúsculas, pois o módulo Wintec WBTV42-D-SPP não é sensível ao tipo enviado.

4.2 Inicialização do módulo Bluetooth

Quando o módulo Bluetooth é inicializado ou energizado, uma seqüência de quatro bytes nulos será enviada antes de começar a responder as mensagens enviadas pelo host, indicando prontidão do módulo para recepção de comandos. Abaixo seguem as respostas iniciais enviadas pelo módulo Bluetooth quando o mesmo é energizado.

AT–ZV –CommandMode–
AT–ZV BDAddress 000F7010205E

O endereço enviado como resposta pelo módulo corresponde ao endereço Bluetooth local do módulo, composto por 12 números hexadecimais equivalente a um número binário de 48 bits.

4.3 Estabelecendo uma conexão Bluetooth

A seqüência seguinte de comandos será utilizada no firmware do host para poder estabelecer a conexão Bluetooth entre o modulo Wintec e o dispositivo remoto que possua suporte ao perfil de porta serial, o que é valido no nosso caso devido ao dispositivo remoto Nokia 6600 suportar o perfil de porta serial.

Comando DISCOVERY: Quando o dispositivo Bluetooth estiver pronto para receber os comandos, o host pode enviar a seguinte mensagem para que o módulo Wintec possa procurar por dispositivos Bluetooth presentes no mesmo recinto.

AT+ZV Discovery All SPP False

As opções "All" e "SPP" requisitam ao módulo Bluetooth que o mesmo procure dispositivos com perfil de porta serial (SPP). A opção "False" requisita que o módulo pule a requisição de nomes dos serviços remotos para poder aumentar a velocidade do processo de procura por dispositivos.

O módulo Bluetooth irá responder ao comando enviado com as seguintes mensagens.

AT–ZV InqPending

Quando o processo de procura por dispositivos for terminado, a resposta enviada ao host será.

AT–ZV DiscoveryPending [number]

Onde "number" corresponde ao número de dispositivos descobertos. Depois de informado a quantidade de dispositivos descobertos, o WBTV42-D-SPP irá retornar a seguinte mensagem.

AT–ZV Device [BT Address] ["Name"] [Service Name]

Onde "BT Address" corresponde ao endereço do dispositivo Bluetooth remoto, seguido pelo "Name" que representa o nome do dispositivo remoto e "Service Name" representam os serviços que o dispositivo remoto suporta.

O procedimento de procura por dispositivos remotos no modulo Wintec duram aproximadamente 10 segundos, dependendo da quantidade de dispositivos descobertos.

Exemplo:

AT+ZV Discovery ALL SPP False
AT–ZV InqPending
AT–ZV DiscoveryPending 2
AT–ZV Device 000f70102005 "WINTEC Serial Port"
AT–ZV Device 00025b016b51 "ENG002PC"

A resposta ao comando DISCOVERY mostra que dois dispositivos Bluetooth foram descobertos, um foi o modulo "Wintec Serial Port" e o outro foi um PC com dispositivo bluetooth chamado "ENG002PC".

Comando BOND: O comando Bond é usado para emparelhamento com o dispositivo remoto o qual o host deseja conectar-se. O comando Bond é descrito pela seguinte sintaxe.

AT+ZV Bond [BT Address] [PIN code]

Onde o [PIN code] é o código de segurança requerido pelo dispositivo remoto para o processo de emparelhamento. Para a versão atual do módulo Wintec o código de segurança do mesmo é determinado pelo os 4 últimos dígitos do endereço Bluetooth do módulo. Caso o dispositivo remoto conheça o código, ele poderá realizar o processo de bond com o módulo Wintec.

Por exemplo, caso o módulo Wintec queira conectar-se a um dispositivo Bluetooth que possua o endereço dado por "000f70102028", então o host deverá enviar o seguinte comando para o modulo Wintec.

AT+ZV Bond 000f70102028 2028

O modulo Bluetooth SPP irá responder:

AT–ZV BondPending 00025b016b51

Se o comando Bond for realizado com sucesso, a resposta será.

AT–ZV BondOk

Senão a resposta enviada será.

AT–ZV BondFail

Após o emparelhamento entre o dispositivo remoto e o módulo Wintec, o host deve enviar o comando SPPConnect para estabelecer a conexão entres os dispositivos.

Comando SPPCONNECT: O comando para instalar a conexão Bluetooth entre o módulo Wintec e o dispositivo remoto emparelhado pelo comando bond anteriormente é.

AT+ZV SPPConnect [BT Address]

Caso o comando seja executado com sucesso, e resposta será.

AT–ZV ConnectionUp
AT–ZV –BypassMode–

Agora, dados podem ser trocados pelos dispositivos conectados como em um modem em modo de dados, a taxa de troca de dados é limitada pela interface UART em 115,2kbps.

Caso o comando SPPConnect não seja executado com sucesso, a resposta será.

AT–ZV SPPConnectionClosed

Dado que o módulo Wintec agora se encontra em modo de dados típico de um modem, para finalizar a conexão e voltar ao modo de comando, será necessário o envio de uma seqüência de escape pelo host ao modulo Wintec definida da seguinte maneira.

Seqüência de escape: Para voltar ao modo de comando, o host deve enviar a seqüência de escape ^#^$^% e manter o host por aproximadamente dois segundos sem enviar dado algum ao longo da conexão estabelecida. Caso a seqüência de escape seja enviada ao módulo e o tempo de espera respeitado pelo host, a confirmação da desconexão será enviada pelo modulo sob a seguinte forma.

AT–ZV –CommandMode-

Notar que após o modulo voltar ao modo de comando, para o host não recebe mais dado algum do dispositivo remoto, porém a conexão não foi ainda terminada, para terminar a mesma será necessário enviar o seguinte comando.

AT+ZV SPPDisconnect

E o módulo Bluetooth irá responder ao comando enviado da seguinte maneira.

AT–ZV SPPConnectinClosed
AT–ZV ConnectionDown

As respostas acima indicam que a conexão Bluetooth foi terminada.

5. Microcontrolador Microchip PIC 18XXXX

Tipicamente um microcontrolador se caracteriza por incorporar no mesmo encapsulamento um microprocessador, memória de programa e dados e vários periféricos como temporizadores, "*watchdog timers*", comunicação serial, conversores Analógico/Digital, geradores de PWM, entre outros periféricos, fazendo com que o hardware final fique extremamente complexo.

A *Microchip* é uma empresa precursora no uso de tecnologia *RISC* (*Reduced Instruction Set Computer*) em microcontroladores. Diferente da arquitetura Von Neumann, a estrutura *RISC* é baseada em barramentos independentes para dados e para programa, e tem como característica fundamental os tamanhos diferenciados, o barramento de programa é maior que o barramento de dados visando empacotar toda instrução em uma só palavra para fixar todas instruções com o mesmo tempo de execução.

A família 18XXXX de onde o microcontrolador utilizado neste trabalho se origina, é a opção que nos proporciona a maior relação custo benefício e características disponíveis dentre todas as famílias de microcontroladores da microchip. Dentre as principais características podemos destacar:

- Alta eficiência no uso de compiladores C.
- Arquitetura de alta performance (RISC).
- Alta capacidade de armazenamento de dados e programa.
- Grande quantidade de pinos de I/O.
- Flexibilidade para reprogramação.
- Microcontrolador líder em seu segmento na industria.

5.1 Microcontrolador PIC18F452 [4]

O microcontrolador PIC18F452 é um poderoso microcontrolador de 10MIPS (executa uma instrução em 100 nano segundos), fácil de programar (Devido arquitetura RISC, possui somente 77 instruções), memória CMOS-Flash de 8 bit, encapsulamento

PLLC, TQFP, DIP e SOIC com 40 – 44 pinos, compatível com dispositivos da família 12CXXXX, 16C5X, 16CXXX e 17CXX provendo caminhos simples para migração de código entres os dispositivos compatíveis e o PIC18F452.

O PIC18F452 foi desenvolvido para compatibilidade com os firmwares desenvolvidos em ambientes de desenvolvimento que utilizam a linguagem de programação C, possui como principais características:

- 256 bytes de EEPROM.
- Capacidade de reprogramação.
- Capacidade de debug in circuit.
- 2 PWM com 10 bit de resolução.
- 8 Canais de conversão Analógico/Digital (A/D).
- Porta serial síncrona configurável como porta SPI, ou I^2C.
- UART interna.
- Memória de programa com capacidade para 32kbytes (16384 instruções).
- Memória RAM com capacidade de 1,5kBytes.

O microcontrolador PIC18F42 será o núcleo do nosso sistema de segurança, pois o mesmo irá controlar o módulo Bluetooth, a memória E2PROM externa, o circuito de acionamento da porta e a interface do sistema de segurança com o usuário, recebendo requisições e processando as mesmas.

A Figura 6 ilustra o encapsulamento do microcontrolador PIC18F452 enquanto a Figura 7 ilustra o diagrama em blocos do PIC16F452.

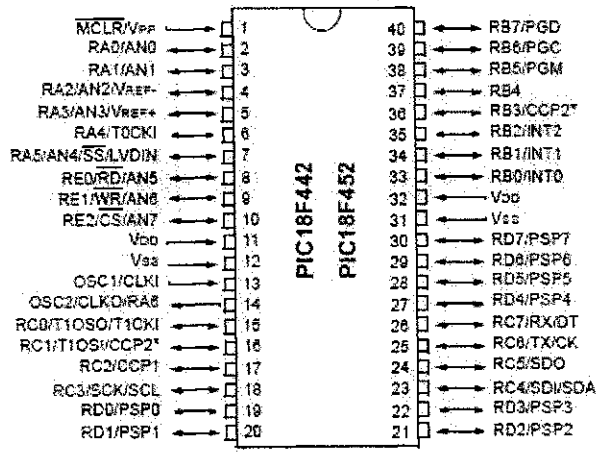

Figura 6 – Encapsulamento e pinagem do PIC18F452

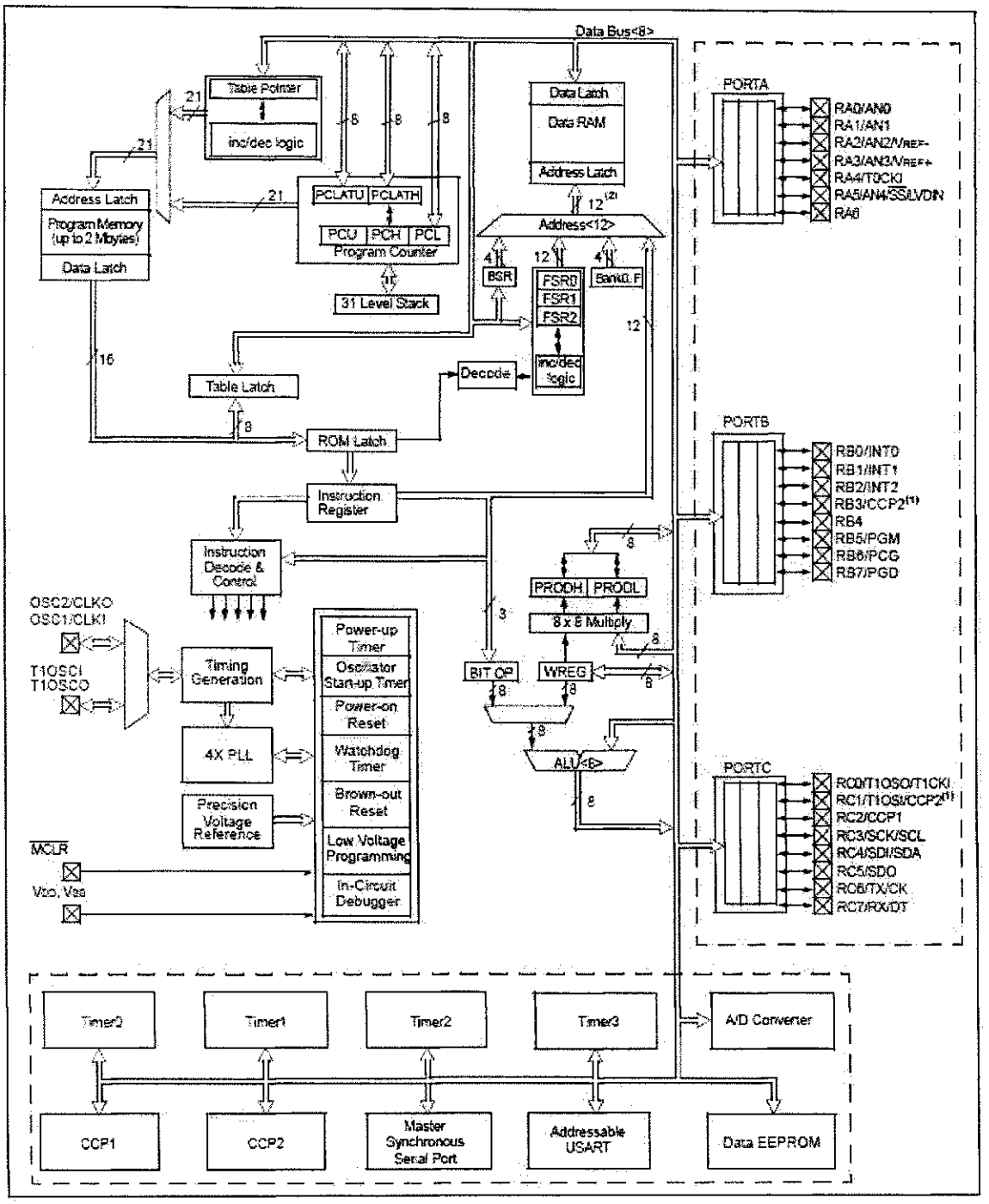

Figura 7 – Diagrama de blocos do PIC18F452

6. Memória Externa E^2PROM 24LC256 I^2C [5]

Devido à necessidade de armazenamento de um código único para cada usuário do sistema, o mesmo foi definido pela composição entre um nome do usuário contendo no máximo 48 caracteres e uma senha de no máximo 16 caracteres, totalizando 64 bytes por usuário. Devido à memória EEPROM do PIC18F452 ser bastante limitada neste aspecto, a solução encontrada foi utilização de uma memória E^2PROM externa 24LC256 da Microchip para armazenamento dos dados referentes aos usuários que terão acesso ao sistema.

A memória serial 24LC256 é uma memória do tipo PROM eletricamente apagável com capacidade de 256kbit (32k x 8bit) capaz de operar com tensões de 1,8 – 5,5V, e foi desenvolvida visando aplicações de aquisição de dados em sistemas com baixos consumos de potência.

A comunicação com o sistema host é realizada através da comunicação via protocolo I^2C, o ciclo de leitura dura aproximadamente 5ms, suporta 1000000 de ciclos de escrita/limpeza e retém os dados por aproximadamente 200 anos.

A máxima freqüência do clock suportada pela 24LC256 é de 400kHz e a memória é comercializada envolvida sob encapsulamentos de 8 pinos do tipo PDIP, SOIC, TSSOP, MSOP e DFN.

6.1 Organização dos dados na memória E^2PROM 24LC256

O código de identificação do usuário será composto por no máximo 64Bytes organizados na forma de no máximo 48Bytes para o login do usuário e 16Bytes para a senha do mesmo. Cada Byte do login e senha do usuário são compostos por caracteres ASCII, as strings de dados que representam o login ou senha do usuário, podem conter menos caracteres que o máximo caso a string seja terminada pelo caractere nulo (\0).

A Figura 8 representa a organização dos dados na memória E^2PROM 24LC256, devido à capacidade 32768 x 8bit da memória, obtemos a capacidade de armazenamento de 512 usuários no sistema de segurança eletrônico Bluetooth.

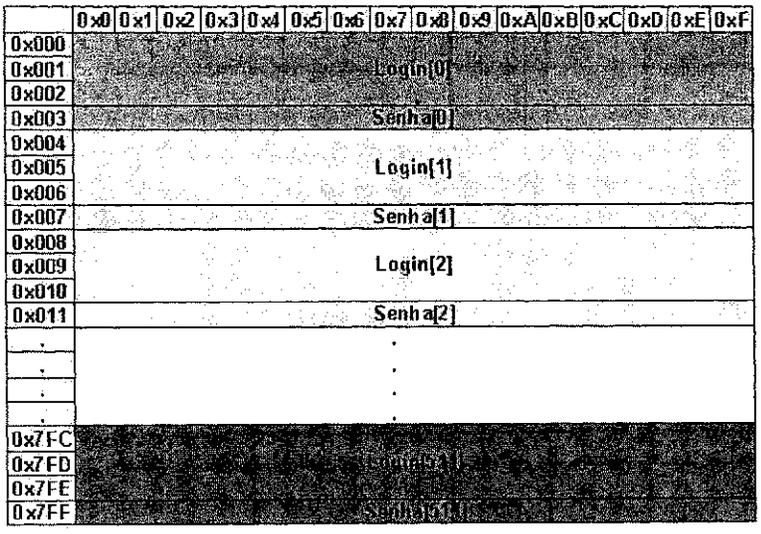

Figura 8 – Organização dos dados do usuário na memória E^2PROM 24LC256

7. Interface com o Usuário

O telefone inteligente Nokia modelo 6600 [6] foi o modelo utilizado como fonte para desenvolvimento da interface com o usuário do sistema de segurança eletrônica Bluetooth, os principais fatores que levaram a escolha do mesmo foram a sua disponibilidade em laboratório e suas características técnicas que atendem ao requisito do sistema, com memória interna de 7Mbytes e conectividade sem fio via tecnologia Bluetooth (SPP).

Devido ao conhecimento prévio da linguagem de programação Java 2 [7], foi utilizado o Nokia Java wireless toolkit [8] (conhecido formalmente como o conjunto de ferramentas de programação para dispositivos sem fio que utilizam a plataforma Java 2 micro edição – J2ME [9]), o qual possui as ferramentas ideais para desenvolvimento de aplicações para dispositivos móveis baseados do tipo MIDP (Perfil de dispositivo móvel de informação).

O conjunto de ferramentas inclui ambiente de simulação, características para otimização e ajuste de performance, documentação e exemplos para os desenvolvedores que precisam de rapidez na implementação de aplicações para dispositivos portáteis sem fio, porém a interface da plataforma de desenvolvimento é bastante rudimentar, foi então necessário à utilização da plataforma de desenvolvimento Eclipse [10] associado ao plugin EclipseME [11] e o wireless toolkit citado anteriormente no desenvolvimento do software que realiza a interface com o usuário em telefones inteligentes Nokia serie 60.

Para conexão Bluetooth os software desenvolvido baseia-se no código Benhui BlueLet [12], uma biblioteca de componentes que permitem de forma bastante simples a comunicação do Midlet desenvolvido anteriormente com dispositivos Bluetooth remotos.

A base da aplicação do telefone inteligente Nokia 6600 utiliza como base o exemplo referente ao estabelecimento de uma conexão Bluetooth cliente através do perfil de porta serial (SPP_Client) do código BlueLet.

A aplicação desenvolvida consiste inicialmente na definição das três frases de caracteres estáticas, uma contendo o nome do sistema de segurança Bluetooth a ser acessado (Wintec Serial Port), outra contendo o endereço do mesmo (000F70102060), e a última contendo o código de autenticação definido por três sub frases concatenadas definidas abaixo:

1. Código da operação (0 para acesso ao sistema, 1 para cadastro de login e 4 para limpeza dos dados cadastrados na memória);
2. Login do usuário seguido do caractere de retorno de carro '\r' (máximo 48 bytes);
3. Senha do usuário do caractere de retorno de carro '\r' (máximo 16 bytes).

Por exemplo, caso o usuário "Juliano" esteja cadastrado com senha "29051982" no sistema e deseje obter acesso ao mesmo, a frase de caracteres a enviar através da conexão Bluetooth SPP será: "0Juliano\r29051982\r". Após definição das variáveis citadas, o Midlet ao ser carregado executa a conexão Bluetooth com o sistema de segurança e envia o código de identificação do usuário para obter a permissão de acesso. Caso a conexão entre o telefone inteligente e o sistema de segurança não seja permitida, uma exceção será lançada e através do tratamento da mesma o processo de conexão é repetido, caso seja gerado novamente a exceção o aplicativo é finalizado e o acesso não permitido.

A Figura 9 ilustra o fluxograma do loop principal do J2ME SPP Midlet e da função que executa a conexão entre o telefone inteligente e o sistema de segurança eletrônica Bluetooth.

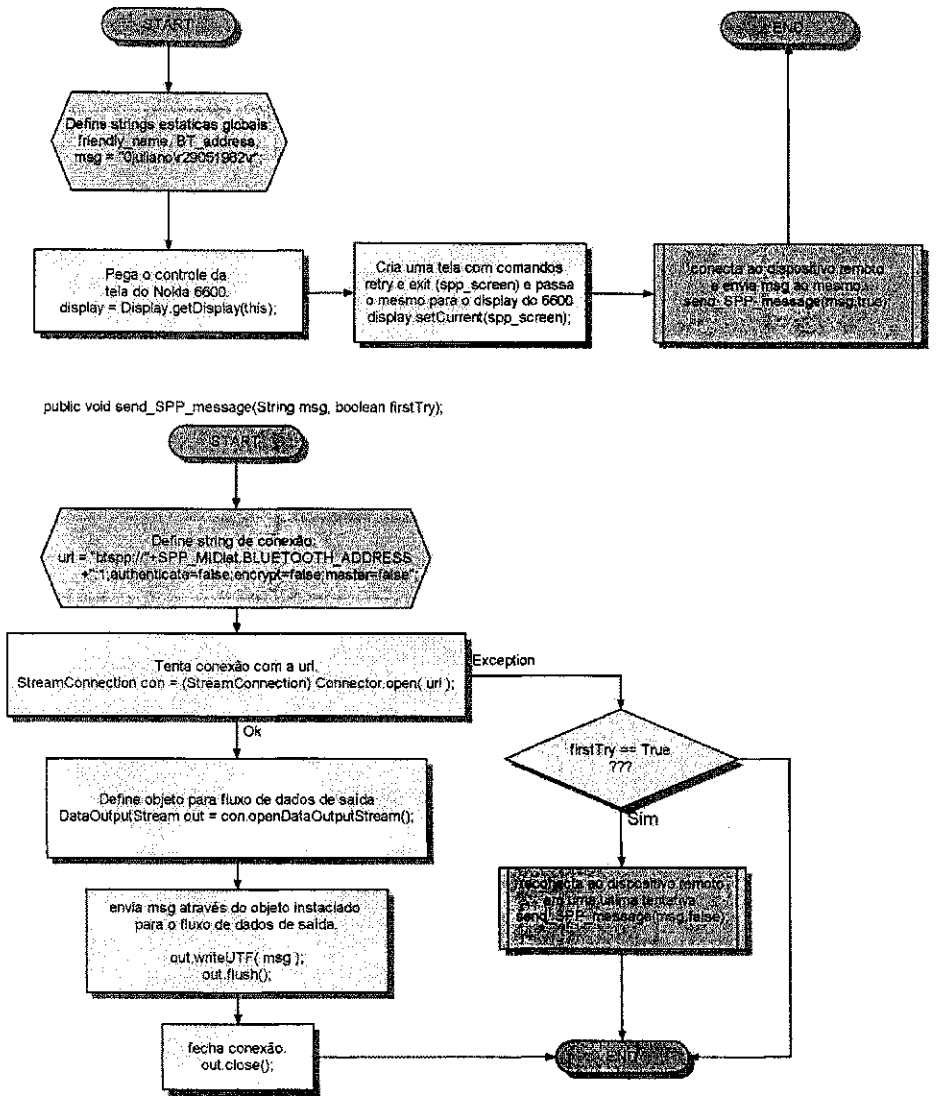

Figura 9 – Fluxograma do Midlet SPP J2ME que executa a conexão ao sistema de segurança e acesso ao sistema de segurança eletrônico Bluetooth

8. Sistema de Segurança Eletrônica Bluetooth

8.1 Descrição Geral do Sistema de Segurança Eletrônica Bluetooth

O sistema de segurança eletrônica Bluetooth é descrito pelo conjunto composto pelo modulo Bluetooth Wintec WBTV42-D-SPP, o núcleo de processamento representado pelo PIC18F452, a unidade de armazenamento de dados externa representada pela memória E2PROM 24LC256,o circuito de acionamento (drive de corrente para acionamento da tranca elétrica indutiva) e a interface da tranca elétrica representada pelos led's indicadores das operações.

8.2 Diagrama do Sistema de segurança eletrônica Bluetooth

A Figura 10 ilustra o diagrama do sistema de segurança eletrônica Bluetooth.

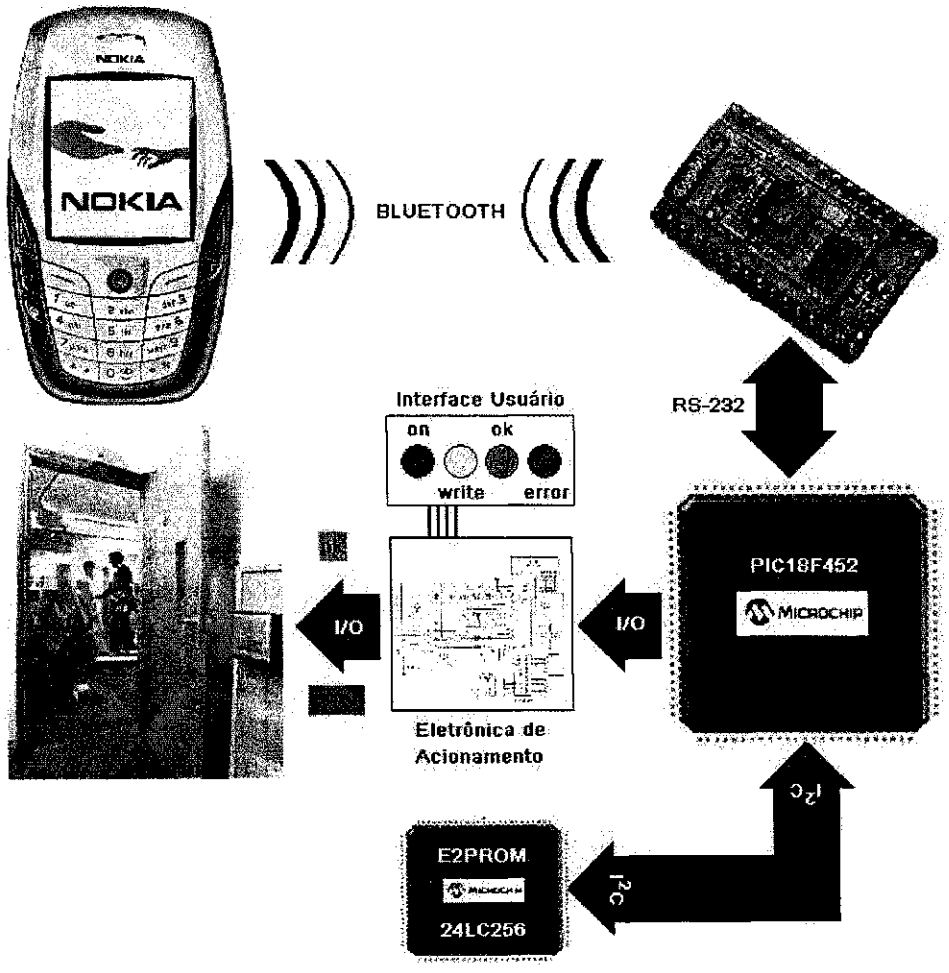

Figura 10 – Diagrama do sistema de segurança eletrônico Bluetooth

Baseado neste diagrama, os tópicos seguintes tratam as interfaces e os protocolos de comunicação utilizados entre cada par de dispositivos que compõem o sistema de segurança eletrônica Bluetooth.

Para explicação de todo o processo de autenticação do usuário, o caminho tomado partirá do dispositivo móvel celular ate o acionamento da tranca indutiva, o qual consiste do envio do código de autenticação do usuário através da conexão Bluetooth, que re-passa tal informação ao núcleo de processamento determinado pelo microcontrolador PIC18F452, que ao receber o código de autenticação executará a busca e comparação da chave de acesso na memória externa E^2PROM 24LC256, e ao obter o resultado envia a interface com o usuário o mesmo e aciona o dispositivo de liberação da tranca caso a chave de identificação do usuário seja válida.

As próximas seções detalham os protocolos utilizados em cada conexão juntamente com os processamentos realizados por cada dispositivo durante a duração da conexão estabelecida.

8.2.1 Nokia 6600 – WBTV42-D-SPP

O software embarcado no dispositivo móvel (baseado no código Bluelet – J2ME) possui todo o processo de negociação da conexão utilizando os protocolos (provenientes da pilha de protocolos Bluetooth) necessários para conexão via perfil de porta serial (SPP). O procedimento básico realizado para negociação da conexão, consiste na busca pelo módulo bluetooth remoto (Discovery) denominado pelo nome "Wintec Serial Port" ou pelo endereço Bluetooth especifico do mesmo, emparelhamento através do envio do código de autenticação da conexão do dispositivo móvel ao módulo Bluetooth (Bond), e finalmente o estabelecimento da conexão (Connect) que baseado no perfil de porta serial, emula na conexão sem fio uma porta serial UART com controle de fluxo por hardware (CTS/RTS) entre o módulo Bluetooth e o dispositivo móvel, não é necessária atenção sobre o controle de fluxo devido ao mesmo ser realizado de forma automática através dos métodos SPP do código do Bluelet utilizado no sistema embarcado e pela pilha de protocolos Bluetooth embarcada no módulo Bluetooth WBTV42-D-SPP.

Depois de estabelecida a conexão Bluetooth entre o dispositivo móvel celular Nokia 6600 e o módulo Bluetooth WBTV42-D-SPP, o sistema de segurança aguarda a

chave de identificação do dispositivo que está armazenada no mesmo, sendo enviada após determinação do usuário o qual opera o dispositivo móvel. O código de identificação é cadastrado uma única vez pelo usuário do dispositivo móvel, através do sistema de armazenamento de dados persistente do mesmo, facilitando ao usuário com auxilio apenas uma tecla enviar o seu código de identificação ao sistema de segurança eletrônica Bluetooth que processará o mesmo respondendo com a liberação da tranca em caso de chave válida.

O dispositivo móvel celular pode finalizar a conexão a qualquer momento que o usuário desejar, já do lado do módulo Wintec WBTV42-D-SPP, a desconexão só poderá ser realizada pelo sistema host o qual controla o módulo, que neste caso é o microcontrolador PIC18F452, assunto tratado na próxima seção.

8.2.2 WBTV42-D-SPP – PIC18F452

O módulo WBT42 se comunica com o microcontrolador host através de uma conexão serial (UART) com controle de fluxo por hardware (CTS/RTS). O controle de fluxo por hardware é assim denominado devido à necessidade pinos adicionais (além dos pinos de transmissão e recepção de dados) do hardware para funcionamento do mesmo, trabalhando como um método de sinalização entre os dispositivos que realizam a comunicação visando a manutenção de sincronismo para recepção e envio das mensagens AT.

No sistema de segurança eletrônica Bluetooth o CTS do WBTV42 é conectado ao RTS do sistema host e virce–versa.

Na recepção de dados, o sinal RTS indica que o dispositivo que o ativou está pronto para receber informações, ao receber-las, desativa o RTS para executar o processamento e torna a ativar o RTS quando estiver pronto para recepção de novas informações.

Na transmissão de dados, o dispositivo que desejar efetuar tal ação, deve previamente realizar o monitoramento do seu pino de CTS, e só enviar dados quando o mesmo estiver ativado (indicando a permissão para envio dos dados), a cada dado enviado o sistema deverá realizar uma nova monitoração do sinal CTS antes de um novo envio de informação.

Durante o procedimento de estabelecimento da conexão entre o dispositivo móvel celular e o módulo WBTV42, mensagens AT em formato ASCII são enviadas ao PIC18F452 como resposta a cada passo do procedimento de estabelecimento da conexão realizado entre o módulo e o dispositivo móvel celular, o firmware do PIC18F452 monitora estas mensagens aguardando a mensagem final de estabelecimento da conexão com dispositivo Bluetooth remoto, então o firmware prossegue aguardando o código de autenticação a ser enviado pelo dispositivo móvel, ao receber tal código, analisa o mesmo e caso esteja cadastrado em seu banco de dados, responde com a liberação da tranca. Após troca de dados realizada entre os dispositivos, o firmware do PIC18F452 trata enviar a seqüência de escape para chaveamento para o modo de comando do módulo e conseqüentemente enviando os comandos AT necessários para finalização da conexão bluetooth entre os dispositivos.

Os fluxogramas do firmware do PIC18F452 mostram de maneira mais clara o funcionamento da inicialização, finalização da conexão Bluetooth e aquisição do código do usuário através da conexão Bluetooth estabelecida entre o dispositivo remoto e o sistema de segurança eletrônica Bluetooth.

8.2.2 PIC18F452 – 24LC256

O protocolo I^2C ou "two wire protocol" é um protocolo voltado para simplificação da comunicação digital a dois fios que utiliza somente uma linha de dados (SDA) e uma linha de clock (SCL). Para que um sistema funcione corretamente alguns protocolos bem definidos devem ser obedecidos, como os sinais de start, stop e endereçamento. Os sitemas que utilizam comunicação I^2C utilizam arquitetura mestre/escravo, ou seja, o dispositivo mestre controla o envio/recebimento das informações com relação aos dispositivos escravos que apenas respondem aos comandos do mestre que geralmente é um microcontrolador ou microprocessador. A velocidade do sistema é determinada pela freqüência do sinal de clock (SCL) que é controlado pelo dispositivo mestre (geralmente o processador).

A memória externa 24LC256 é utilizada como dispositivo de armazenamento persistente de dados no sistema de segurança eletrônico Bluetooth devido capacidade reduzida da memória EEPROM disponibilizada internamente pelo microcontrolador PIC18F452. Para comunicação I^2C entre o microcontrolador e a memória, o compilador

CCS PICC possui a biblioteca de comunicação embutida para a memória 24LC256, possuindo então as funções de escrita e leitura necessárias para comunicação entre o microcontrolador PIC18F452 e a memória EEPROM 24LC256.

A organização dos dados na memória foi discutida no tópico 6 deste mesmo trabalho e o mapa da memória foi ilustrado pela Figura 8, foi necessário definir tal organização dos dados na memória para definir funções de busca otimizada pelos códigos de identificação do usuário armazenados na memória 24LC256 e não procurar sempre por toda memória byte a byte a informação requerida.

Um apontador para posição livre de memória foi utilizado para indicar a partir de qual posição de memória temos espaço livre para gravação de novos códigos de usuários (ou indicar até qual ponto da memória temos dados gravados), indicando conseqüentemente o fim de espaço para armazenamento caso o ponteiro seja igual à posição final da memória.

O método de gravação do código de autenticação do usuário começa a partir da recepção do comando que indica gravação do mesmo, a informação de login e senha que procede ao comando é adquirida e armazenada na memória 24LC256 a partir da posição livre indicada pelo ponteiro de posição livre, caso o ponteiro possua o valor da posição final de memória um código de erro será enviado para interface, senão o código será armazenado e o ponteiro será incrementado no valor de $0x0040_{hex}$ (tamanho total de um login mais o tamanho total de uma senha) para apontar para nova posição livre para armazenamento de novos códigos.

O método de busca do código de autenticação do usuário começa a partir da recepção do comando que indica a requisição de acesso pelo dispositivo móvel, a informação de login e senha que procede ao comando é adquirida e armazenada em vetores na memória RAM do PIC18F452, para uma busca otimizada, é comparada o primeiro caractere ASCII do login adquirido com o primeiro caractere de cada código de autenticação do usuário gravado na memória 24LC256 (evitando executar leitura byte a byte de toda a memória) que ao ser validado, comprara o restante dos caracteres deste código armazenado com o código adquirido, caso o login e senha sejam validados antes de o ponteiro de leitura tenha atingido o valor apontado pelo ponteiro de posição livre, o acesso é validado, caso não a operação não será bem sucedida e a tranca não será acionada.

A Figura 11 ilustra a validação de um código de usuário representado pelo login "Juliano Rodrigues Fernandes de Oliveira" mais o caractere nulo "\0" (terminador de

strings) e senha "29051982" mais o caractere nulo "\0", os caracteres em negrito representam os caracteres lidos a partir da memória externa 24LC256 e comparados ao código recebido, e como explicado anteriormente, caso um caractere comparado com o código recebido retorne erro de comparação, o ponteiro de comparação move-se para o próximo bloco de código de usuário e a comparação recomeça, quando um código completo consegue ser comparado com sucesso antes que o ponteiro atinga a posição do ponteiro de espaço livre temos a validação do código recebido, senão temos um código de autenticação incorreto e a permissão de acesso é negada.

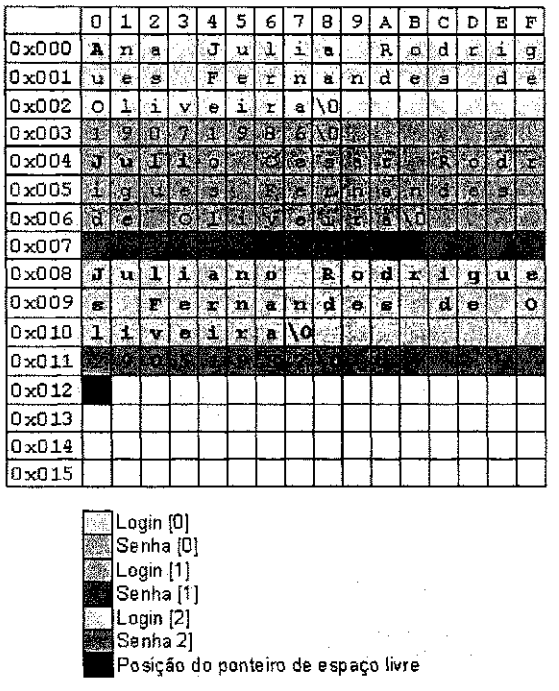

Figura 11 – Sistema de busca para identificação do código do usuário.

Os fluxogramas do firmware do PIC18F452 mostram de maneira mais clara o funcionamento das funções de busca, comparação e validação do código do usuário adquirido do dispositivo remoto.

8.2.3 PIC18F452 – Interface Local (Tranca Eletrônica)

A interface local é representada pelo painel de interface com o usuário e o circuito de acionamento da tranca indutiva.

O painel de interface é composto por quatro Leds que informam o status do circuito ao usuário, o Led azul acionado indica que o circuito se encontra energizado e

operante, o Led amarelo acionado indica que a operação que está sendo realizada entre o usuário e o sistema de segurança é uma operação de gravação de um novo código de identificação de usuário, o Led verde acionado indica que a operação de identificação do código de identificação de usuário foi realizada com sucesso e libera a tranca indutiva permitindo acesso ao usuário, o Led vermelho acionado indica que a operação de identificação do código de identificação de usuário foi realizada sem sucesso (código de identificação invalido) e a tranca indutiva não é liberada e o acesso ao usuário não é permitido.

Quando o código do usuário é validado a tranca indutiva deve ser acionada porém, os pinos de entrada e saída do microcontrolador não fornecem a quantidade de corrente necessária para a tranca indutiva e nem a tensão de 5V do sistema de segurança é compatível com a tensão de alimentação da tranca (12V), para resolução deste problema foi implementado um circuito de acionamento da tranca indutiva que consiste simplesmente em um drive de corrente definido por um transistor em configuração emissor comum com um resistor limitador de corrente na base que está ligado ao pino de entrada e saída do microcontrolador e a tranca indutiva que está conectada entre o terminal da fonte de alimentação de 12V CC e o coletor do transistor, como o terminal terra da fonte de 12V está conectado ao emissor (junto com o terminal terra da fonte de 5V do microcontrolador). Caso o pino de entrada e saída do microcontrolador conectado ao resistor limitador de corrente esteja ativo (5V), a corrente irá percorrer a junção base-emissor saturando o transistor e conseqüentemente tornando a tensão de coletor para emissor igual a zero, conseqüentemente conectando o pino terra do emissor ao coletor e alimentando a tranca com tensão e corrente necessárias para ativação sem prejudicar o pino de entrada e saída do microcontrolador.

8.3 Fluxogramas do Software Embarcado PIC18F452

O fluxograma representado pela Figura 12 explica graficamente os passos executados pelo loop principal do firmware do sistema de segurança eletrônica Bluetooth, que após realizar chamadas às funções de inicialização da conexão Bluetooth recebe uma seqüência de dois bytes nulos (enviados pelo dispositivo móvel celular Nokia 6600 ao iniciar uma conexão Bluetooth) e logo em seguida recebe o código da operação seguido do código de autenticação do dispositivo remoto, então o sistema de

segurança realiza a ação definida pelo código da operação recebido sobre o código de autenticação do usuário recebido, que podem ser as ações de cadastro de código ou identificação do mesmo. Ao terminar o processamento o sistema de segurança Bluetooth libera ou não a tranca, dependendo do resultado do processamento do código de autenticação, finaliza a conexão Bluetooth com o dispositivo remoto aguarda uma nova conexão Bluetooth ser iniciada por um dispositivo remoto.

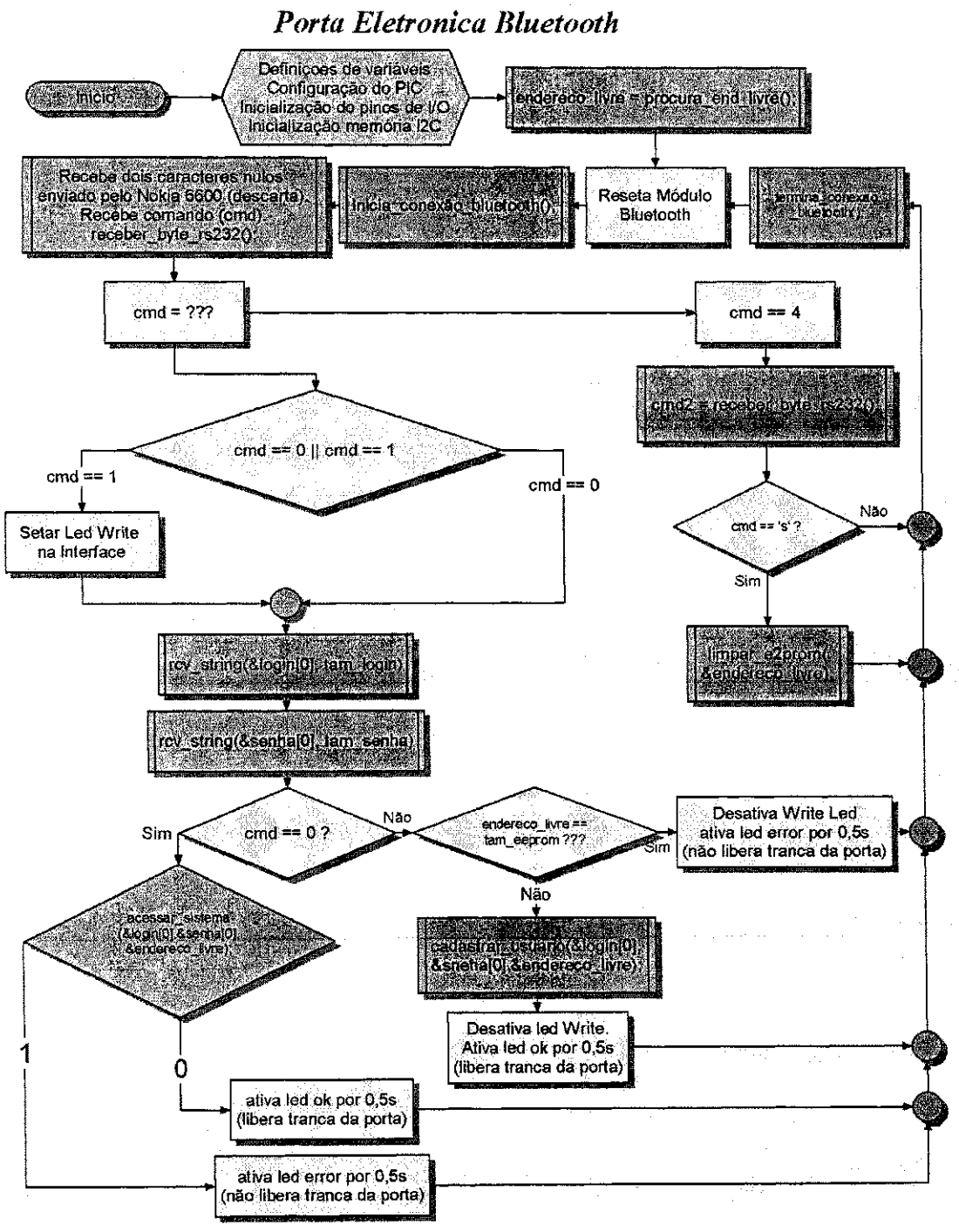

Figura 12 – Fluxograma do loop principal do firmware PIC18F452

Os fluxogramas ilustrados pelas Figuras 13-15 explicam graficamente as sub-rotinas utilizadas pelo loop principal do firmware do PIC18F452, o núcleo de processamento do sistema de segurança Bluetooth

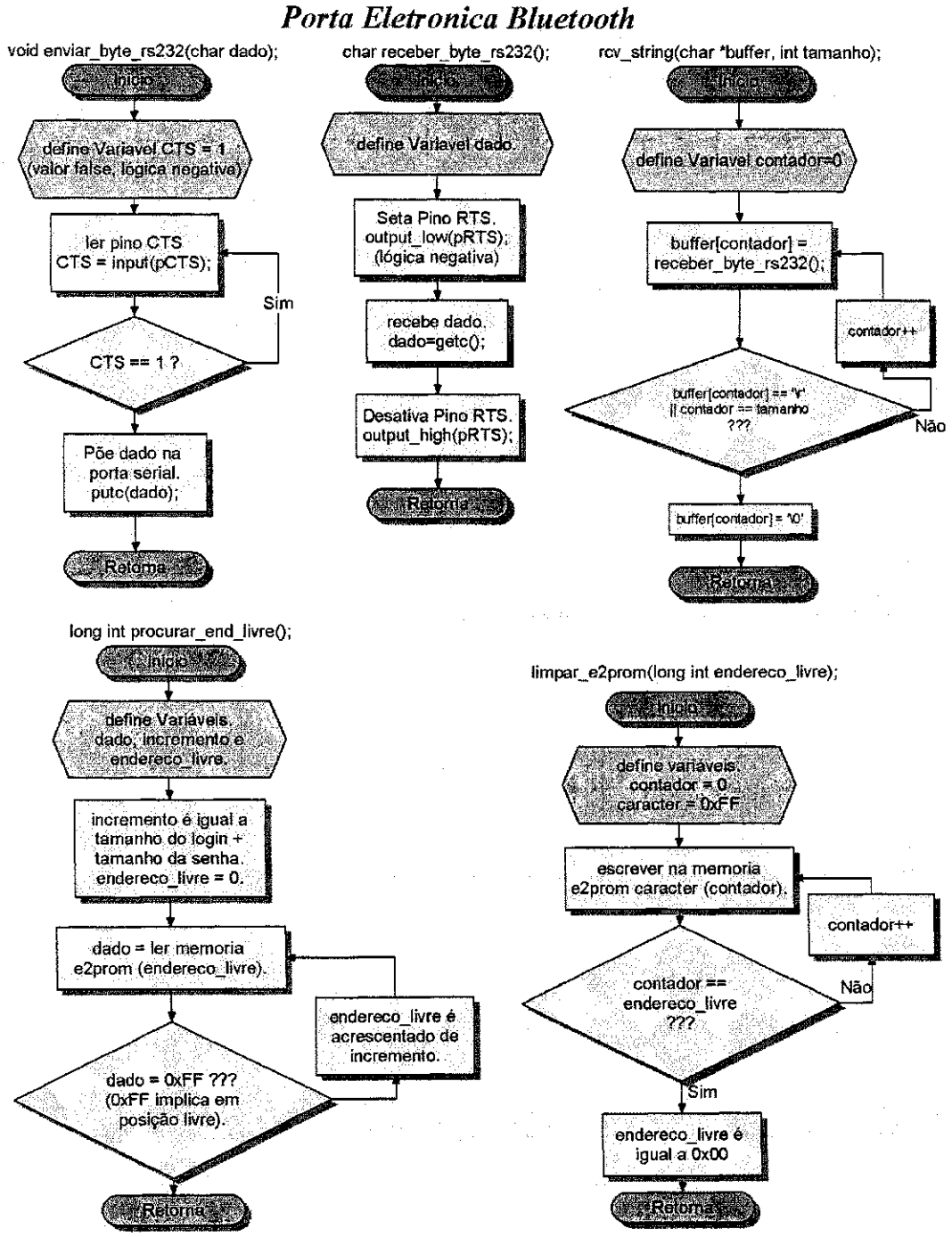

Figura 13 – Fluxograma das sub-rotinas para recepção de caracteres e strings através da conexão serial com o WBTV42 e sub-rotinas de limpeza da memória externa 24LC256 e determinação do ponteiro de espaço livre

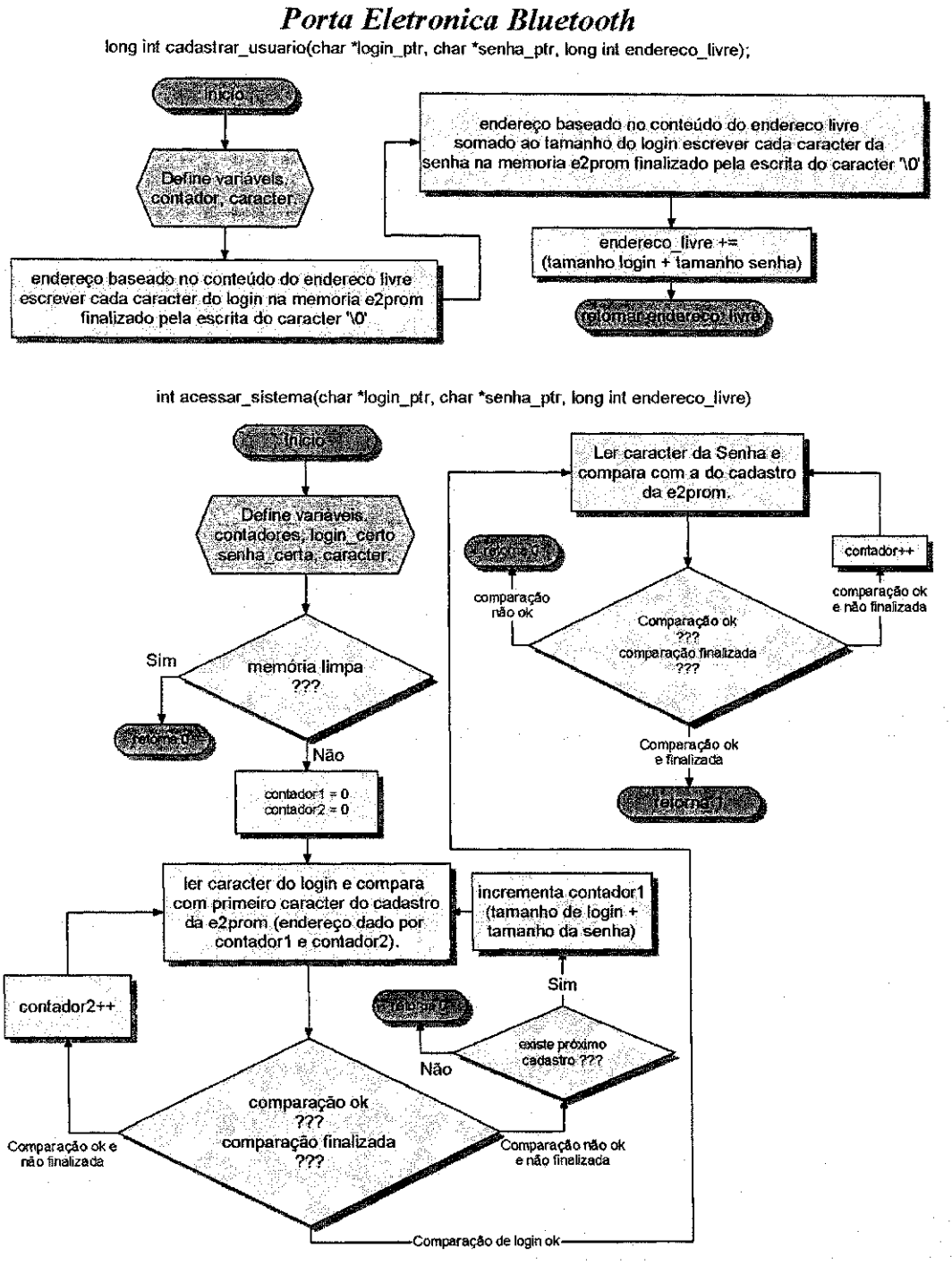

Figura 14 – Fluxograma das sub-rotinas para comparação e cadastro do código de autenticação comunicando-se com a memória 24LC256.

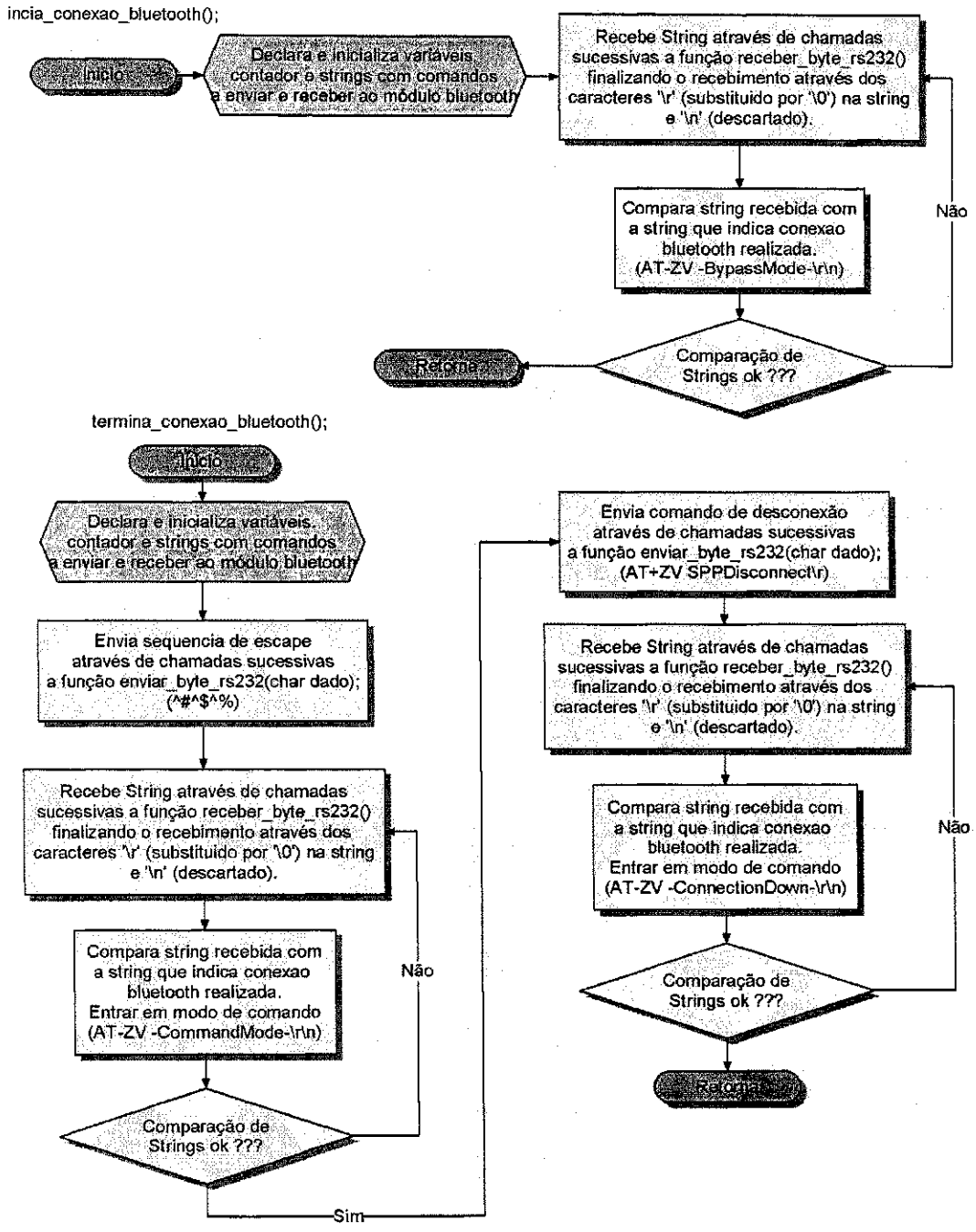

Figura 15 – Fluxograma das sub-rotinas para inicialização e finalização das conexões Bluetooth com o dispositivo remoto

8.4 Diagrama esquemático do sistema de segurança eletrônico Bluetooth

A Figura 16 ilustra o diagrama esquemático do circuito implementado para a tranca eletrônica bluetooth.

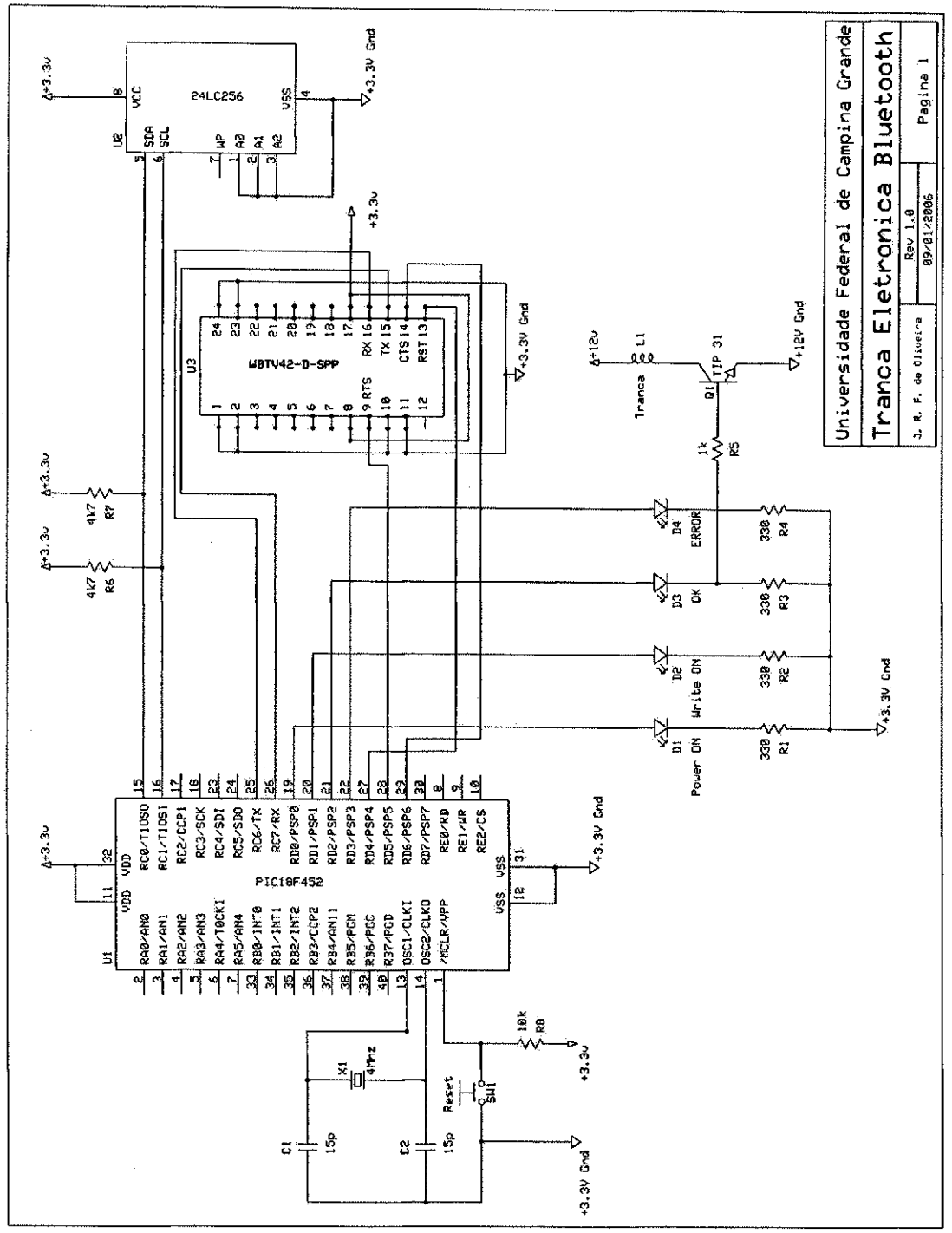

Figura 16 – Diagrama esquemático do sistema de segurança eletrônico Bluetooth

9. Conclusões

Foi desenvolvida com sucesso a primeira versão do sistema de segurança eletrônico Bluetooth.

Revisões do *firmware* serão necessárias futuramente para agregarem maior segurança às trocas de dados entre o dispositivo remoto e o sistema de segurança eletrônico Bluetooth através desenvolvimento de novas sub-rotinas para autenticação de usuário administrador (que deverá ser realizado antes do cadastramento de novos códigos de autenticação), remoção de somente um código de autenticação especificado e envio de dados referentes aos códigos de autenticação cadastrados na memória externa 24LC256.

O desenvolvimento do sistema de segurança Bluetooth proporcionou uma excelente oportunidade de aprofundar e consolidar os conhecimentos na área de desenvolvimento de sistemas embarcados.

A oportunidade do desenvolvimento deste trabalho de conclusão de curso no laboratório de sistemas embarcados da UFCG criou um ambiente de trabalho favorável que implicou em um tranqüilo andamento das atividades, de tal forma que a conclusão das mesmas esteve de acordo com os cronogramas estabelecidos no inicio das atividades.

10. Referências Bibliográficas

[1] *WBTV42-D-XXX Bluetooth Module Rev 0.8*, Wintec Industries– 24/03/2005.

[2] MICROSOFT. *Microsoft HyperTerminal ver. 5.1*. Microsoft Corporation – 2001.

[3] *Wintec Bluetooth SPP Command Interface Quick Start Guide,* Wintec Industries – 08/12/2004.

[4] *Microchip PIC18FXX2 Datasheet*. Microchip Technology – 2002.

[5] *Microchip 24LC256 256k I^2C CMOS Serial EEPROM Datasheet*. Microchip Technology – 2002.

[6] Nokia 6600 – http://www.nokiausa.com/phones/6600 - 20/01/2006

[7] J2SE – http://java.sun.com/j2se/ - 20/01/2006

[8] Sun Java Wireless Toolkit – http://java.sun.com/products/sjwtoolkit/download-2_2.html - 20/01/2006

[9] J2ME – http://java.sun.com/j2me/index.jsp - 20/01/2006

[10] Eclipse – http://www.eclipse.org/ - 20/01/2006

[11] Eclipse ME – http://eclipseme.org/ - 20/01/2006

[12] Benhui Bluelet – http://benhui.net/modules.php?name=Bluetooth&page=bluelet.html - 20/01/2006

[13] Ericsson Bluetooth – http://www.ericsson.com.br/bluetooth/index.asp - 07/02/2006