

**FELIPE GIUNTE YOSHIDA
MARIANA RAMOS FRANCO
VINICIUS TOSTA RIBEIRO**

**MICROKERNEL PARA A PLACA ARM
EVALUATOR-7T**

Monografia apresentada à Escola
Politécnica da Universidade de São
Paulo para a Conclusão do Curso de
Engenharia da Computação.

São Paulo
2009

**FELIPE GIUNTE YOSHIDA
MARIANA RAMOS FRANCO
VINICIUS TOSTA RIBEIRO**

**MICROKERNEL PARA A PLACA ARM
EVALUATOR-7T**

Monografia apresentada à Escola
Politécnica da Universidade de São
Paulo para a Conclusão do Curso de
Engenharia da Computação.

Orientador:
Prof. Dr. Jorge Kinoshita

São Paulo
2009

DEDICATÓRIA

Aos meus pais, Noboru e Sonia, que me apoiaram e possibilitaram que chegasse até aqui.

Aos meus avós, por todo o suporte e carinho, essenciais para percorrer esta longa jornada.

E aos meus mestres, que me guiaram ao longo do caminho.

-Felipe Giunte Yoshida

Aos meus pais, Edson e Waldinéia, por sempre me apoiarem e me guiarem nas decisões importantes que me levaram até aqui.

E aos meus irmãos, Vinicius e Fernando, pelo carinho e amizade que nos une.

-Mariana Ramos Franco

À toda minha família, por todo seu amor e apoio incondicionais durante toda a minha vida.

E a todos os meus amigos politécnicos, que colaboraram para que toda essa jornada valesse a pena.

-Vinicius Tosta Ribeiro

AGRADECIMENTOS

Ao Professor Jorge Kinoshita, pelo incentivo, orientação e disposição em todos os momentos durante o projeto.

A Escola Politécnica da Universidade de São Paulo, que nos deu a oportunidade de aprendizagem e crescimento.

Ao Departamento de Engenharia de Computação e Sistemas Digitais (PCS), pelo Curso Cooperativo de Engenharia da Computação.

RESUMO

O uso de dispositivos móveis como celulares, *smartphones*, tocadores de MP3 e *video-games* portáteis é cada vez mais comum. A atual líder no segmento de processadores de baixa potência, essencial nestes tipos de aparelhos, é a empresa inglesa ARM. À fim de se modernizar o equipamento usado em aulas, ela disponibilizou à Escola Politécnica algumas placas ARM Evaluator 7-T, cujo processador, o ARM7TDMI, é usado em eletrônicos muito populares atualmente, como o Apple iPod e o Nintendo DS.

Assim, utilizando-se desse hardware mais moderno e pensando em aproximar o ensino das disciplinas de Sistemas Operacionais e do Laboratório de Microprocessadores, este projeto visa o desenvolvimento de um *microkernel* para a placa ARM Evaluator-7T, tema que engloba conhecimento de ambas as disciplinas.

O *microkernel* desenvolvido, chamado de KinOS, é provido de algumas funções básicas, e é apenas o primeiro passo para um projeto muito maior, de desenvolvimento de um sistema operacional totalmente feito por alunos da Escola Politécnica.

Dentre as funções básicas deste *microkernel*, podemos citar o chaveamento de *threads*, algumas chamadas de sistema (*fork*, *exec* e *exit*), funções para manipulação de periféricos e comunicação através de um terminal.

ABSTRACT

Mobile devices such as smartphones, MP3 players and portable video-games are becoming ubiquitous. Low power processors are essential in this market, where the English company ARM is the leader. In order to upgrade the equipment being used in the classes, ARM provided a set of ARM Evaluator 7-T boards to the Escola Politécnica. It has the ARM7TDMI processor, which is used in popular devices such as the Apple iPod and the Nintendo DS.

Using this updated hardware and willing to unite the Operating Systems and Microprocessors Laboratory courses, this project aims the development of a microkernel for the ARM Evaluator 7-T board, which would encompass both courses.

The microkernel, named KinOS, has some basic functions. It is the first step towards a bigger project, the development of a operating system totally created by the Escola Politécnica students.

The functions encompassed by this microkernel include the thread switching, some system calls (fork, exec and exit), functions for peripheral manipulation, and shell communication.

LISTA DE FIGURAS

2.1	<i>Pipeline</i> de 3 estágios (ARM LIMITED, 2001b)	22
2.2	<i>Pipeline</i> do ARM7TDMI (RYZHYK, 2006)	23
2.3	Organização dos registradores no modo ARM (ARM LIMITED, 2001b)	26
2.4	Formato dos registradores de estado CPSR e SPSR (ARM LIMITED, 2001b)	28
2.5	Esquema de uma interrupção no ARM7TDMI (ZAITSEFF, 2003)	32
2.6	Passagem de argumentos (SLOSS; SYMES; WRIGHT, 2004)	36
2.7	Arquitetura da placa Evaluator-7T. (ARM LIMITED, 2000)	37
2.8	Editor de linha de comando do BSL via HyperTerminal	39
2.9	Screenshot da IDE CodeWarrior	43
2.10	Screenshot do AXD Debugger	44
3.1	Estrutura de arquivos.	46
3.2	Estrutura de dados do PCB. Fonte: (SLOSS, 2001)	49
3.3	Vetor de <i>threads</i>	49
3.4	Estrutura da memória. Fonte: (SLOSS, 2001)	50
3.5	Fluxograma de inicialização.	52
3.6	Encadeamento de interrupções. Fonte: (SLOSS, 2001)	56
3.7	Chaveamento de <i>threads</i>	57
3.8	Fluxo de funcionamento do fork.	64
3.9	Comunicação da Evaluator-7T em cada porta serial.	69

LISTA DE TABELAS

2.1	Modos de operação (ARM LIMITED, 2005)	25
2.2	Valores para o bit de modo (ARM LIMITED, 2005)	30
2.3	Vetor de interrupção (ARM LIMITED, 2005)	31
2.4	Ordem de prioridade das interrupções (ARM LIMITED, 2001b)	31
2.5	Mapa da memória flash (ARM LIMITED, 2000)	38
3.1	Registradores mapeados em memória da UART0 (SAMSUNG ELECTRONICS, 2007)	69
3.2	Registradores mapeados em memória da UART0 (SAMSUNG ELECTRONICS, 2007)	70

LISTA DE ABREVIATURAS

ADS ARM Developer Suite

ALU Arithmetic Logic Unit

ARM Advanced RISC Machine

AXD ARM eXtended Debugger

CISC Complex Instruction Set Computer

CPSR Current Program Status Register

FIQ Fast Interrupt

IDE Integrated Development Environment

IRQ Interrupt Request

LR Link Register

PC Program Counter

PSR Program Status Register

RISC Reduced Instruction Set Computer

SP Stack Pointer

SPRS Saved Program Register

SWI Software Interruption

USP Universidade de São Paulo

LISTA DE SÍMBOLOS

RX - registrador número X

RX_Y - registrador número X do modo de operação Y

SUMÁRIO

1	Introdução	17
1.1	Objetivo	17
1.2	Motivação	17
1.3	Justificativa	18
1.4	Metodologia de Trabalho	18
1.5	Organização do Documento	19
2	Conceitos e Tecnologias Envolvidas	21
2.1	O Processador ARM7TDMI	21
2.1.1	Arquitetura RISC	21
2.1.2	Pipeline	22
2.1.3	Estados de Operação	24
2.1.4	Modos de Operação	24
2.1.5	Registradores	25
2.1.6	Registradores de Estado	27
2.1.7	Interrupções	30
2.1.8	Programando em C pra o ARM7TDMI	35
2.2	A Placa Experimental Evaluator-7T	36
2.2.1	Bootstrap Loader	38
2.2.2	Angel Debug Monitor	41
2.3	O ambiente de desenvolvimento	42
2.3.1	CodeWarrior	42

2.3.2	AXD Debugger	43
3	O Sistema Operacional KinOS	45
3.1	Organização do código	45
3.1.1	Raiz	46
3.1.2	Pasta "apps"	47
3.1.3	Pasta "interrupt"	47
3.1.4	Pasta "peripherals"	47
3.1.5	Pasta "syscalls"	47
3.1.6	Pasta "mutex"	47
3.2	Estruturas de dados	48
3.2.1	Process Control Block	48
3.2.2	Vetor de <i>threads</i>	48
3.3	Configuração de <i>hardware</i> e <i>software</i>	49
3.3.1	Memória	49
3.3.2	Modos do processador	50
3.3.3	Modos de teste	51
3.3.4	Angel	51
3.4	Inicialização	52
3.4.1	Ponto de entrada e tipo de código	52
3.4.2	Pilhas	53
3.4.3	Vetor de <i>threads</i> e número da <i>thread</i>	53
3.4.4	Periféricos	54
3.4.5	Instalação do tratamento de interrupção	54
3.4.6	Interrupção de <i>timer</i>	56
3.4.7	Habilitando interrupções	56
3.5	Chaveamento de <i>threads</i>	57

3.5.1	Identificação da interrupção	57
3.5.2	Limpeza da interrupção de <i>timer</i>	58
3.5.3	Identificação da próxima <i>thread</i>	59
3.5.4	Localização dos PCBs	59
3.5.5	A troca de <i>threads</i>	60
3.5.6	Retorno à execução da nova rotina	62
3.6	Chamadas de sistema	62
3.6.1	Propriedades gerais	62
3.6.2	<code>fork</code>	64
3.6.3	<code>exec</code>	66
3.6.4	<code>exit</code>	68
3.7	Shell	68
3.7.1	Comunicação via terminal	69
3.7.2	Configuração e uso da COM0	69
3.7.3	Funcionalidades do Shell	70
3.8	<i>Mutex</i>	71
3.9	<i>Threads</i>	72
3.10	Inspiração	73
3.11	Avanços Finais	74
3.11.1	Shell	74
3.11.2	Threads	75
3.11.3	Mutex	75
3.11.4	Chamadas de sistema	76
4	Considerações Finais	77
4.1	Conclusão	77
4.2	Contribuições	77

4.3	Trabalhos Futuros	77
Referências Bibliográficas		79
A	Pesquisas iniciais	81
A.1	O Sistema Operacional <i>eCos</i>	81
A.2	O Sistema Operacional <i>uCLinux</i>	82
B	Arquivos Fonte	83
B.1	cinit.h	83
B.2	cinit.c	83
B.3	constants.h	85
B.4	startup.s	87
B.5	apps/tasks.h	89
B.6	apps/tasks.c	90
B.7	apps/terminal.h	100
B.8	apps/terminal.c	100
B.9	apps/tictactoe.h	114
B.10	apps/tictactoe.c	114
B.11	interrupt/handler_irq.s	120
B.12	interrupt/handler_swi.s	125
B.13	interrupt/irq.h	128
B.14	interrupt/irq.c	129
B.15	interrupt/swi.h	131
B.16	interrupt/swi.c	132
B.17	mutex/mutex.h	133
B.18	mutex/mutex.c	134
B.19	peripherals/button.h	136

B.20 peripherals/button.c	136
B.21 peripherals/dips.h	138
B.22 peripherals/dips.c	138
B.23 peripherals/led.h	139
B.24 peripherals/segment.h	140
B.25 peripherals/segment.c	140
B.26 peripherals/serial.h	142
B.27 peripherals/serial.c	145
B.28 peripherals/timer.h	150
B.29 peripherals/timer.c	151
B.30 syscalls/exec.s	153
B.31 syscalls/exit.s	155
B.32 syscalls/fork.s	156
B.33 syscalls/routine_print.h	160
B.34 syscalls/routine_print.c	160

1 INTRODUÇÃO

1.1 Objetivo

O objetivo deste projeto de formatura é desenvolver um *microkernel* para a placa experimental ARM Evalutator-7T, constituída de um processador ARM7TDMI e de alguns periféricos simples.

O *microkernel* implementa os mecanismos básicos de um sistema operacional, como o chaveamento de *threads*, as chamadas de sistema e utiliza algumas rotinas para a comunicação com os periféricos da placa.

Além disso, foram criados alguns programas para testar e exemplificar o funcionamento do *microkernel*. Entre esses programas, um simples terminal foi desenvolvido para a interação dos usuários com o sistema.

1.2 Motivação

As disciplinas de Laboratório de Microprocessadores e de Sistemas Operacionais do curso de Engenharia da Computação na Escola Politécnica da USP, atualmente, estão muito distantes entre si, no entanto o conteúdo das mesmas é muito próximo.

Pensando em como aproximar essas duas disciplinas, surgiu a idéia de desenvolver uma ferramenta didática que unisse um *hardware* e sistema operacional de estudo simples, e que pudesse ser utilizada nas experiências do Laboratório de Microprocessadores.

Para criação desta ferramenta, foi escolhida a placa experimental ARM Evaluator-7T, que possui uma arquitetura ARM e um poder de processamento bastante superior aos sistemas didáticos utilizados atualmente (baseados nos processadores Intel 8051 e no Motorola 68000). Assim sendo, pretende-se atualizar o material didático da disciplina de microprocessadores, trazendo um sistema mais moderno e mais próximo da realidade atual, além de poder se relacionar com o conteúdo da disciplina de Sistemas Operacionais.

Outra motivação do projeto foi aprofundar nossos conhecimentos sobre sistemas operacionais e sobre a arquitetura dos processadores ARM, visto que este processador é, hoje em dia, largamente utilizado em sistemas embarcados e aparelhos celulares.

1.3 Justificativa

O objetivo inicial do projeto era portar um sistema operacional Unix já existente para a placa didática Evaluator-7T.

Inicialmente pensamos em utilizar os sistemas Android e Minix 3, mas ao estudar o *kernel* dos dois sistemas, vimos que os recursos de memória necessários para executá-los era muito maior que os 512kB disponíveis na placa. Além disso, no caso do Minix 3, teríamos que reescrever o *assembly* do *kernel* que atualmente só tem versão para i386, para *assembly* ARM, o que seria impossível com o tempo disponível para o projeto. Também foram realizadas pesquisas sobre outros Sistemas Operacionais para sistemas embarcados, cujos resultados e conclusões encontram-se no apêndice A.

Assim surgiu a idéia de desenvolver um *microkernel* próprio, com as funcionalidades básicas de um sistema operacional, e que fosse de fácil entendimento; pois como mencionado anteriormente, espera-se que o material desenvolvido seja destinado a melhorar e aproximar o ensino de Sistemas Operacionais com as experiências do Laboratório de Microprocessadores.

1.4 Metodologia de Trabalho

Para a realização desse projeto de formatura procurou-se seguir uma metodologia de trabalho cujas etapas são descritas a seguir:

- Estudo da Arquitetura ARM e da Placa Didática Evaluator-7T:

Antes de especificar as funcionalidades que seriam desenvolvidas, um estudo aprofundado da arquitetura ARM foi realizado para compreender o funcionamento do processador para o qual o *microkernel* foi desenvolvido, o ARM7TDMI.

Além disso, foram executados alguns programas exemplo na placa didática Evaluator-7T para adquirir conhecimentos sobre o seu funcionamento e limitações.

- Montagem do Ambiente de Trabalho:

Paralelamente ao estudo descrito no item anterior, foi montado um ambiente de trabalho utilizando a IDE CodeWarrior para o desenvolvimento do código-fonte e o AXD Debugger para depurar o funcionamento do *microkernel* com ou sem a utilização da placa didática.

Um repositório de controle de versão também foi montado para estocar o material produzido durante do projeto (documentação e código-fonte) e para sincronizar o trabalho dos integrantes do grupo. Seu endereço é <http://code.google.com/p/arm7linux/>

- Especificação Funcional do Microkernel:

O *microkernel* desenvolvido foi especificado nessa etapa, onde foram levantadas as funcionalidades básicas de um sistema operacional que deveriam ser implementadas, como o chaveamento de *threads* e as chamadas de sistema.

- Desenvolvimento do Microkernel:

Nessa fase, foi desenvolvido o *microkernel* utilizando como base a especificação definida no item anterior.

- Análise do Microkernel e Conclusões:

Ao final do desenvolvimento, com base nas dificuldades e soluções encontradas, foi feita uma análise e conclusão sobre o *microkernel* desenvolvido e sua possível utilização no Laboratório de Microprocessadores para exemplificar os conceitos vistos na disciplina de Sistemas Operacionais.

1.5 Organização do Documento

Este documento foi estruturado da seguinte maneira:

- Capítulo 1 (Introdução):

Apresenta objetivo, motivações, justificativas e a metodologia do trabalho.

- Capítulo 2 (Conceitos e Tecnologias Envolvidas):

Contextualiza o leitor em aspectos técnicos específicos utilizados no desenvolvimento do trabalho.

- Capítulo 3 (O Sistema Operacional KinOS):

Descreve como o *microkernel* foi desenvolvido, quais as suas funcionalidades e como funciona a sua integração com os periféricos da placa didática, com o terminal e com os outros programas implementados.

- Capítulo 4 (Considerações Finais):

Analisa os resultados obtidos em relação ao objetivo do projeto, as conclusões, as contribuições deste trabalho e indica possíveis trabalhos futuros com base neste.

2 CONCEITOS E TECNOLOGIAS ENVOLVIDAS

2.1 O Processador ARM7TDMI

O ARM7TDMI faz parte da família de processadores ARM7 32 bits conhecida por oferecer bom desempenho aliado a um baixo consumo de energia. Essas características fazem com que o ARM7TDMI seja bastante utilizado em media players, videogames e, principalmente, em sistemas embarcados e num grande número de aparelhos celulares (SLOSS; SYMES; WRIGHT, 2004).

2.1.1 Arquitetura RISC

Os processadores ARM, incluindo o ARM7TDMI, foram projetados com a arquitetura RISC.

RISC (*Reduced Instruction Set Computer*) é uma arquitetura de computadores baseada em um conjunto simples e pequeno de instruções capazes de serem executadas em um único ou poucos ciclos de relógio.

A idéia por trás da arquitetura RISC é de reduzir a complexidade das instruções executadas pelo *hardware* e deixar as tarefas mais complexas para o *software*. Como resultado, o RISC demanda mais do compilador do que os tradicionais computadores CISC (*Complex Instruction Set Computer*) que, por sua vez, dependem mais do processador já que suas instruções são mais complicadas (SLOSS; SYMES; WRIGHT, 2004).

As principais características da arquitetura RISC são:

1. Conjunto reduzido e simples de instruções capazes de serem executadas em único ciclo de máquina.
2. Uso de *pipeline*, ou seja, o processamento das instruções é quebrado em pequenas unidades que podem ser executadas em paralelo.

3. Presença de um conjunto de registradores.
4. Arquitetura *Load-Store*: o processador opera somente sobre os dados contidos nos registradores e instruções de *load/store* transferem dados entre a memória e os registradores.
5. Modos simples de endereçamento de memória.

2.1.2 Pipeline

A arquitetura de *pipeline* aumenta a velocidade do fluxo de instruções para o processador, pois permite que várias operações ocorram simultaneamente, fazendo o processador e a memória operarem continuamente (ARM LIMITED, 2001b).

O ARM7 possui uma arquitetura de *pipeline* de três estágios. Durante operação normal, o processador estará sempre ocupado em executar três instruções em diferentes estágios. Enquanto executa a primeira, decodifica a segunda e busca a terceira.

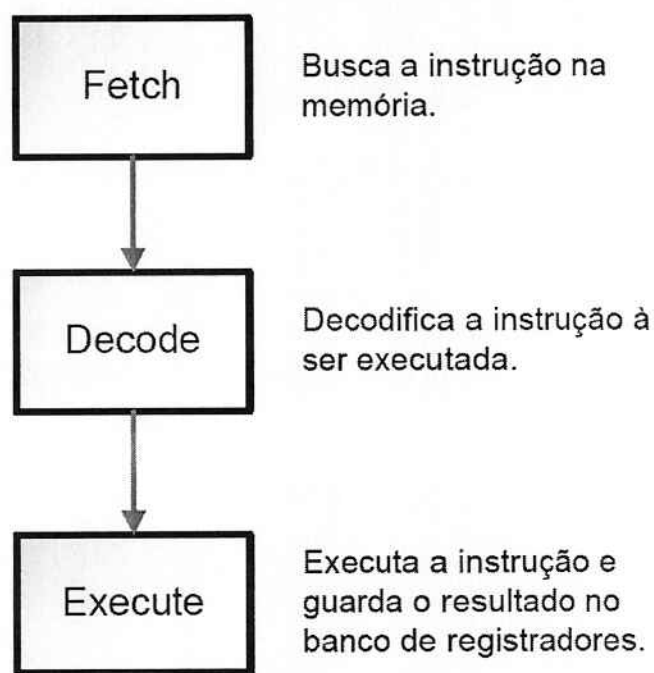


Figura 2.1: Pipeline de 3 estágios (ARM LIMITED, 2001b)

O primeiro estágio de *pipeline* lê a instrução da memória e incrementa o valor do registrador de endereços, que guarda o valor da próxima instrução a ser buscada. O próximo estágio decodifica a instrução e prepara os sinais de controle necessários para executá-la. O terceiro lê os operandos do banco de registradores, executa as operações através da ALU (*Arithmetic*

Logic Unit), lê ou escreve na memória, se necessário, e guarda o resultado das instruções no banco de registradores.

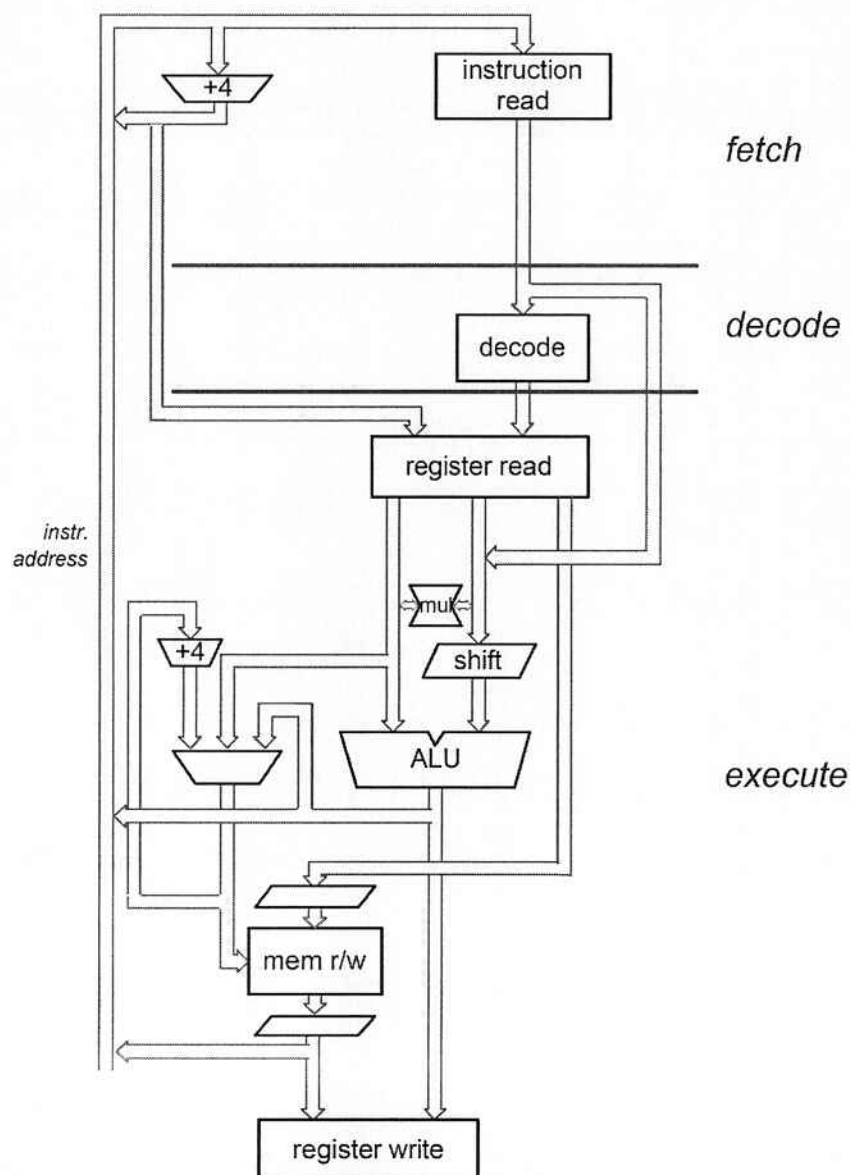


Figura 2.2: Pipeline do ARM7TDMI (RYZHYK, 2006)

Algumas características importantes do *pipeline* do ARM7TDMI:

- O *Program Counter* (PC) ao invés de apontar para a instrução que está sendo executada, aponta para a instrução que está sendo buscada na memória.
- O processador só processa a instrução quando essa passa completamente pelo estágio de execução (*execute*). Ou seja, somente quando a quarta instrução é buscada (*fetched*).

- A execução de uma instrução de *branch* através da modificação do PC provoca a descarga, eliminação, de todas as outras instruções do *pipeline*.
- Uma instrução no estágio *execute* será completada mesmo se acontecer uma interrupção. As outras instruções no *pipeline* serão abandonadas e o processador começará a preencher o *pipeline* a partir da entrada apropriada no vetor de interrupção.

2.1.3 Estados de Operação

O processador ARM7TDMI possui dois estados de operação (ARM LIMITED, 2001b):

- ARM: modo normal, onde o processador executa instruções de 32 bits (cada instrução corresponde a uma palavra);
- Thumb: modo especial, onde o processador executa instruções de 16 bits que correspondem à meia palavra.

Instruções Thumbs são um conjunto de instruções de 16 bits equivalentes as instruções 32 bits ARM. A vantagem em tal esquema, é que a densidade de código aumenta, já que o espaço necessário para um mesmo número de instruções é menor. Em compensação, nem todas as instruções ARM tem um equivalente Thumb.

Neste projeto, o processador é usado no modo ARM que facilita o desenvolvimento por possuir um número maior de instruções.

2.1.4 Modos de Operação

Os processadores ARM possuem 7 modos de operação, como apresentado na tabela 2.1.

Mudanças no modo de operação podem ser realizadas através de programas, ou podem ser causadas por interrupções externas ou exceções (interrupções de software).

A maioria dos programas roda no modo Usuário. Quando o processador esta no modo Usuário, o programa que esta sendo executado não pode acessar alguns recursos protegidos do sistema ou mudar de modo sem ser através de uma interrupção (ARM LIMITED, 2005).

Os outros modos são conhecidos como modos privilegiados. Eles têm total acesso aos recursos do sistema e podem mudar livremente de modo de operação. Cinco desses modos são conhecidos como modos de interrupção: FIQ, IRQ, Supervisor, *Abort* e Indefinido.

Modo	Identificador	Descrição
Usuário	usr	Execução normal de programas.
FIQ (<i>Fast Interrupt</i>)	fiq	Tratamento de interrupções rápidas.
IRQ (<i>Interrupt</i>)	irq	Tratamento de interrupções comuns.
Supervisor	svc	Modo protegido para o sistema operacional.
<i>Abort</i>	abt	Usado para implementar memória virtual ou manipular violações na memória.
Sistema	sys	Executa rotinas privilegiadas do sistema operacional.
Indefinido	und	Modo usado quando uma instrução desconhecida é executada.

Tabela 2.1: Modos de operação (ARM LIMITED, 2005)

Entra-se nesses modos quando uma interrupção ocorre. Cada um deles possui registradores adicionais que permitem salvar o modo Usuário quando uma interrupção ocorre.

O modo remanescente é o modo Sistema, que não é acessível por interrupção e usa os mesmos registradores disponíveis para o modo Usuário. No entanto, este é um modo privilegiado e, assim, não possui as restrições do modo Usuário. Este modo destina-se as operações que necessitam de acesso aos recursos do sistema, mas querem evitar o uso adicional dos registradores associados aos modos de interrupção.

2.1.5 Registradores

O processador ARM7TDMI tem um total de 37 registradores:

- 31 registradores de 32 bits de uso geral
- 6 registradores de estado

Esses registradores não são todos acessíveis ao mesmo tempo. O modo de operação do processador determina quais registradores são disponíveis ao programador (ARM LIMITED, 2001b).

2.1.5.1 Modo Usuário e Sistema

O conjunto de registradores para o modo Usuário (o mesmo usado no modo Sistema) contém 16 registradores diretamente acessíveis, R0 à R15. Um registrador adicional, o CPSR (*Current Program Status Register*), contém os bits de *flag* e de modo.

Os registradores R13 à R15 possuem as seguintes funções especiais (SLOSS; SYMES; WRIGHT, 2004):

- R13: usado como ponteiro de pilha, *Stack Pointer* (SP)
- R14: é chamado de *Link Register* (LR) e é onde se coloca o endereço de retorno sempre que uma sub-rotina é chamada.
- R15: corresponde ao *Program Counter* (PC) e contém o endereço da próxima instrução à ser executada pelo processador.

2.1.5.2 Modos privilegiados

Além dos registradores acessíveis ao programador, o ARM coloca à disposição mais alguns registradores nos modos privilegiados. Esses registradores são mapeados aos registradores acessíveis ao programador no modo Usuário e permitem que estes sejam salvos a cada interrupção.

System and User	FIQ	Supervisor	Abort	IRQ	Undefined
r0	r0	r0	r0	r0	r0
r1	r1	r1	r1	r1	r1
r2	r2	r2	r2	r2	r2
r3	r3	r3	r3	r3	r3
r4	r4	r4	r4	r4	r4
r5	r5	r5	r5	r5	r5
r6	r6	r6	r6	r6	r6
r7	r7	r7	r7	r7	r7
r8	r8_fiq	r8	r8	r8	r8
r9	r9_fiq	r9	r9	r9	r9
r10	r10_fiq	r10	r10	r10	r10
r11	r11_fiq	r11	r11	r11	r11
r12	r12_fiq	r12	r12	r12	r12
r13	r13_fiq	r13_svc	r13_abt	r13_irq	r13_und
r14	r14_fiq	r14_svc	r14_abt	r14_irq	r14_und
r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)	r15 (PC)

ARM-state program status registers

CPSR	CPSR	CPSR	CPSR	CPSR	CPSR
	SPSR_fiq	SPSR_svc	SPSR_abt	SPSR_irq	SPSR_und

 = banked register

Figura 2.3: Organização dos registradores no modo ARM (ARM LIMITED, 2001b)

Como se pode verificar na figura 2.3, cada modo tem o seu próprio R13 e R14. Isso permite que cada modo mantenha seu próprio ponteiro de pilha (SP) e endereço de retorno (LR) (ZAITSEFF, 2003).

Além desses dois registradores, o modo FIQ possui mais cinco registradores especiais: R8_fiq-R12_fiq. Isso significa que quando o processador muda para o modo FIQ, o programa não precisa salvar os registradores de R8 à R12.

Esses registradores especiais mapeiam de um pra um os registradores do modo Usuário. Se ocorrer uma mudança de modo do processador, um registrador particular do novo modo irá substituir o registrador existente.

Por exemplo, quando o processador está no modo IRQ, as instruções executadas continuarão a acessar os registradores R13 e R14. No entanto, esses serão os registradores especiais R13_irq e R14_irq. Os registradores do modo usuário (R13_usr e R14_usr) não serão afetados pelas instruções referenciando esses registradores. O programa continua tendo acesso normal aos outros registradores de R0 à R12 (SLOSS; SYMES; WRIGHT, 2004).

2.1.6 Registradores de Estado

O *Current Program Status Register* (CPSR) é acessível em todos os modos do processador. Ele contém as *flags* de condição, os bits para desabilitar as interrupções, o modo atual do processador, e outras informações de estado e controle. Cada modo de interrupção possui também um *Saved Program Register* (SPSR), que é usado para preservar o valor do CPSR quando a interrupção associada acontece (ARM LIMITED, 2005).

Assim, os registradores de estado (ARM LIMITED, 2001b):

- Guardam informação sobre a operação mais recente executada pela ALU.
- Controlam o ativar e desativar de interrupções.
- Determinam o modo de operação do processador.

Como mostrado na figura 2.4 o CPSR é dividido em 3 campos: *flag*, reservado (não utilizado) e controle.

O campo de controle guarda os bits de modo, estado e de interrupção, enquanto o campo *flag* armazena os bits de condição.

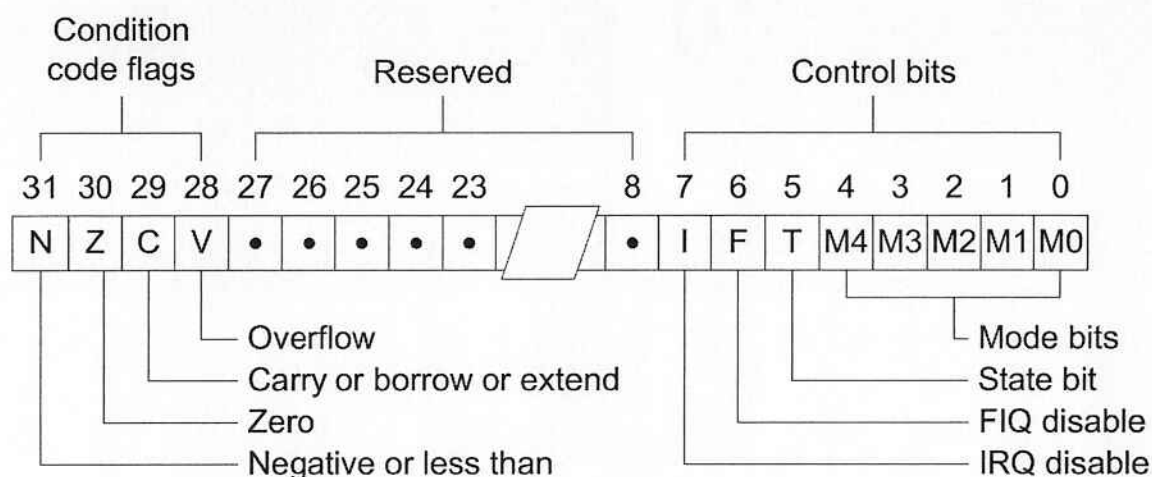


Figura 2.4: Formato dos registradores de estado CPSR e SPSR (ARM LIMITED, 2001b)

2.1.6.1 Flags de Condição

Os bits N, Z, C e V são *flags* de condição, e é possível alterá-los através do resultado de operações lógicas ou aritméticas (ARM LIMITED, 2005).

Os *flags* de condição são normalmente modificados por:

- Uma instrução de comparação (CMN, CMP, TEQ, TST).
- Alguma outra instrução aritmética, lógica ou *move*, onde o registrador de destino não é o R15 (PC).

Nesses dois casos, as novas *flags* de condição (depois de a instrução ter sido executada) normalmente significam:

- N: Indica se o resultado da instrução é um número positivo (N=0) ou negativo (N=1).
- Z: Contém 1 se o resultado da instrução é zero (isso normalmente indica um resultado de igualdade para uma comparação), e 0 se o contrário.
- C: Pode possuir significados diferentes:
 - Para uma adição, C contém 1 se a adição produz "vai-um" (*carry*), e 0 caso contrário.
 - Para uma subtração, C contém 0 se a subtração produz "vem-um" (*borrow*), e 1 caso contrário.

- Para as instruções que incorporam deslocamento, C contém o último bit deslocado para fora pelo deslocador.
- Para outras instruções, C normalmente não é usado.
- V: Possui dois significados:
 - Para adição ou subtração, V contém 1 caso tenha ocorrido um *overflow* considerando os operandos e o resultado em complemento de dois.
 - Para outras instruções, V normalmente não é usado.

2.1.6.2 Bits de Controle

Os oito primeiros bits de um PSR (*Program Status Register*) são conhecidos como bits de controle (ARM LIMITED, 2005). Eles são:

- Bits de desativação de interrupção
- Bit T
- Bits de modo

Os bits de controle mudam quando uma interrupção acontece. Quando o processador esta operando em um modo privilegiado, programas podem manipular esses bits.

Bits de desativação de interrupção

Os bits I e F são bits de desativação de interrupção:

- Quando o bit I é ativado, as interrupções IRQ são desativadas.
- Quando o bit F é ativado, as interrupções FIQ são desativadas.

Bit T

O bit T reflete o modo de operação:

- Quando o bit T é ativado, o processador é executado em estado Thumb.
- Quando o bit T é desativado, o processador é executado em estado ARM.

Bits de modo

Os bits M[4:0] determinam o modo de operação. Nem todas as combinações dos bits de modo definem um modo válido, portando deve-se tomar cuidado para usar somente as combinações mostradas na tabela 2.2.

Bit de modo	Modo de operação	Registradores acessíveis
10000	Usuário(usr)	PC,R14-R0,CPSR
10001	FIQ(fiq)	PC,R14_fiq-R8_fiq,R7-R0,CPSR,SPSR_fiq
10010	IRQ(irq)	PC,R14_irq, R13_irq,R12-R0,CPSR,SPSR_irq
10011	Supervisor(svc)	PC,R14_svc, R13_irq,R12-R0,CPSR,SPSR_svc
10111	Abort(abt)	PC,R14_abt, R13_irq,R12-R0,CPSR,SPSR_abt
11011	Indefinido(und)	PC,R14_und, R13_irq,R12-R0,CPSR,SPSR_und
11111	Sistema(sys)	PC,R14-R0,CPRS

Tabela 2.2: Valores para o bit de modo (ARM LIMITED, 2005)

2.1.7 Interrupções

Interrupções surgem sempre que o fluxo normal de um programa deve ser interrompido temporariamente, por exemplo, para servir uma interrupção vinda de um periférico ou a tentativa de executar uma instrução desconhecida. Antes de tentar lidar com uma interrupção, o ARM7TDMI preserva o estado atual de forma que o programa original possa ser retomado quando a rotina de interrupção tiver acabado (ARM LIMITED, 2001b).

A arquitetura ARM suporta 7 tipos de interrupções. A tabela 2.3 lista os tipos de interrupção e o modo do processador usado para lidar com cada tipo. Quando uma interrupção acontece, a execução é forçada para um endereço fixo de memória correspondente ao tipo de interrupção. Esses endereços fixos são chamados de vetores de interrupção (ARM LIMITED, 2005).

Deve-se notar olhando para a tabela 2.3, que existe espaço suficiente para apenas uma instrução entre cada vetor de interrupção (4 bytes). Estes são inicializados com instruções de desvio (*branch*).

2.1.7.1 Prioridade das Interrupções

Quando várias interrupções acontecem ao mesmo tempo, uma prioridade fixa do sistema determina a ordem na qual elas serão manipuladas. Essa prioridade é listada na tabela 2.4:

Tipo de interrupção	Modo de operação	Endereço
<i>Reset</i>	Supervisor	0x00000000
Instrução indefinida	Indefinido	0x00000004
Interrupção de Software (swi)	Supervisor	0x00000008
<i>Prefetch abort</i>	<i>Abort</i>	0x0000000C
<i>Data abort</i>	<i>Abort</i>	0x00000010
Interrupção normal (IRQ)	IRQ	0x00000018
Interrupção rápida (FIQ)	FIQ	0x0000001C

Tabela 2.3: Vetor de interrupção (ARM LIMITED, 2005)

Prioridade	Interrupção
alta	Reset <i>Data abort</i> FIQ IRQ <i>Prefetch abort</i>
baixa	Instrução indefinida e interrupção de software (SWI)

Tabela 2.4: Ordem de prioridade das interrupções (ARM LIMITED, 2001b)

2.1.7.2 Entrada de interrupção

Executar uma interrupção necessita que o processador preserve o estado atual. Em geral, o conteúdo de todos os registradores (especialmente PC e CPSR) devem ser o mesmo depois de uma interrupção.

O processador ARM usa os registradores adicionais de cada modo para ajudar a salvar o estado do processador. Quando uma interrupção acontece, o R14 e o SPSR são usados para guardar o estado atual da seguinte maneira (ARM LIMITED, 2001b):

1. Preserva o endereço da próxima instrução (PC+4 ou PC+8, depende da interrupção) no apropriado LR (R14). Isso permite ao programa continuar do lugar de onde parou no retorno da interrupção.
2. Copia o CPSR para o apropriado SPSR.
3. Força os bits de modo do CPSR para um valor que corresponde ao tipo de interrupção.
4. Força o PC buscar a próxima instrução no vetor de interrupção.

O processador ARM7TDMI também pode ativar a *flag* de interrupção para desabilitar próximas interrupções.

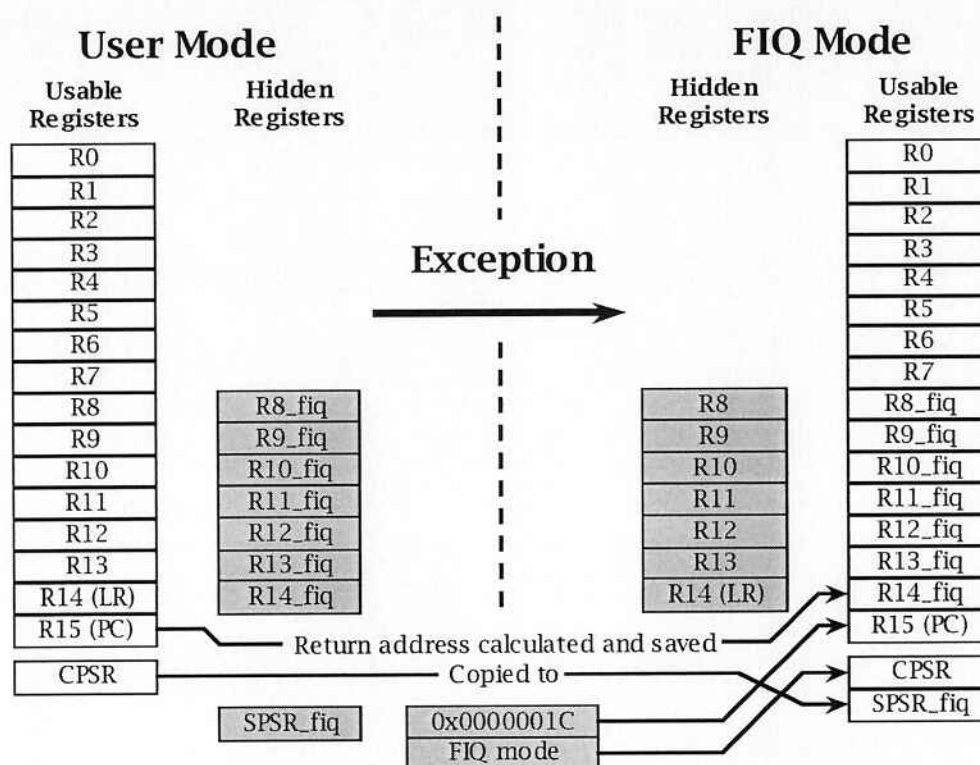


Figura 2.5: Esquema de uma interrupção no ARM7TDMI (ZAITSEFF, 2003)

2.1.7.3 Saída de interrupção

Quando uma interrupção é completada deve-se (ARM LIMITED, 2001b):

1. Mover o LR (R14), menos um *offset*, para o PC. O *offset* varia de acordo com o tipo de interrupção mostrada na figura anterior.
2. Copiar o SPSR de volta para o CPSR.
3. Desativa as *flags* de interrupção que foram ativadas na entrada.

2.1.7.4 Interrupções de software

Uma interrupção de software é uma interrupção inicializada inteiramente por um programa para entrar no modo Supervisor e assim poder utilizar alguma rotina particular, como operações de entrada e saída do sistema (ZAITSEFF, 2003).

Quando uma interrupção de software é executada, as seguintes ações são realizadas (ARM LIMITED, 2005):

1. Copia o endereço da próxima instrução no registrador LR_svc (R14_svc).

```
R14_svc = endereço da próxima instrução
```

2. Copia o CPSR no SPSR_svc.

```
SPSR_svc = CPSR
```

3. Ativa os bits de modo do CPSR com o valor correspondente ao modo Supervisor.

```
CPSR[4:0] = 0b10011 /* modo Supervisor */
```

4. Reforça o estado ARM colocando o bit T do CPSR à zero.

```
CPSR[5] = 0 /* estado ARM */
```

5. Desabilita as interrupções normais ativando o bit I do CPSR. Interrupções FIQ não são desabilitadas e podem continuar ocorrendo.

```
CPSR[7] = 1 /* desabilita interrupções normais */
```

6. Carrega o endereço do vetor de interrupções, 0x00000008, no PC.

```
PC = 0x00000008
```

Para retornar da operação de interrupção, é usada a seguinte instrução para restaurar o PC (a partir do R14_svc) e o CPSR (a partir do SPSR_svc):

```
MOVS PC, LR
```

2.1.7.5 Interrupções de hardware

Interrupções de hardware são mecanismos que permitem que um sinal externo (pedido de interrupção) interrompa a execução normal do programa corrente e desvie a execução para um bloco de código chamado de rotina de interrupção (KINOSHITA, 2007).

Interrupções são úteis, pois permitem que o processador manuseie periféricos de uma maneira mais eficiente. Sem elas, o processador teria que verificar periodicamente a entrada/saída de um dispositivo para ver se esse necessita de tratamento. Com elas, por outro lado, a entrada/saída do dispositivo pode indicar diretamente a ocorrência de um dado evento externo, que será tratado com maior facilidade e rapidez, de modo que o microprocessador não necessite consumir tempo de processamento para pesquisar a ocorrência de eventos externos.

O processador ARM fornece dois sinais que são usados pelos periféricos para pedir uma interrupção: o sinal de interrupção nIRQ e o sinal de interrupção rápida nFIQ. Ambos são ativados em nível baixo, ou seja, colocando o sinal em nível baixo gera-se a interrupção correspondente, se a interrupção não tiver sido desabilitada no CPSR (ZAITSEFF, 2003).

Quando uma interrupção de *hardware* IRQ (ou FIQ) é detectada, as seguintes ações são realizadas (ARM LIMITED, 2005):

1. Copia o endereço da próxima instrução a ser executada + 4 no registrador LR_irq (R14_irq). Isso significa que o LR_irq irá apontar para a segunda instrução a partir do ponto de pedido da interrupção.

```
R14_irq = endereço da próxima instrução + 4
```

2. Copia o CPSR no SPSR_irq.

```
SPSR_irq = CPSR
```

3. Coloca os bits de modo do CPSR para o valor correspondente ao modo IRQ.

```
CPSR[4:0] = 0b10010 /* modo IRQ */
```

4. Reforça o estado ARM colocando o bit T do CPSR a zero.

```
CPSR[5] = 0 /* estado ARM */
```

5. Desabilita as interrupções normais ativando o bit I do CPSR. Interrupções FIQ não são desabilitadas e podem continuar ocorrendo.

```
CPSR[7] = 1 /* desabilita interrupções normais */
```

6. Carrega o endereço do vetor de interrupções, 0x00000008, no PC.

```
PC = 0x00000018
```

Assim que a rotina de interrupção é terminada, o processador retorna ao que estava fazendo antes através das seguintes ações:

1. Move o conteúdo do registrador LR_irq menos 4 para o PC.
2. Copia SPSR_irq de volta para CPSR.

A seguinte instrução executa os passos mostrados acima:

```
SUBS PC, R14, #4
```

Note que a instrução é SUBS, e não SUB: a instrução SUBS copia automaticamente SPSR no CPSR, mas apenas quando o registrador de destino é o PC (R15) e a instrução é executada em um modo privilegiado.

O processamento das *Fast Interrupt* (FIQ) é praticamente igual ao de uma interrupção normal (IRQ). As diferenças são que um conjunto diferente de registradores é usado (i.e. R14_fiq no lugar de R14_irq), que tanto as interrupções IRQ quanto as FIQ são desativadas (ou seja, os bits I e F do CPSR são ativados), e que o endereço do vetor de interrupção é 0x0000001C (ZAITSEFF, 2003).

2.1.8 Programando em C pra o ARM7TDMI

Neste item são apresentados alguns pontos importantes a serem considerados quando se esta programando em C para o processador ARM7.

2.1.8.1 Alocação de Registradores

O compilador tenta alocar um registrador do processador para cada variável local que encontra em uma função C. Ele tenta usar o mesmo registrador para diferentes variáveis locais se a utilização das variáveis não se sobrepõem. Quando há mais variáveis locais que registradores disponíveis, o compilador armazena as variáveis em excesso na pilha do processador (SLOSS; SYMES; WRIGHT, 2004).

2.1.8.2 Chamadas de Função

A *ARM Procedure Call Standard* (APCS) define como passar argumentos de função e obter valores de retorno.

Os primeiros quatro argumentos inteiros são passadas nos quatro primeiros registradores ARM: R0, R1, R2 e R3. Argumentos inteiros posteriores são colocados na pilha, como na figura 2.6. Se o valor de retorno for inteiro, este é obtido através do registrador R0 (SLOSS; SYMES; WRIGHT, 2004).

Esta descrição abrange apenas os argumentos de tipo inteiro ou ponteiro. Argumentos que ocupam o espaço de duas palavras, como *long long* e *double*, são passados em um par de

registradores consecutivos e retornam em R0, R1.

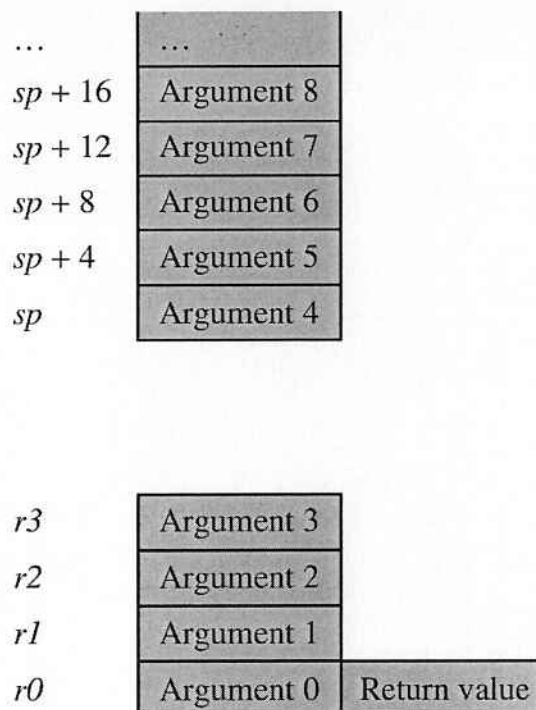


Figura 2.6: Passagem de argumentos (SLOSS; SYMES; WRIGHT, 2004)

2.2 A Placa Experimental Evaluator-7T

O principal elemento de hardware deste projeto é a placa experimental ARM Evaluator-7T, baseada no processador ARM7TDMI, um processador RISC de 32 bits capaz de executar o conjunto de instruções denominado Thumb.

Os principais elementos presentes na arquitetura da placa Evaluator-7T são os seguintes:

- Microcontrolador Samsung KS32C50100
- 512kB EPROM flash
- 512kB RAM estática (SRAM)
- Dois conectores RS232 de 9 pinos tipo D
- Botões de reset e de interrupção

- Quatro LEDs programáveis pelo usuário e um display de 7 segmentos
- Entrada de usuário por um interruptor DIP com 4 elementos
- Conector Multi-ICE
- Clock de 10MHz (o processador usa-o para gerar um clock de 50MHz)
- Regulador de tensão de 3.3V

A figura 2.7 mostra a organização desses elementos na placa experimental.

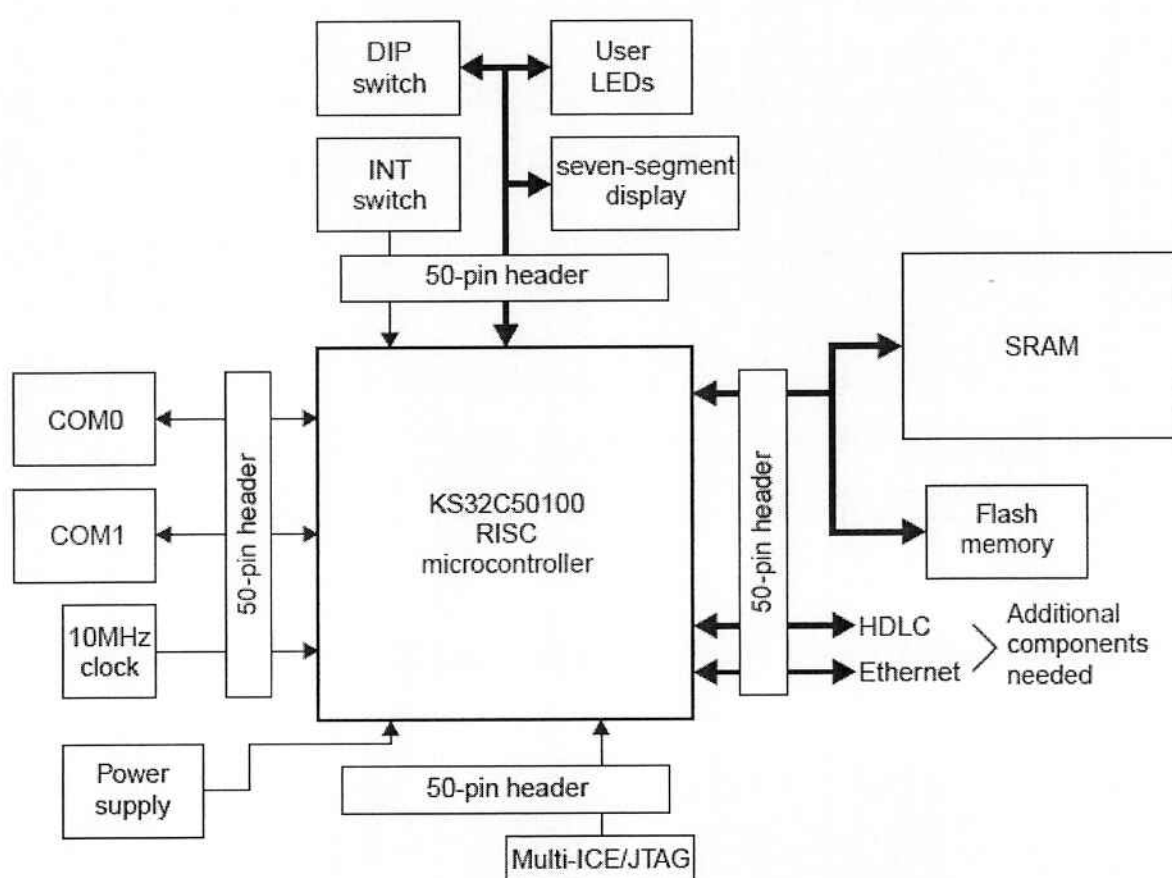


Figura 2.7: Arquitetura da placa Evaluator-7T. (ARM LIMITED, 2000)

Com relação à memória flash da placa, ela vem de fábrica com o bootstrap loader da placa e programa monitor de debug. O restante dela pode ser usado para os programas de usuário. A tabela 2.5 mostra a faixa de endereços de cada região da memória.

Já em relação às duas portas seriais presentes na placa, cada uma tem usos específicos. A primeira, chamada DEBUG, é usada pelo monitor de debug ou pelo programa bootstrap presente na placa. Ela está conectada ao UART1 do microcontrolador. A segunda, chamada

Tabela 2.5: Mapa da memória flash (ARM LIMITED, 2000)

Faixa de endereço	Descrição
0x01800000 a 0x01806FFF	Bootstrap loader
0x01807000 a 0x01807FFF	Teste de produção
0x01808000 a 0x0180FFFF	Reservado
0x01810000 a 0x0181FFFF	Angel
0x01820000 a 0x0187FFFF	Disponível para outros programas e dados

USER, é de uso genérico e está disponível para uso em programas. Ela está conectada ao UART0 do microcontrolador.

2.2.1 Bootstrap Loader

Como mencionado anteriormente, a memória flash da placa contém uma região reservada para os programas Bootstrap Loader (BSL) e o programa monitor de debug chamado Angel.

O BSL é o primeiro programa a ser executado pelo microcontrolador quando esta é ligada ou reiniciada. Suas principais funções são:

- Fazer a conexão com o computador através da porta serial e uma aplicação de terminal, como o HyperTerminal do Windows
- Prover a infraestrutura necessária à configuração da placa
- Prover ajuda ao usuário
- Gerenciar imagens de memória como um conjunto de módulos executáveis
- Carregar aplicações na SRAM e executá-las

2.2.1.1 Comunicação com o PC

Neste projeto, foi usado um PC com o sistema operacional Windows XP para fazer a comunicação com o BSL da placa Evaluator-7T. Essa comunicação é feita através de um cabo serial conectado à porta COM1 (Debug) da placa. Estando a placa conectada à porta serial e energizada com uma fonte de alimentação própria, pode-se estabelecer a comunicação com o BSL por meio do programa HyperTerminal. As configurações de comunicação utilizadas foram:

- Velocidade de transferência de 9600 bauds

- 8 bits de dados
- Sem paridade
- 1 bit de parada
- Sem controle de fluxo

Após a configuração adequada da placa, é preciso reiniciá-la, pressionando o botão SW1 (SYS RESET). Então, a placa envia a seguinte mensagem ao terminal:

```
ARM Evaluator7T Boot Strap Loader Release 1.01  
Press ENTER within 2 seconds to stop autoboot
```

Pressionando a tecla *Enter* em até dois segundos da exibição da mensagem acima, nenhum outro módulo da memória é executado, além do BSL. Desse momento em diante, o BSL exibe seu editor de linha de comando, a partir do qual é possível gerenciar, embarcar e executar programas na placa. A figura 2.8 mostra o HyperTerminal com o BSL carregado e aguardando um comando.

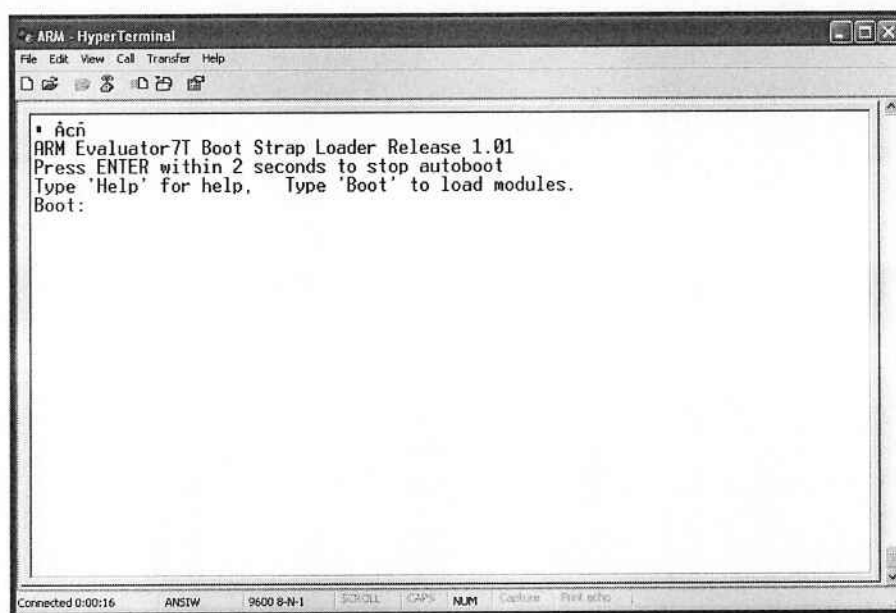


Figura 2.8: Editor de linha de comando do BSL via HyperTerminal

2.2.1.2 Carregando e executando programas via BSL

Após a compilação de um projeto, o ambiente de desenvolvimento cria uma imagem de memória em formato binário (extensão *.bin*). Essa imagem, no entanto, não pode ser carregada

diretamente na placa através do BSL. Ela deve ser convertida para o formato UUE (Unix-to-Unix Encoding), o qual é uma representação em arquivo texto do arquivo binário original. Neste projeto, foi utilizado para essa conversão o programa *uuencode* fornecido no CD-ROM que acompanha a placa Evaluator-7T.

Uma vez convertido o arquivo para o formato adequado, ele está pronto para ser enviado à Evaluator-7T. Para isso, pode-se usar dois diferentes comandos do BSL: *Download* ou *FlashLoad*.

O comando *Download* carrega uma imagem na memória RAM da placa. A sintaxe desse comando é:

```
download [<endereço>]
```

O parâmetro <endereço>, que é um número em base hexadecimal, indica em qual endereço da RAM a imagem será carregada. Se esse endereço não for especificado, a imagem é carregada na posição 0x8000.

Assim que o comando é executado, o BSL espera a transferência de um arquivo texto com a imagem de memória desejada. No HyperTerminal, isso é feito pelo comando "Enviar arquivo texto" e apontando para o arquivo desejado, no formato UUE. Terminada a transferência, o BSL informa quantos bytes foram recebidos e a posição de memória a partir da qual eles foram gravados.

Já o comando *FlashLoad* carrega uma imagem na placa e a salva diretamente na memória flash da mesma. Sua sintaxe é a seguinte:

```
flashload <endereço>
```

Neste comando, o parâmetro <endereço> é obrigatório, também é um número em base hexadecimal e especifica o endereço da memória flash no qual a imagem será gravada. O envio do arquivo é feito da mesma maneira que o comando *Download*. Como não há restrições quanto ao valor que o usuário pode inserir nesse comando, cabe a ele mesmo tomar cuidado para não escrever dentro da faixa de endereços de 0x01800000 a 0x0180FFFF, uma vez que é nessa área da flash que estão os módulos BSL e de teste de produção.

O comando *FlashLoad* não é o único que manipula a memória flash da placa no BSL. Existem também os comandos *FlashWrite* e *FlashErase*. O primeiro escreve na memória flash uma determinada área da RAM, enquanto que o segundo sobrescreve uma faixa de endereços da flash com 0xFF. As sintaxes desses comandos são:

```
flashwrite <endereço> <font> <comprimento>
```

```
flasherase <endereço> <comprimento>
```

Mais uma vez, é preciso exercer cautela durante a utilização desses comandos para não comprometer a área de memória onde se encontram os módulos BSL e de teste de produção.

Carregada a imagem na memória RAM ou na memória flash, ela está pronta para execução. Para executá-la, deve-se, primeiramente, verificar se o Program Counter (PC) do BSL está apontando para a posição de memória onde foi gravada a imagem. Isso é feito através do comando *PC*, cuja sintaxe está abaixo.

```
pc [<endereço>]
```

Esse comando permite verificar a posição a partir da qual o BSL iniciará a execução, se o parâmetro *<endereço>* não for especificado. Quando esse comando é feito com um argumento, o valor do PC é alterado para o valor do argumento inserido. Por exemplo, *pc 10000* coloca o PC na posição de memória 0x10000. Quando os comandos *Download* e *FlashLoad* são executados, o PC é atualizado automaticamente para o valor inserido no parâmetro *<endereço>* desses comandos.

O próximo passo para a execução da imagem pode ser feito com dois comandos diferentes: *Go* ou *GoS*. Ambos iniciam a execução de um programa a partir da posição de memória definida no PC. Enquanto o primeiro executa o programa em Modo Usuário, o segundo o faz em Modo Supervisor (SVC). Opcionalmente, pode-se inserir argumentos de entrada do programa quando esses comandos são chamados. A sintaxe deles é:

```
go [<argumentos do programa>]
```

```
gos [<argumentos do programa>]
```

Assim, o programa começa a executar na placa. Caso seja necessário retornar ao BSL, deve-se reiniciar a placa, pressionando-se o botão SYS RESET. Qualquer imagem que tenha sido carregada apenas na RAM será perdida.

2.2.2 Angel Debug Monitor

O monitor de debug Angel é fornecido conjuntamente com diversas placas da ARM e suas parceiras. Suas principais funcionalidades são:

- Função de depuração de código, incluindo inspeção de memória, download e execução

de imagens de memória, uso de breakpoints e execução passo-a-passo

- Inicialização da CPU e da placa e tratamento básico de exceções
- Uma biblioteca ANSI C completa, com uso de semihosting para prover serviços do computador host que não estão disponíveis na placa

Há duas maneiras pelas quais o Angel se comunica com o ambiente de desenvolvimento de software.

A primeira é através da biblioteca de interfaces chamada "Remote_A". Por ela, os depuradores se comunicam com um alvo do Angel quando fazem depuração ou execução de código.

A segunda é por meio de interrupções de software (SWI). O código do programa faz uma SWI para solicitar serviços dos Angel diretamente ou através da biblioteca C do toolkit.

2.3 O ambiente de desenvolvimento

O hardware descrito na seção 2.2 não pode realizar muitas tarefas se não houver o software adequado embarcado nele. Assim, o desenvolvimento de programas é parte fundamental do projeto. Para realizar tal tarefa, é necessária a existência de um ambiente de desenvolvimento que permita escrever, compilar, embarcar e depurar programas para a Evaluator-7T.

Neste projeto, foi utilizado o ambiente ARM Developer Suite (ADS) versão 1.2. Ele contém a IDE CodeWarrior e o debugger AXD. Ambos estão descritos em detalhes nas subseções abaixo.

2.3.1 CodeWarrior

O CodeWarrior é um ambiente integrado de desenvolvimento, ou seja, é um software que provê diversas funcionalidades para facilitar o desenvolvimento de programas. Dentre as funcionalidades que ele fornece, pode-se citar:

- Editor de código-fonte em C/C++ e ARM Assembly
- Compilador C/C++ para Assembly ARM e Thumb

- Automatização da compilação e geração de imagens de memória

O CodeWarrior permite a criação de projetos, ou seja, conjuntos de arquivos de código-fonte conjuntamente com as configurações de compilação, (por exemplo, arquitetura para a qual o código-objeto será gerado) e ligação dos mesmos. Essa organização é fundamental para a criação de uma única imagem de memória quando a compilação do projeto é realizada, pois assim todo o trabalho se torna automatizado.

A figura 2.9 mostra a aparência da IDE durante sua utilização normal.

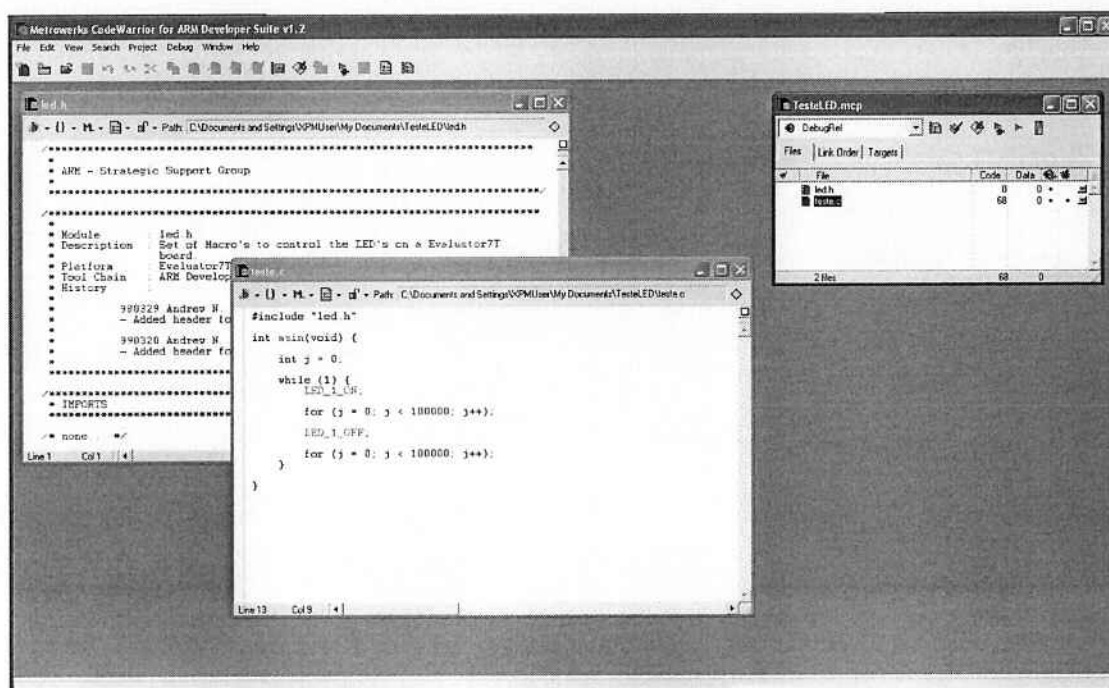


Figura 2.9: Screenshot da IDE CodeWarrior

Quando um projeto é compilado com sucesso no CodeWarrior, a imagem de memória gerada por ele pode ser aproveitada diretamente pelo debugger AXD, uma vez que ambas as ferramentas estão fortemente interligadas. Desse modo, é possível inicializar o AXD diretamente a partir do CodeWarrior através dos botões "Run" ou "Debug".

2.3.2 AXD Debugger

O AXD Debugger é um programa destinado à execução e depuração de código dentro do ambiente ADS. Suas principais funcionalidades são:

- Execução de código passo a passo e por pontos de parada (*breakpoints*)
- Inspeção de variáveis e de registradores do processador

- Suporte para alvos em *hardware* e em *software* (emuladores)
- Envio e gravação de imagens de memória na RAM do *hardware*-alvo
- Suporte a diferentes arquiteturas ARM
- Persistência das configurações em múltiplas sessões de debug

A figura 2.10 mostra a aparência do ambiente AXD em operação normal.

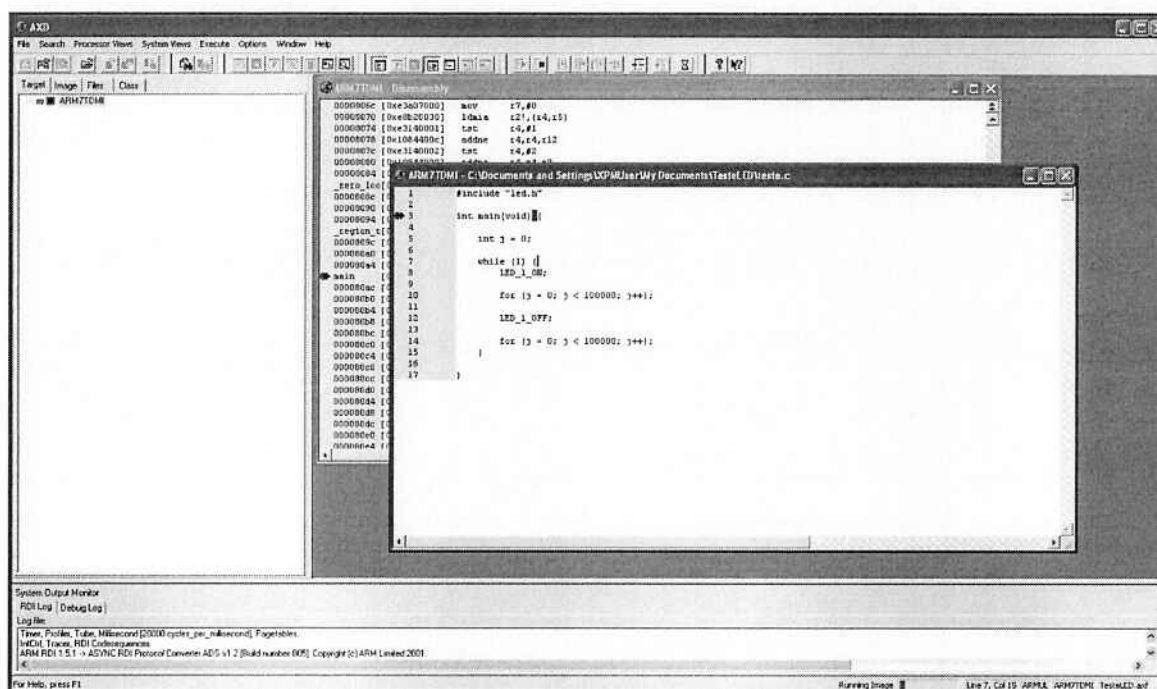


Figura 2.10: Screenshot do AXD Debugger

Durante o projeto, para a realização de testes dos programas desenvolvidos, utilizou-se frequentemente o ambiente emulado do processador ARM7TDMI fornecido pelo AXD, uma vez que nem sempre houve acesso à placa Evaluator-7T.

3 O SISTEMA OPERACIONAL KINOS

O principal objetivo do projeto é auxiliar o ensino de sistemas operacionais e da arquitetura ARM nas disciplinas de Sistemas Operacionais e Laboratório de Microprocessadores. Para tal, foi desenvolvido um *microkernel*, apelidado de KinOS, cujas funções básicas são o chaveamento de *threads* através de interrupção de *timer*, as chamadas de sistema, as rotinas de manipulação de *hardware*, funções de *mutex* e um *shell*.

3.1 Organização do código

A estrutura de arquivos do projeto pode ser vista na figura 3.1. Pode-se dividi-lo em cinco partes:

- **Raiz** Arquivos de inicialização da placa
- **Pasta “apps”** Programas que serão executados pelo *microkernel*
- **Pasta “interrupt”** Rotinas de tratamento de interrupção
- **Pasta “peripherals”** Rotinas de manipulação de *hardware*
- **Pasta “syscalls”** Chamadas de sistema
- **Pasta “mutex”** Rotinas do *mutex*

A pasta KinOS_Data não é considerada parte do projeto pois é utilizada pelo CodeWarrior para o armazenamento do código compilado.

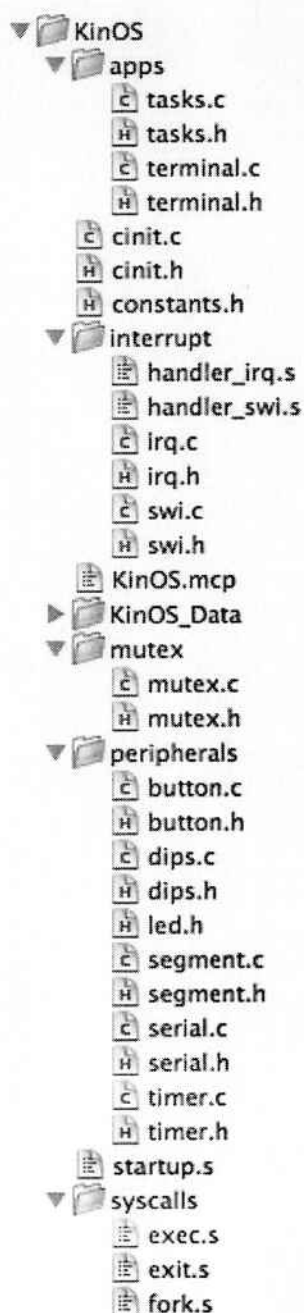


Figura 3.1: Estrutura de arquivos.

3.1.1 Raiz

Os arquivos encontrados na raiz do projeto são responsáveis pela inicialização da placa e pela declaração de constantes globais. O arquivo `startup.s` contém a chamada inicial do *microkernel*, onde toda parte de inicialização em *assembly* é feita. Já o arquivo `cinit.c` também contém a parte de inicialização, porém, o código está escrito em C. Finalmente, o arquivo `constants.h` é responsável por armazenar as constantes que são utilizadas em todo o projeto.

3.1.2 Pasta “apps”

No arquivo `tasks.c`, várias funções são declaradas, onde cada declaração é considerada uma *thread* pelo *microkernel*. Mais à frente, na seção 3.9, os programas exemplo serão descritos com mais detalhe. Já no arquivo `terminal.c` é responsável pela implementação do *shell* do sistema.

3.1.3 Pasta “interrupt”

Todas as rotinas que tratam e instalam interrupções – tanto de *hardware* quanto de *software* – estão localizadas nesta pasta. O arquivo `handler_irq.s` contém a rotina em *assembly* que trata das interrupções de *hardware*, as encaminha para a rotina específica de acordo com a sua fonte e faz o chaveamento de *threads*. O arquivo `irq.c` contém uma única rotina, que realiza a instalação da rotina de tratamento de interrupção tanto de *hardware* quanto de *software*. A rotina de tratamento de interrupção de *software* é feita no arquivo `handler_swi.s`, que identifica o tipo de interrupção e encaminha para alguma das chamadas de sistema, encontradas em `swi.c`.

3.1.4 Pasta “peripherals”

As rotinas de inicialização e controle dos periféricos se encontram todas nesta pasta. As do botão estão no arquivo `button.c`, da chave DIP no arquivo `dips.c`, do display de sete segmentos em `segment.c`, dos LEDs em `led.c` e do *timer* em `timer.c`.

3.1.5 Pasta “syscalls”

As chamadas de sistema estão escritas em *assembly* e se encontram em três arquivos, uma para cada chamada. São elas as chamadas *fork*, *exec* e *exit*.

3.1.6 Pasta “mutex”

No arquivo `mutex.c` há apenas as funções que permitem a exclusão mútua de código por espera ativa, feita através de um *mutex*.

3.2 Estruturas de dados

A fim de se facilitar a programação e o entendimento do projeto, foram criadas duas estruturas de dados que são acessadas em *assembly*. A primeira, o *Process Control Block* é responsável pelo armazenamento do estado de uma *thread*. Já o "vetor de *threads*" realiza o controle de quais *threads* estão ativas.

3.2.1 Process Control Block

O *Process Control Block* (ou simplesmente PCB) é uma estrutura de dados que guarda todas as informações de uma *thread* que aguarda para ser executada enquanto outras estão ativas. Há um PCB para cada uma das nove *threads* e cada um ocupa 68 bytes. Ou seja, o espaço total ocupado pelos PCBs é de $9 \cdot 68 = 612$ bytes. Estes 68 bytes estão estruturados como explicitado na figura 3.2. Cada posição da tabela ocupa uma palavra (4 bytes). A primeira posição é em (base do PCB - 4), a segunda em (base do PCB - 8) e assim por diante. Como pode-se observar pela figura, as posições 1 a 15 ((base do PCB - 4) a (base do PCB - 60)) armazenam o conteúdo dos registradores r0 a r14 do modo *user* em ordem inversa. A posição 16 (base do PCB - 64) armazena o *link register* do modo IRQ, ou seja, o endereço de retorno da interrupção. Finalmente, a posição 17 armazena o registrador de estado do modo *user*. Estes registradores armazenados permitem estabelecer um retrato preciso do estado da *thread* quando houve o chaveamento e permite também que este estado seja restabelecido quando for o turno desta *thread* voltar a ser executada. A estrutura tem seu espaço reservado no arquivo *handler_irq.s*, e é nomeado com a variável *process_control_block*, que indica a base da estrutura. Cada um dos PCBs está logo a seguir do anterior. Por exemplo, a base do primeiro PCB está em (*process_control_block* - 68), do segundo em (*process_control_block* - $2 \cdot 68$) e assim por diante.

3.2.2 Vetor de threads

O vetor de *threads* é uma lista que armazena quais das *threads* estão ativas e quais não estão, a fim de se identificar quais devem ser colocadas em execução. Cada identificador ocupa 4 bytes, e pode ter os valores 0 (inativo) ou 1 (ativo). Como há 9 *threads*, o tamanho deste vetor é de $4 \cdot 9 = 36$ bytes. Seu espaço é reservado no arquivo *handler_irq.s*, com o nome de *thread_array*. No exemplo na figura 3.3 pode-se ver que as *threads* 1, 2 e 4 estão ativas, enquanto que as outras não estão.

Offset	Task Register
-4	r14_usr
-8	r13_usr
-12	r12_usr
-16	r11_usr
-20	r10_usr
-24	r9_usr
-28	r8_usr
-32	r7_usr
-36	r6_usr
-40	r5_usr
-44	r4_usr
-48	r3_usr
-52	r2_usr
-56	r1_usr
-60	r0_usr
-64	r14_irq
-68	SPSR

Figura 3.2: Estrutura de dados do PCB. Fonte: (SLOSS, 2001)

T1	T2	T3	T4	T5	T6	T7	T8	T9
1	1	0	1	0	0	0	0	0

Figura 3.3: Vetor de *threads*.

3.3 Configuração de hardware e software

Nesta seção são apresentados os modos como o *hardware* e o *software* descritos anteriormente são utilizados. Será indicado como foi feito o particionamento da memória, a utilização dos modos do processador e os modos de teste do código.

3.3.1 Memória

A memória volátil da placa foi estruturada como indicado na figura 3.4. Para todo espaço das pilhas, programas, código, vetor de interrupções e área de dados, o espaço disponível é de 128KB (de 0x0 a 0x20000). Como pôde ser visto na seção 2.1.7, a memória entre 0x0 e 0x20 contém o vetor de interrupções e deve ser reservado. A pilha do modo SVC começa

no endereço 0x7F80, cresce para baixo e não deve invadir a área reservada para o vetor de interrupção. Já a pilha do modo IRQ, começa no endereço 0x8000, também cresce para baixo e não deve invadir o espaço reservado para a pilha do modo SVC. O código do *kernel* e dos programas começa no endereço 0x8000, mas ao contrário da pilha do modo SVC, cresce para cima. Logo após o código, temos uma área reservada para os dados globais. Finalmente, as pilhas do modo *user* começam no endereço 0x20000 e crescem para baixo. Cada uma tem um *offset* relativo à anterior de 4048 bytes.

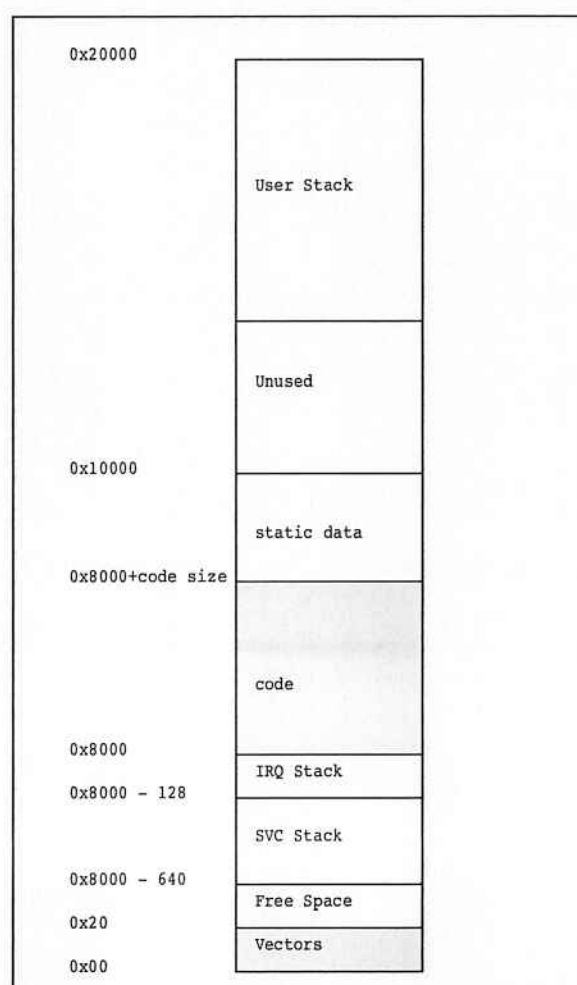


Figura 3.4: Estrutura da memória. Fonte: (SLOSS, 2001)

3.3.2 Modos do processador

Dentre os sete modos do processador, apenas quatro deles são utilizados: o modo de usuário (*user*), o modo de serviço (SVC), o modo de sistema (SYS) e o modo de interrupção (IRQ). O primeiro é o modo não privilegiado no qual as *threads* são executadas. O segundo, é o modo de inicialização do *kernel* e de execução das chamadas de sistema, que é privilegiado. Já o terceiro, é idêntico ao modo de usuário, mas com privilégios. Ele é utilizado na inicialização do

sistema para definir a pilha do modo de usuário. Finalmente, o quarto é um modo que também é privilegiado, mas que é usado quando há interrupções de *hardware* e portanto, é usado quando há o chaveamento de *threads* (interrupção de *timer*) ou qualquer outra interrupção que não a de *software*. É importante ressaltar que os modos privilegiados quando chamados por interrupção desabilitam outras interrupções. Isso bloqueia interrupções aninhadas, essencial para o funcionamento do código.

3.3.3 Modos de teste

Depurar o código com a placa não é possível em todas as situações. Quando o código que está sendo executado está dentro de uma região onde as interrupções estão desabilitadas, como no código de tratamento de interrupção, não se pode fazê-lo. Para contornar tal problema, foi utilizado o emulador disponível na IDE CodeWarrior, o ARMulator. Como ele foi desenvolvido para vários modelos de placa, utiliza endereços de periféricos diferentes da placa Evaluator 7-T e não têm o módulo Angel de *debug*. Para manter a compatibilidade entre o emulador e a placa nas partes onde o código se diferencia, como na inicialização do *timer*, foram colocados ambos os códigos. A seleção de qual dos dois será executado depende de uma variável global emulador, que é declarada no arquivo constants.h. Caso seja 1, o código executado é o do emulador, caso seja 0, o código da placa com Angel e caso seja 2, o código para a placa sem o Angel. Uma outra vantagem da utilização do emulador é que ele permite que o *microkernel* possa ser testado sem a presença da placa.

3.3.4 Angel

O Angel é um programa armazenado na ROM da placa que realiza a comunicação entre a mesma e o computador que efetuou o upload do código. Além de permitir com que o código seja carregado na placa, o Angel realiza o processo de *debug* do código durante a execução. Para isso, deve haver uma comunicação constante entre a placa e o computador, que é feita através de interrupções. Uma vez que a placa é iniciada, o endereço do vetor de interrupções responsável pelas interrupções de *hardware* e se *software* apontam para um endereço pré-estabelecido do Angel.

Caso se queira adicionar alguma outra rotina de tratamento de interrupções, como é o caso deste projeto, deve-se encadear o Angel (como será descrito na seção 3.4.5) quando a rotina instalada não consegue tratar a interrupção. Isto é necessário para que a comunicação com a placa não seja perdida.

3.4 Inicialização

O início do programa se dá no arquivo `statup.s`. Nele, são realizadas todas as operações necessárias em *assembly*, como a inicialização das pilhas ou a criação da tabela de *threads*. Após esta etapa, há a inicialização em C, feita no arquivo `cinit.c`, que inicializa periféricos, instala rotinas de tratamento e inicia a primeira *thread* em modo usuário. A rotina completa de inicialização pode ser vista no esquema da figura 3.5.



Figura 3.5: Fluxograma de inicialização.

3.4.1 Ponto de entrada e tipo de código

O ponto de entrada do código é indicado pela instrução `ENTRY`. Por padrão, o compilador assume que o código de entrada é ARM. Como descrito no item 2.1.3, há dois tipos de *assembly*, o ARM e o THUMB, onde o ARM é favorecido pelo número de instruções e pela legibilidade. Neste caso, será utilizado apenas código ARM.

3.4.2 Pilhas

Antes de poder utilizar as pilhas é preciso que elas sejam inicializadas em cada um dos modos que virão a ser utilizados. Neste *microkernel*, são utilizados os modos SVC, *user/system* e IRQ. O modo como isto é feito é descrito abaixo:

```
MOV    r0, #0xC0|0x12    ; r0 = 0xC0 or 0x12 (0xC0 = IRQ disabled, 0x12 =
                        IRQ mode)
MSR     CPSR_c, r0        ; status_register = r0
MOV     sp, #0x8000       ; stack pointer = 0x8000
```

A primeira instrução copia para r0 o valor que será substituído no registrador de estado. Neste exemplo, é desabilitada as interrupções e alterado o modo do processador para o modo IRQ. Em seguida, os dados do registrador r0 são colocados no registrador de estado CPSR. Uma vez que o estado foi alterado, pode-se mudar o ponteiro de pilha, que neste caso aponta para o endereço 0x8000. Uma operação semelhante pode ser feita tanto no modo SVC quanto no modo *user*, usando os endereços de pilha indicados na figura 3.4. Porém, se o estado for alterado para o modo *user* fica impossível de se alterar o estado novamente. Para se resolver este problema, ao invés de se mudar para o estado *user*, muda-se para o estado SYS. Este é semelhante ao modo *user* (usa a mesma pilha e registradores), mas permite a alteração de modo por ser privilegiado.

3.4.3 Vetor de threads e número da thread

O outro ponto importante da inicialização do código em *assembly* é a criação do vetor de *threads*. Para tal, tem de se definir que todos as *threads* exceto a primeira são inicialmente desabilitadas. Isto é feito com o código apresentado a seguir:

```
; Initializes the thread array with zeros (0 = thread disabled,
; 1 = thread enabled)
LDR    r0, =thread_array    ; r0 = thread_array start address
MOV     r1, #1              ; r1 = 1
STR     r1, [r0]            ; address(r0) = r1
MOV     r1, #0              ; r1 = 0 (disabled)
MOV     r2, #0              ; r2 = 0
init_thread_array_loop
ADD     r2, r2, #4           ; r2 = r2 + 4
CMP     r2, #36             ; r2 = 36?
BEQ     set_active_thread    ; if yes, go to set_active_thread
ADD     r3, r0, r2           ; r3 = r0 + r2
STR     r1, [r3]            ; address(r3) = r1
```

```
B    init_thread_array_loop    ; return to init_thread_array_2
```

Nele, *r0* armazena a base do vetor, que coincide com o espaço relativo à primeira *thread*. *r1* contém o dado que será colocado na posição de memória. Na posição 1 este valor é 1, e nos demais 0. *r2* contém o *offset* que será somado à base para o cálculo do endereço absoluto, armazenado em *r3*. O algoritmo funciona inicialmente colocando 1 na base. Após isso, entra em um *loop* que aumenta o *offset* de 4 em 4 e coloca 0 em todos os outros espaços.

Ainda na inicialização em *assembly*, deve-se definir o número da *thread* que está sendo executada. Este dado é armazenado na variável *current_thread_id*. Pode-se ver abaixo como é definido o id da primeira *thread* para 1:

```
LDR    r0, =current_thread_id    ; r0 = current thread id address
MOV     r1, #1                    ; r1 = 1
STR     r1, [r0]                  ; current thread id = 1
```

Finalmente, a inicialização em C pode ser iniciada. A chamada é feita definindo como endereço de retorno a função *C_entry* e colocando este mesmo endereço no *process counter*.

```
LDR    lr, =C_Entry              ; link register = C entry
MOV     pc, lr                   ; process counter = C entry
```

3.4.4 Periféricos

Para alguns periférico da placa, como o *display* de sete segmentos, o *timer* e os botões, há uma rotina de inicialização que os habilita e define suas configurações. Suas chamadas são *segment_init()*, *timer_init()* e *button_init()* respectivamente. Estas funções se encontram nos arquivos de cada um dos periféricos e são executadas logo no início da etapa C do processo de inicialização da placa.

3.4.5 Instalação do tratamento de interrupção

Como descrito anteriormente na seção 2.1.7, caso uma interrupção de *hardware* ocorra, a instrução no endereço 0x18 é executada e caso seja uma interrupção de *software*, a instrução no endereço 0x08. Toda vez que se reinicia a placa, são colocados nestes endereços uma instrução que realiza um desvio para a rotina Angel (vide seção 3.3.4).

Porém, se algum dos periféricos vai ser utilizado, a interrupção gerada por esse periférico não deve desviada para o Angel, e sim para uma rotina adequada que trate tal periférico. Para

poder identificar qual a origem da interrupção e desviar para a rotina correta, deve-se instalar uma nova rotina no vetor de interrupções, substituindo o desvio para o Angel. A instalação da rotina dá-se através do desvio para a tal rotina. Todavia, não se pode apenas descartar o endereço do Angel, já que caso não se identifique a origem da interrupção, ainda deve-se desviar para ele. Este processo pode ser observado na figura 3.6. Nele, Handler2 é a rotina de tratamento de interrupções, e Handler1 é o Angel.

A instalação da rotina de tratamento de interrupção é a mesma para interrupções de *hardware* e de *software* conforme mostrado abaixo:

```
/* Angel branch instruction */
unsigned Angel_branch_instruction;
/* Angel instruction */
unsigned *Angel_address;
/* Getting Angel branch instruction */
Angel_branch_instruction = *vector_address;
/* Separate the instruction from the address */
Angel_branch_instruction ^= 0xe59ff000;
/* Calculating absolute address */
Angel_address = (unsigned *) ((unsigned)vector_address +
    Angel_branch_instruction + 0x8);
/* Store address in the proper position */
if ((unsigned)vector_address == 0x18) {
    Angel_IRQ_Address = *Angel_address;
}
else {
    Angel_SWI_Address = *Angel_address;
}
/* Inserting handler instruction in the vector table */
*Angel_address = handler_routine_address;
```

Os parâmetros de entrada desta função são *handler_routine_address*, o endereço da rotina de tratamento de interrupção e *vector_address*, um ponteiro para a posição no vetor de interrupções onde será instalada a rotina. Sucintamente, o que esta rotina realiza é obter a instrução que está em *vector_address*, aplica uma máscara à rotina para obter apenas o endereço e o salva em uma das variáveis: *Angel_IRQ_Address* caso se esteja instalando a rotina de interrupção de *hardware* ou *Angel_SWI_Address* caso seja a de *software*, além de colocar a nova instrução no vetor de interrupções.

Um fator importante que deve ser ressaltado é a importância do Angel quando se está usando a placa. Como já descrito anteriormente, o Angel se utiliza das interrupções de *hard-*

ware e *software* para se comunicar com a placa. Portanto, se o código for apenas modificado e a instrução que está contida no vetor de interrupção for substituída, essa comunicação não se realiza e tanto a placa quanto o programa *debugger* travam. Para se solucionar este problema, deve-se passar para a rotina de tratamento de interrupção os endereços que estavam anteriormente no vetor de interrupção, para o caso da interrupção ser do Angel, a rotina correta ser executada. Já no caso em que o código é apenas simulado no emulador, não é preciso armazenar o endereço do Angel.

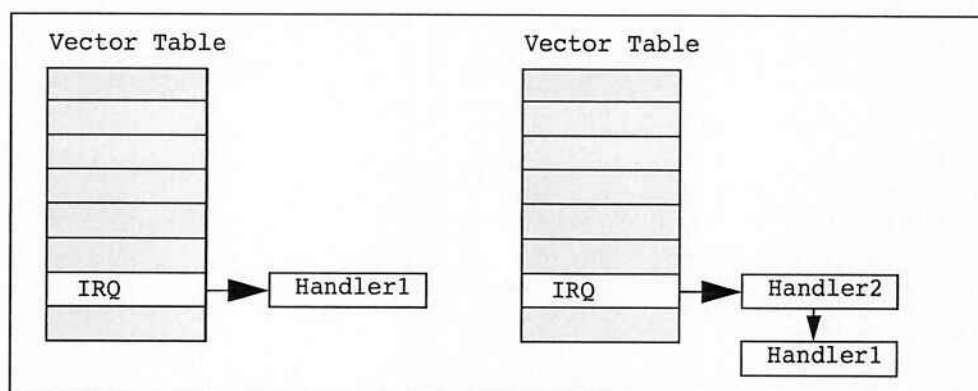


Figura 3.6: Encadeamento de interrupções. Fonte: (SLOSS, 2001)

3.4.6 Interrupção de timer

A interrupção de *timer* é utilizada neste projeto para realizar o chaveamento entre as *threads*. Uma vez que haja a interrupção, o estado da *thread* atual é salva e a próxima é colocada em processamento. Para utilizá-la, deve-se tanto habilitar quanto iniciar o *timer*. Essas tarefas são executadas com duas rotinas, sendo que a primeira já foi descrita no item 3.4.4. Já o início do *timer* é dado pela função `timer_start()`.

3.4.7 Habilitando interrupções

O último passo antes de se começar a executar o código do primeiro programa é habilitar simultaneamente o modo de usuário e as interrupções. Como isso só pode ser feito por código *assembly*, é utilizado a instrução especial de C `__asm`, conforme o exemplo abaixo

```

__asm {
    MOV    r1, #0x40|0x10
    MSR    CPSR_c, r1
}
  
```

O registrador r1 recebe 0x40, que indica a habilitação das interrupções e 0x10 que altera para o modo *user*. Logo em seguida, o conteúdo deste registrador é passado para o registrador de estado. Finalmente, o primeiro programa é chamado com a função `shell()`.

3.5 Chaveamento de threads

O chaveamento de *threads* é realizado inteiramente com o *assembly* escrito no arquivo `handler_irq.s`. Ele consiste em sete passos, indicados na figura 3.7.

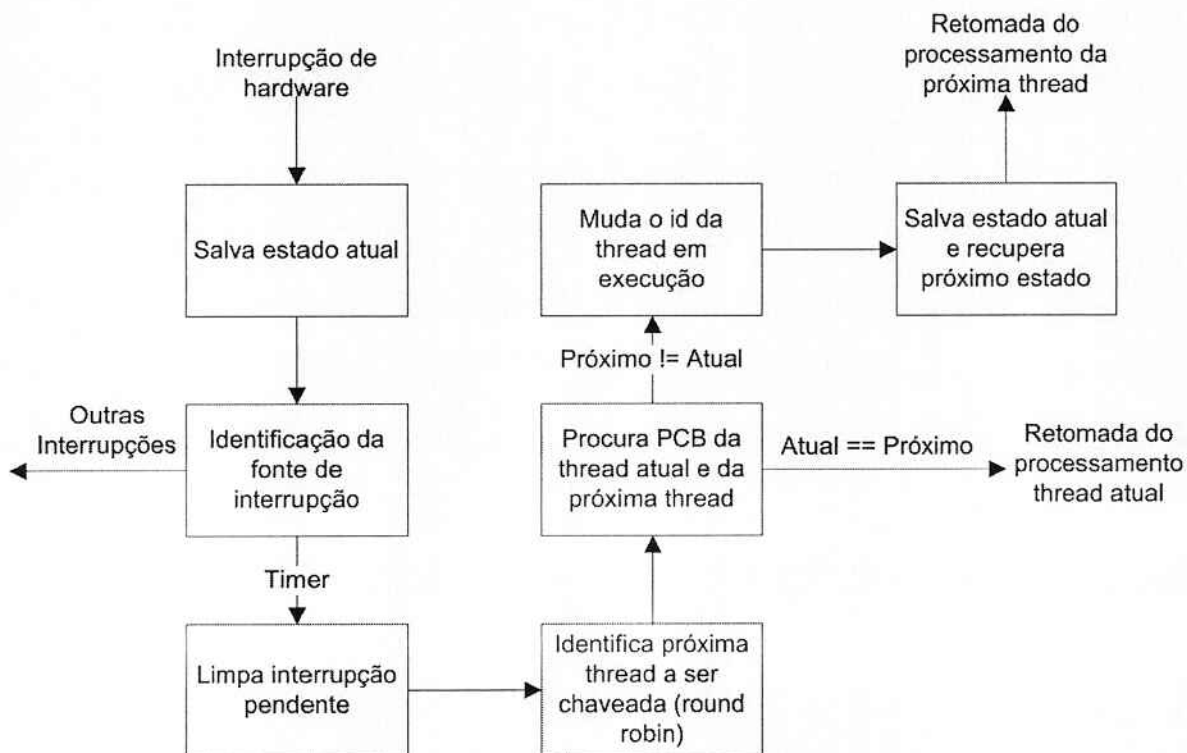


Figura 3.7: Chaveamento de *threads*.

3.5.1 Identificação da interrupção

```

STMFD sp!, {r0 - r3, lr}    ; Stacking r0 to r3 and the link register
LDR  r0, IRQStatus          ; r0 = irq type address
LDR  r0, [r0]                ; r0 = irq type
TST  r0, #0x0400             ; irq type == 0x0400?
BNE  handler_timer           ; If yes, go to handler_timer
TST  r0, #0x0001             ; irq type = 0x0001?
BNE  handler_button          ; If yes, go to handler_button

```

```

LDMFD sp!, {r0 - r3, lr}    ; If it is not any of them, restore r0-r3 and
                             lr
LDR    pc, Angel_IRQ_Address ; and branch to the Angel routine

```

Uma vez que há a interrupção de *timer*, a chamada de interrupção de *hardware* que se encontra no vetor de interrupção é executada. Durante a instalação da rotina de tratamento de interrupção de *hardware*, colocou-se nesta posição a rotina `handler_board_angel` caso se estivesse usando a placa com o Angel, a rotina `handler_board_no_angel` caso se estivesse usando a placa sem o Angel ou a rotina `handler_emulator` caso estivesse usando o emulador. A diferença é que enquanto a primeira e a segunda tentam identificar qual a fonte de interrupção, a terceira já assume que a fonte é o *timer*, já que não há outros periféricos no emulador. Deve-se armazenar toda informação contida nos registradores que são alterados durante o processo de tratamento de interrupção. Para tal, empilha-se os valores dos registradores r0 a r3, usados durante a rotina de chaveamento, a fim de que nenhum dado se perca durante o processo.

No caso do uso da placa, a fonte da interrupção se encontra no endereço 0x03ff4004, identificado com a variável `INTPND`. Se o valor contido neste endereço é 0x0400, a fonte foi uma interrupção de *timer*, caso seja 0x0001, a fonte foi o botão da placa e caso contrário, a fonte foi o Angel. No primeiro caso, há um desvio para a rotina `handler_timer`, no segundo para a rotina `handler_button` e na terceira, para o endereço salvo durante a instalação de rotina de tratamento.

3.5.2 Limpeza da interrupção de timer

Quando é identificada a interrupção de *timer*, deve-se limpar a interrupção de *timer*, a fim de que ele possa interromper novamente no futuro. Para tal, executa-se a rotina `timer_irq`, encontrada no arquivo `timer.c`. Como não se pode garantir que a rotina em C manterá intactos os registradores, há de se salvar todos e recuperá-los após a chamada. Abaixo pode-se observar o código que realiza o salvamento e a recuperação destes registradores.

```

STMFD sp!, {r4 - r12}    ; Stack the rest of the registers (r4-r12)
BL    timer_irq           ; Clear timer interruption
LDMFD sp!, {r4 - r12}    ; Load r4-12 registers again

```

Os registradores r0 a r3 não precisam ser salvos ou recuperados, pois no início da rotina de tratamento eles já foram empilhados para recuperação futura.

3.5.3 Identificação da próxima thread

O método de escolha da próxima *thread* que será posta em execução é escolhida pelo método *round-robin*, ou seja, a próxima *thread* é escolhida por ordem numérica. O código para tal tarefa é apresentado abaixo:

```

CMP    r0, #9          ; r0 == 9? (it is the last thread?)
BEQ    last_thread     ; If yes, branch last_thread
ADD    r1, r0, #1      ; If not, r1 = r0 + 1
B      next_thread     ; and branch to next_thread
last_thread
MOV    r1, #1          ; r1 = 1
next_thread
SUB    r2, r1, #1      ; r2 = r1 - 1
MOV    r3, #4          ; r3 = 4
MUL    r2, r3, r2      ; r2 = r2 * r3
LDR    r3, =thread_array ; r3 = thread_array bottom address
ADD    r2, r2, r3      ; r2 = r3 + r2
LDR    r2, [r2]        ; r2 = thread array content
CMP    r2, #1          ; thread array content == 1?
BEQ    set_addresses   ; If yes, branch to set_addresses
                        ; Send to the next step the next active
                        ; thread in r1
MOV    r0, r1          ; If not, r0 = r1
B      get_next_taskid_loop ; and loop to get_next_taskid_loop

```

Nele, *r0* inicia com o número da *thread* atual. Caso ele seja igual a 9, a última *thread* da lista, deve-se iniciar novamente a procura desde a *thread* 1. Caso contrário, inicia-se com o próximo número. O resultado é armazenado em *r1*, onde se encontra o número da próxima *thread*. O valor em *r1* é incrementado sucessivamente até encontrar um ponto no vetor de *threads* que tenha o valor 0, indicando que a *thread* não está ativa. O cálculo da posição de memória é dado a partir da seguinte função: $(r1 - 1) \cdot 4 + \text{bottom} = \text{posição relativa à thread } r1$, onde *bottom* é o endereço do início do vetor e 4 é o tamanho de cada espaço dentro do vetor.

3.5.4 Localização dos PCBs

A rotina de troca de *threads* tem como entrada duas variáveis: o PCB da *thread* atual e o PCB do próxima *thread*. Para obter tais dados, é necessário o número de ambas. Como visto nos itens anteriores, estes dados já foram obtidos. Pode-se então aplicar o seguinte algoritmo:

```

LDR  r2, =current_thread_id    ; r2 = current thread id address
LDR  r2, [r2]                  ; r2 = current thread id
CMP  r2, r1                    ; Is r2 = current thread id ==
                                ; next thread id
BEQ  no_thread_switch          ; If yes, branch to no_thread_switch
; Setting current_task_addr
MOV  r0, #68                   ; Else start thread switch. r0 = 68
MUL  r0, r2, r0                ; r0 = current thread id * 68
LDR  r2, =process_control_block ; r2 = PCB bottom
ADD  r0, r0, r2                ; r0 = PCB bottom + id * 68
LDR  r2, =current_task_addr     ; r2 = current task addr addr
STR  r0, [r2]                  ; current_task_addr = r0
; Setting next_task_addr
MOV  r0, #68                   ; r0 = 68
MUL  r0, r1, r0                ; r0 = next thread id * 68
LDR  r2, =process_control_block ; r2 = PCB_bottom
ADD  r0, r2, r0                ; r0 = PCB bottom + next id * 68
LDR  r2, =next_task_addr        ; r2 = next_task_addr addr
STR  r0, [r2]                  ; next_task_addr = r0

```

O primeiro ponto checado é se a *thread* atual é igual à *thread* que vai ser substituída. Caso isso se confirme, o chaveamento se encerra e nada ocorre. Caso contrário, o cálculo dos endereços dos PCBs é iniciado. A fórmula utilizada é: $PCB_{id} = (id - 1) \cdot 68 + base$, onde *id* é o número da *thread* e *base* é o endereço do início dos PCBs. Ao fim do cálculo, estes dados são armazenados nas variáveis *current_task_addr* e *next_task_addr*, que serão utilizadas na próxima etapa do processo.

3.5.5 A troca de threads

A troca de *threads* se dá em poucos passos usando-se instruções especiais que permitem que haja um grande número de dados empilhados/desempilhados com apenas uma instrução. Inicialmente zera-se a pilha do modo de interrupção e restabelece-se os registradores *r0* a *r3*, que estavam empilhados desde o início da rotina de tratamento. Nota-se que o ponteiro não é totalmente zerado, ele é colocado em uma posição 20 bytes acima do esperado. Isto se dá porque há empilhadas 5 palavras (*r0* a *r3* e o *link register*) que logo em seguida virão a ser desempilhadas.

Depois disso, muda-se o endereço do ponteiro de pilha para o PCB da *thread* atual. Um truque vem no próximo passo: empilha-se todos os registradores com o ponteiro de pilha

apontando para a posição (base - 60) do PCB. Deste modo, em uma única instrução todos os registradores são colocados em suas respectivas posições. Como a estrutura do PCB foi feita tendo este processo em mente, a posição dos dados dos registradores cai exatamente como foi descrito na figura 3.2. Após o armazenamento do estado atual, muda-se novamente o endereço do ponteiro de pilha para o PCB da próxima instrução. Do mesmo modo que o armazenamento, desempilha-se os o valor dos registradores, que são exatamente como estava empilhado este processo quando foi armazenado.

```
; Reset and save IRQ stack
LDR  r0, =irq_stack_pointer    ; r0 = irq_stack_pointer addr
MOV  r1, sp                    ; r1 = irq stack pointer
ADD  r1, r1, #5*4              ; r1 = irq stack pointer + 5 (# of data in
                                ; the stack, r0-r3, lr) * 4 (size of a word)
STR  r1, [r0]                  ; irq_stack_pointer = irq stack pointer
                                ; without the data that will be removed next
LDMFD sp!, {r0-r3, lr}        ; Restore the remaining registers
; Load and position r13 to point into current PCB
LDR  r13, =current_task_addr   ; r13 = current task PCB bottom address
                                address
LDR  r13, [r13]                ; r13 = current task PCB bottom address
SUB  r13, r13, #60              ; r13 = current task PCB bottom address - 60
                                ; to point to the right place for the stacking
                                ; (next step)
; Store the current user registers in current PCB
STMIA r13, {r0-r14}^           ; Stacks the r0-r14 registers in the PCB
MRS  r0, SPSR                  ; r0 = status register
STMDB r13, {r0, r14}           ; Stacks r0 and r14
; Load and position r13 to point into next PCB
LDR  r13, =next_task_addr      ; r13 = next task PCB bottom address
                                address
LDR  r13, [r13]                ; r13 = next task PCB bottom address
SUB  r13, r13, #60              ; r13 = next task PCB bottom address - 60
                                ; to point to the right place for the stacking
                                ; (next step)
; Load the next task and setup PSR
LDMNEDB r13, {r0, r14}         ; Restore r0 and r14 (IRQ mode)
MSRNE spsr_cxsf, r0            ; Restore status register
LDMNEIA r13, {r0-r14}^         ; Restore r0-r14 for the user mode
NOP                               ; NOP! (required for the above instruction)
; Load the IRQ stack into r13_irq
LDR  r13, =irq_stack_pointer   ; r13 = stack pointer address address
LDR  r13, [r13]                ; Restore previous stack pointer
```



```

STMFD  sp!,{r0-r12,lr}      ; Stack registers r0-12 and link register
LDR    r0,[lr,#-4]          ; Calculate address of SWI instruction (r0 = lr-4)
BIC    r0,r0,#0xff000000    ; Mask off top 8 bits of instruction to give SWI
                                ; number
LDR    r1, Angel_SWI_Number ; r1 = Angel SWI Number
CMP    r0, r1               ; Compare SWI number to angel interrupt number
BEQ    goto_angel           ; If it is angel interrupt, branch to goto_angel
MOV    r1, #0               ; r1 = 0
CMP    r0, r1               ; Compare SWI number to r1
BEQ    os_swi               ; If it is OS SWI, branch to os_swi

```

Novamente há uma rotina de identificação da fonte de interrupção, que pode vir a ser uma do sistema operacional, ou do Angel. O primeiro passo desta rotina é o empilhamento de todos os registradores, para poder futuramente restaurar o estado atual. Em seguida, ocorre a identificação em si, onde uma máscara de bits é aplicada para se obter o identificador da interrupção. Caso ela seja Angel_SWI_Number (0x0123456), o estado do processador é restaurado e há um desvio para a instrução previamente armazenada durante a instalação. Caso seja 0, o valor estabelecido para o sistema, há um desvio para outro código que identifica quais das chamadas de sistema foi ativada.

Esta nova identificação pode ser observada abaixo. O primeiro passo é restaurar e armazenar novamente os valores dos registradores, já que na arquitetura ARM os valores passados pelos parâmetros de uma função são passados nos primeiros registradores. Neste caso, r1 contém o tipo da chamada. Dependendo de qual for o valor, há desvios para `pre_routine_fork`, `pre_routine_exec` e `pre_routine_exit`.

```

LDMFD  sp!,{r0-r12,lr}      ; Restore r0-r12 registers and link registers
STMFD  sp!,{r0-r12,lr}      ; and stores them again (in order to clean the
                                registers)
MOV    r1, #0               ; r1 = 0
CMP    r0, r1               ; Compare the first parameter to 0
BEQ    pre_routine_fork     ; If it is equal, branch to the fork
MOV    r1, #1               ; r1 = 1
CMP    r0, r1               ; Compare the first parameter to 1
BEQ    pre_routine_exec     ; If it is equal, branch to the exec
MOV    r1, #2               ; r1 = 2
CMP    r0, r1               ; Compare the first parameter to 2
BEQ    pre_routine_exit     ; If it is equal, branch to the exit
LDMFD  sp!,{r0-r12,pc}^     ; If it is an unidentified syscall, go back to the
                                program,
                                ; restoring the registers and putting the return address in

```

; the process counter

3.6.2 fork

Em um sistema operacional, a chamada de sistema `fork` é responsável pela criação de novos processos. Para tal, ela duplica o processo que a invocou, e retorna o identificador do processo. Este identificador é o único meio de se identificar qual o processo pai e qual é o filho. Caso o número de retorno seja 0, significa que este é o processo filho, e caso seja qualquer outro número, é o processo pai que retornou o identificador do processo filho.

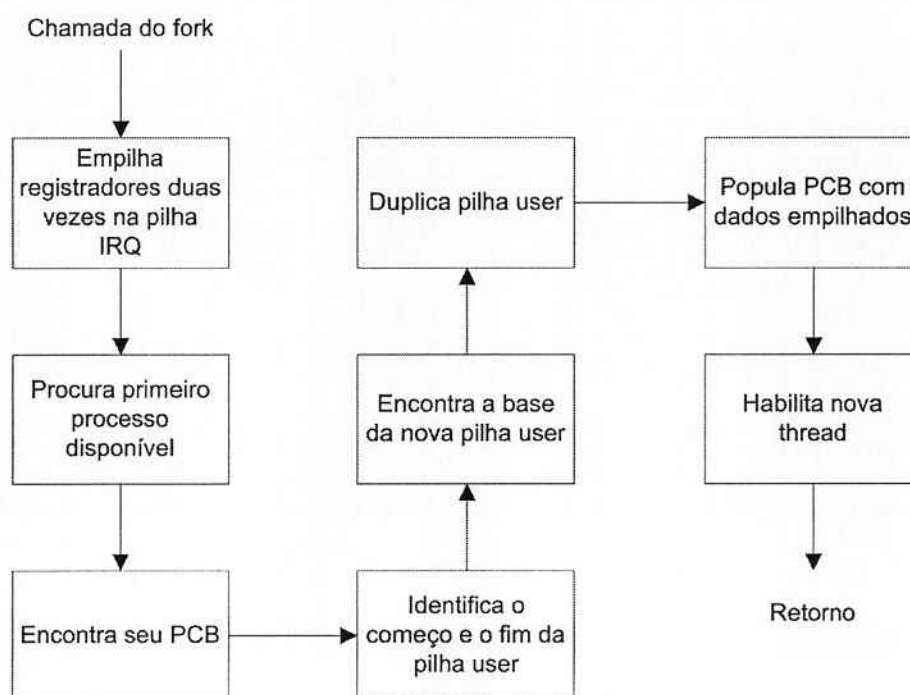


Figura 3.8: Fluxo de funcionamento do `fork`.

O processo de duplicação de uma *thread* se inicia com o empilhamento dos registradores de dados (`r0` a `r12`) e do endereço de retorno (*link register*) por duas vezes, como pode ser visto abaixo. O motivo é que o primeiro empilhamento serve para a restauração do estado ao fim do processo de duplicação e a segunda para a nova cópia da *thread*, como será visto mais à frente.

```

STMFD    sp!,{r1-r12,lr}    ; Stacks the link register and r1-r12
STMFD    sp!,{r0-r12}       ; Stacks r0-r12
STMFD    sp!,{lr}           ; Stacks the link register (In a separate instruction
                             ; to stack it in the top)
  
```

Em segundo lugar, procura-se o primeiro espaço disponível no vetor de *threads*, o que

indica qual dos PCBs está livre. Na rotina apresentada abaixo, *r0* contém o id da posição sendo procurada e *r1* seu endereço. O *loop* é feito verificando de posição em posição, um ponto onde o valor seja 0. Caso se encontre, passa-se ao próximo passo, ao contrário, soma-se 1 ao número da *thread* e 4 no endereço do vetor.

```

LDR    r1, =thread_array ; r1 = bottom of the thread array address
MOV    r0, #1             ; r0 = 1
routine_fork_loop
LDR    r2, [r1]           ; r2 = thread array position
CMP    r2, #0             ; r2 = 0?
BEQ    pcb_bottom        ; If the position is available (r2 = 0), go to
    pcb_bottom
ADD    r0, r0, #1         ; r0 = r0 + 1 (next id)
CMP    r0, #9             ; Is this the last thread slot being checked?
BEQ    fork_fail         ; if it is, there is no available slot, go to
    fork_fail
ADD    r1, r1, #4         ; r1 = r1 + 4 (next address)
B      routine_fork_loop ; Check next slot (go to routine_fork_loop)

```

Calcula-se então o endereço do PCB da *thread* encontrada. A fórmula, já vista anteriormente, é $PCB = id \cdot 68$

Para se realizar a cópia da pilha de *user*, há de se obter três informações: a base e o ponteiro da pilha original e a base da nova pilha. O ponteiro é obtido apenas copiando-se o valor do ponteiro de pilha do modo *user*. As bases são calculadas a partir da equação $0x20000 - (id - 1) \cdot 4048$, onde $0x20000$ é onde começa a área reservada às pilhas do modo *user*, *id* é o número da *thread* cuja base deseja-se obter e 4048 é o tamanho do espaço reservado para cada pilha.

Com os dados obtidos no passo anterior, pode-se usar a rotina a seguir para se duplicar a pilha:

```

LDR    r6, [r4]           ; r6 = original stack data
STR    r6, [r5]           ; Stores data in new stack (stack_top = r6)
CMP    r4, r3             ; Is this the top of the stack? (r4 == r3?)
BEQ    build_new_pcb      ; if it is, branch to build_new_pcb
SUB    r5, r5, #4         ; if not, go to next space in the new stack (r5 = r5
    - 4)
SUB    r4, r4, #4         ; and next data in the original stack (r4 = r4 - 4)
B      loop_stack_copy    ; restart sequence (go to loop_stack_copy)

```

O registrador *r6* serve como memória intermediária para a cópia. *r4* contém o endereço

que está sendo copiado, e é incrementado de 4 em 4 até chegar ao seu topo, enquanto r5 guarda o endereço equivalente da nova pilha, que também é incrementado de 4 em 4.

Finalmente, se começa a construir o novo PCB. Na posição que guarda o registrador de estado, guarda-se o valor 0x10, que indica que a *thread* deve ser iniciada em modo *user*. O ponteiro de pilha foi obtido no passo anterior, vindo no registrador r5. Tanto o endereço de retorno do modo *user* quanto o do modo *IRQ* são o mesmo, e coloca-se o endereço inicial da rotina que se quer executar. A cópia dos valores dos registradores r0 a r12 se dá através de um *loop*, como pode-se observar abaixo.

```
; Copy registers
MOV    r3, #0      ; r3 = 0
MOV    r4, #12     ; r4 = 12
registers_loop
ADD    r2, r2, #4   ; r2 = r2 + 4 (Next PCB register space)
LDMFD  sp!, {r5}   ; Restore register from the stack to r5
STR    r5, [r2]     ; Store register in the PCB
CMP    r3, r4       ; r12 was copied? (r3 == r4?)
BEQ    enable_thread ; If yes, go to enable_thread
ADD    r3, r3, #1   ; r3 = r3 + 1 (Next register)
B      registers_loop ; Copy next register
```

r2 contém o endereço do PCB onde os dados serão colocados, r5 funciona como intermediária entre a pilha e a memória, r4 contém o valor final da iteração e r3 o *id* do registrador sendo copiado.

O último passo antes de se retornar à execução do programa é a habilitação do programa no vetor de *threads*.

3.6.3 exec

A chamada de sistema *exec* é responsável por substituir a imagem núcleo de um processo pela imagem do programa passado como argumento (TANENBAUM; WOODHULL, 2006).

Nos sistemas operacionais tradicionais, como o Linux ou o Minix, o *exec* é utilizado para iniciar um novo programa no mesmo ambiente do programa que executa a chamada de sistema. Normalmente o *exec* é utilizado na criação de um novo processo da seguinte maneira: um processo já existente se duplica através da chamada de sistema *fork*. O processo filho tem, então, seu código substituído pelo código que deve ser executado através da chamada de sistema *exec*, que permite ao processo filho assumir seu próprio conteúdo, apagando de si o

conteúdo do processo pai.

No KinOS, para que um *thread* passe a executar outro programa, é necessário reinicializar o seu PCB, isso é feito pela chamada de sistema *exec*.

Existem 4 principais entradas do PCB que necessitam ser reinicializadas:

- o *program counter* (PC - R13);
- o *link register* (LR - R14);
- o *stack pointer* (SP - R15);
- e o *saved processor status register* (SPSR).

Para reinicializar essas entradas, de forma que a *thread* passe à executar um novo programa, primeiro é necessário calcular o início do PCB da *thread* correspondente.

A rotina *exec*, recebe como parâmetros o id da *thread* que será alterada e o ponteiro para a função/programa que pretende-se executar, como mostrado a seguir:

```
void exec(int process_id, pt2Task process_addr);
```

Assim para calcular o endereço inicial do PCB, obtêm-se o endereço inicial da área reservada para armazenar todos os PCBs, a **process_control_block**, e adiciona-se à esta o valor de 68 multiplicado por **process_id**, visto que cada PCB ocupa um espaço de 68 endereços de memória como mencionado na sessão 3.2.1. O código responsável por calcular o PCB é apresentado a baixo:

```
LDR r3, =process_control_block ; r3 = the start address of the PCB area
MOV r4, #68 ; r4 = 68 (space for each process in the PCB)
MUL r5, r1, r4 ; r5 = (task id) * 68
ADD r3, r3, r5 ; r3 = PCB start address + r5
```

Em seguida, calculado o endereço inicial do PCB, altera-se suas entradas da seguinte maneira:

- LR (PCB[-4]) e PC (PCB[-64]) recebem o endereço da primeira instrução do novo programa (**process_addr**).

```
PCB[-4] = process_addr;
PCB[-64] = process_addr;
```

- SP (PCB[-8]) recebe o endereço de início da pilha da *thread*, fazendo com que esta seja zerada. Para cada pilha de *thread*, 4048 bytes são reservados.

```
PCB[-8] = início da pilha do modo usuário - (4048 * thread id);
```

- SPSR (PCB[-68]) recebe 0x10, pois os programas devem rodar no modo usuário.

```
PCB[-68] = 0x10;
```

Finalmente, após alterar as entradas mostradas a cima, a *thread* começa a executar o novo programa.

3.6.4 exit

A chamada de sistema *exit* é responsável por finalizar um processo, liberando espaço de memória para a execução de um novo processo (TANENBAUM; WOODHULL, 2006).

No KinOS isso é realizado apenas colocando como desativado (igual à 0) o byte na lista de processos que corresponde a *thread* que se deseja finalizar.

Para isso a rotina *exit* recebe como parâmetro o id da *thread* a ser terminada.

```
void exit(int process_id);
```

3.7 Shell

Com o desenvolvimento do microkernel e de suas system calls, torna-se necessário o desenvolvimento de outro ramo do projeto, destinado a permitir a interação do usuário com o Sistema Operacional. Essa interação é feita por um editor de linha de comando, também conhecido por Shell.

Na inicialização do microkernel, o Shell é o primeiro processo criado no sistema. Desse momento em diante, cabe ao usuário solicitar a execução ou o término de outras *threads*. Além disso, o Shell permite a visualização das diferentes *threads* em execução no sistema.

3.7.1 Comunicação via terminal

O Shell, para fazer a interação com o usuário, utiliza a porta serial COM0 (de uso geral) conectada a uma segunda porta serial da máquina host. A porta COM1 (Debug) deve permanecer conectada, pois o Angel mantém comunicações através dela com o AXD (descrito na seção 2.3.2) durante a execução do KinOS, como ilustrado na figura 3.9.

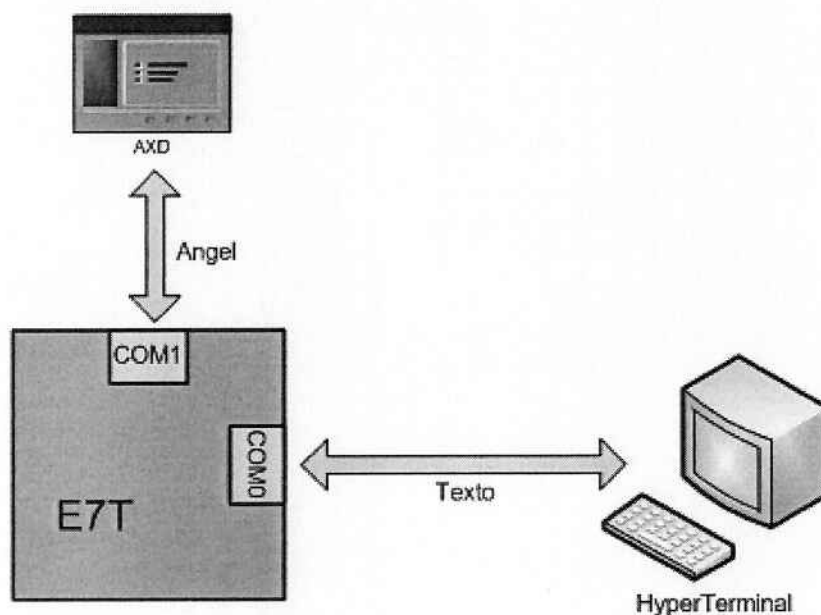


Figura 3.9: Comunicação da Evaluator-7T em cada porta serial.

3.7.2 Configuração e uso da COM0

Para utilizar a porta COM0 da Evaluator-7T, é preciso configurar um conjunto de registradores mapeados em memória relativos à UART0 do microcontrolador. A tabela 3.1 lista os registradores usados no projeto e suas respectivas funções.

Tabela 3.1: Registradores mapeados em memória da UART0 (SAMSUNG ELECTRONICS, 2007)

Registrador	Offset	R/W	Descrição
ULCON0	0xD000	R/W	Registrador de controle de linha
UCON0	0xD004	R/W	Registrador de controle
USTAT0	0xD008	R	Registrador de status
UTXBUF0	0xD00C	W	Registrador de buffer de transmissão
URXBUF0	0xD010	R	Registrador de buffer de recepção
UBRDIV0	0xD014	R/W	Registrador de divisor de taxa de transmissão

A coluna *offset* da tabela 3.1 indica o endereço de memória do registrador a partir do

endereço inicial, que é 0x03FF0000. Esse endereço é o do registrador SYSCFG, de configuração de sistema, o qual encabeça a lista dos registradores mapeados em memória.

Na inicialização da COM0, escreve-se nos registradores ULCON0, UCON0 e UBRDIV0. Os valores a serem colocados em cada um seus respectivos significados estão descritos na tabela 3.2.

Tabela 3.2: Registradores mapeados em memória da UART0 (SAMSUNG ELECTRONICS, 2007)

Registrador	Valor	Significado
ULCON0	0x03	8 bits de dados, 1 bit de parada, sem paridade, fonte de clock interna e modo de operação normal.
UCON0	0x09	Rx e Tx por requisição de interrupção, sem geração de interrupção por status de recepção, sem loop-back.
UBRDIV0	0xA20	Define a taxa de transmissão em 9600 bauds.

Inicializada a COM0, a transmissão de um caractere por ela é feita da seguinte maneira: observa-se o conteúdo do bit 6 de USTAT0. Quando este é igual a 1, significa que UTXBUF0 não contém dados válidos e, portanto, pode-se escrever nele o caractere que pretende-se enviar. Em seguida, coloca-se o caractere desejado em UTXBUF0. A lógica do controlador UART do microcontrolador se encarrega de enviar o dado para o terminal.

A recepção de caracteres é feita de forma similar: dessa vez, a verificação é feita no bit 5 de USTAT0, o qual é igual a 1 quando contém dados válidos recebidos pela porta serial. Quando isso acontece, copia-se o conteúdo de URXBUF0 para uma variável no programa do tipo *char*.

3.7.3 Funcionalidades do Shell

O editor de linha de comando do KinOS possui cinco funcionalidades básicas: listar *threads* ativas (*ps*), inicializar novas *threads* (*start*), encerrar *threads* ativas (*end*), listar as *threads* disponíveis. As sintaxes de cada comando são, respectivamente:

```
ps

start <nome da thread>

end <nome da thread>
```

listtasks

O comando *ps* utiliza o vetor de threads do sistema operacional para saber quais *threads* estão ativas. A partir daí, buscam-se as informações sobre cada *thread* ativa em seu respectivo PCB. Essas informações são, então, listadas ao usuário.

O comando *start* utiliza as system calls *fork* e *exec* para iniciar novas *threads* no sistema. O usuário deve fornecer o nome da *thread* como parâmetro do comando. Cada *thread* que pode ser disparada dentro do KinOS já está definida dentro do código-fonte, e cada um de seus nomes também já está definido.

O comando *end* é similar ao *start*. Dessa vez, o comando recebe o nome de uma *thread* ativa no sistema e utiliza a system call *exit* para encerrá-la.

O comando *listtasks* apresenta uma lista com o nome das *threads* disponíveis no sistema.

Além desses comandos, foi implementado o comando *help* que lista a sintaxe de todos os possíveis comandos da *shell*.

3.8 Mutex

O *mutex* ou exclusão mútua, é uma técnica usada para evitar que dois processos tenham acesso a um mesmo espaço de memória. Seu funcionamento é baseado em uma variável que pode ter apenas dois valores, 0 ou 1. Caso ela seja 0, ela indica que a área crítica pode ser acessada e 1 caso contrário. No caso de um processo não obter acesso, ele fica em espera ativa, até que o processo que o bloqueou o desfaça.

No exemplo que é dado no KinOS, tem-se duas funções que realizam o travamento e o destravamento do *mutex* e a variável *semaphore*, que guarda o valor do *mutex*. A primeira função se chama *mutex_gatelock*, que pode ser observada abaixo.

```
void mutex_gatelock (void) {
    __asm {
        spin:
        mov    r1, &semaphore
        mov    r2, #1
        swp    r3, r2, [r1]
        cmp    r3, #1
```

```

    beq    spin
}
}

```

r1 recebe o endereço da variável semaphore, e r2 recebe 1. A função atômica swp é que permite o correto funcionamento do *mutex*: em uma instrução indivisível, o conteúdo de semaphore é colocado em r3, e 1 é colocado em semaphore. Com isso, é impossível que haja uma interrupção entre estas duas ações, o que poderia arruinar uma rotina de *mutex*. Finalmente, caso semaphore já estivesse ativo quando chamado, a rotina seria executada novamente.

```

void mutex_gateunlock (void) {
    __asm {
        mov    r1 , &semaphore
        mov    r2 , #0
        swp    r0 , r2 , [ r1 ]
    }
}

```

O destravamento é feito de modo similar, com a mesma instrução. Só que neste caso, o valor 0 é colocado em semaphore.

Porém, as rotinas apresentadas não são chamadas diretamente. Usa-se as chamadas abaixo.

```

#define WAIT    while (semaphore==1) {} mutex_gatelock();
#define SIGNAL    mutex_gateunlock();

```

O motivo é que ao se usar o WAIT quando o *mutex* está ativo, faz com que o programa entre em uma espera ativa.

3.9 Threads

O *kernel* pode lidar com no máximo nove *threads*, contidas na pasta apps. Como eles não têm área de dados própria, não pode-se chamá-los de processos. A implicação de se ter uma área de dados em comum é que todos os processos que rodam um mesmo programa compartilham os valores das variáveis globais, mas não locais. O mais correto, portanto, seria chamá-las de *threads*.

Foram criados alguns programas exemplo que se utilizam dos periféricos da placa. Eles testam:

- O chaveamento de processos
- Os diversos periféricos da placa: LEDs, display de 7 segmentos, chave DIPs e o botão
- Comunicação da placa com um terminal
- A duplicação, criação e morte de um processo
- Rotina de exclusão mútua

3.10 Inspiração

Grande parte do código foi baseada do código presente nos exemplos incluídos no CD de demonstração da placa, desenvolvido por Andrew N. Sloss. O principal deles, é o código *mutex*, de onde foi baseado o chaveamento de processos, a função de mutex e as rotinas de manipulação de hardware. Eis a inspiração de cada uma das partes do projeto:

Chaveamento de processos O chaveamento de processos original, contido no projeto mutex era de apenas duas threads. Modificações foram realizadas para fazer com que o número de processos passasse de duas para nove.

Inicialização A inicialização foi baseada no código do mutex, mas grandes alterações foram feitas e pouquíssimas coisas ainda restam do código original

Shell O código foi baseado no exemplo da porta serial e também no Sistema Operacional ISOS (MEIGNAN, 2003).

Interrupção de hardware O código foi baseado no exemplo do mutex, mas grandes alterações foram realizadas

Interrupção de software Foi baseado no exemplo SWI, também contido no CD da placa

Rotinas de manipulação de periféricos As rotinas foram praticamente copiadas do código do mutex, que utiliza todas elas

Chamadas de sistema Todas as chamadas de sistema foram inteiramente desenvolvidas durante o projeto

Mutex O código do mutex foi inteiramente copiado do exemplo com o mesmo nome

3.11 Avanços Finais

Após a primeira revisão da monografia, algumas modificações foram realizadas para o término do sistema.

3.11.1 Shell

Novos comandos foram adicionados:

- `start <name> [<arg>]` : inicializa a *thread* com o parâmetro passado em `<arg>`. O parâmetro deve ser um número em hexadecimal de 0 à F.
- `end pid <num>` : finaliza a *thread* pelo número de seu pid (de 2 à 9). Não é possível finalizar o *shell*.
- `end all` : finaliza todas as *threads* ativas, menos o *shell*.

Além disso, uma estrutura, **pid_name**, foi criada no arquivo **terminal.c** para que fosse possível relacionar o nome de uma *thread* com o seu pid.

E no arquivo **tasks.c**, criou-se a estrutura **name_address** para relacionar o nome de todas as *threads* disponíveis do sistema e seus respectivos ponteiros de função. Assim, para adicionar uma nova *thread* é necessário criar uma nova entrada nessa estrutura para que o nome da *thread* passe à figurar na lista apresentada pelo comando *listtasks*, podendo-se então inicializá-la normalmente pelo comando *start*.

3.11.2 Threads

Para guardar o ponteiro de função de uma *thread* na estrutura **name_address**, citada do item anterior, esta deve possuir a seguinte assinatura:

```
void <nome_da_thread>(int <value>);
```

Ou seja, toda *thread* do sistema consiste de uma função do tipo *void* que tem como argumento um valor do tipo inteiro.

Deste modo, foram criadas 8 *threads* para exemplificar o funcionamento do *microkernel*:

- **display_pid**: Apresenta no display de 7 segmentos o pid da *thread*.
- **set_led**: Acende os leds conforme o valor em hexadecimal passado em argumento.
- **set_segment**: Coloca o valor passado em argumento no display.
- **mutex_test**: Exemplo de mutex. Acende o led passado em argumento (1 à 4) e coloca no display o pid da *thread*.
- **fork_test**: Imprime na tela o valor do pid da *thread* filha retornado pelo *fork* para a *thread* mãe.
- **dips_to_leds**: Acende os leds conforme o valor apresentados nos *switches* da placa.
- **dips_to_segments**: Coloca no display o valor apresentados nos *switches* da placa.
- **malicious_handler**: Altera o vetor de interrupção para apontar para um rotina maliciosa. Ao executar essa *thread* o sistema é bloqueado, devendo-se então reinicializar o mesmo.
- **tictactoe**: Jogo da velha que utiliza o terminal para a entrada dos comandos.

3.11.3 Mutex

A rotina descrita no item 3.8 foi utilizada em duas rotinas. A primeira, chamada de *mutex_test*, acende e apaga um led. Caso o led esteja aceso, o mutex está habilitado. Ao se iniciar uma outra *thread* com o mesmo código, percebe-se que os dois leds não acendem ao mesmo tempo.

Outro uso do mutex é no programa tictactoe, que concorre com o shell no uso da porta serial e da tela. Para tal, força-se uma troca de threads com a chamada de sistema `switch_thread` (descrita abaixo) e habilita-se a exclusão mútua de código entre o shell e o tictactoe.

3.11.4 Chamadas de sistema

Para o melhor funcionamento do terminal, duas novas chamadas de sistema foram criadas.

3.11.4.1 print

Chamada quando se deseja imprimir uma seqüência de caracteres completa (linha) no terminal. Como as chamadas de sistema são executadas em modo privilegiado, outras interrupções são desabilitadas, permitindo com que nada interrompa a rotina até sua finalização.

3.11.4.2 switch_thread

Chamada de sistema criada para forçar o chaveamento de threads. Ao ser chamada, simula uma interrupção de timer, fazendo com que se chaveie para a próxima thread e com que o timer seja reinicializado. É um artifício utilizado para que se force que o mutex da próxima thread seja inicializado antes do mutex da thread atual.

4 CONSIDERAÇÕES FINAIS

4.1 Conclusão

Através deste projeto de formatura foi possível desenvolver, como previsto, um *microkernel* simples para a placa ARM Evaluator-7T.

O KinOS é um *microkernel* que implementa, de maneira didática, os mecanismos básicos de um sistema operacional, como: chaveamento de threads, chamadas de sistema e rotinas de comunicação com os periféricos da placa (*leds*, *display*, botão, *switches*). Além disso, o KinOS possui um simples terminal para a interação do usuário com o sistema e de onde é possível executar os programas adicionados ao *microkernel*.

4.2 Contribuições

Pretende-se que a monografia e a parte prática desenvolvida durante o projeto, sejam utilizados como material didático para o Laboratório de Microprocessadores, fazendo assim com que este se torne mais atual e mais próximo da disciplina de Sistemas Operacionais.

Quanto à contribuição para os integrantes do grupo, este estudo possibilitou principalmente o aprendizado da arquitetura de processadores ARM, além da consolidação dos aspectos teóricos aprendidos em Sistemas Operacionais, através da implementação do *microkernel*.

4.3 Trabalhos Futuros

O conteúdo desenvolvido neste projeto, embora com um número apreciável de funcionalidades e com a implementação de vários conceitos relacionados aos Sistemas Operacionais modernos, ainda não é possível considerá-lo como completo. Devido a restrições de tempo para a realização do projeto, não foi possível implementar todas as funcionalidades desejadas no KinOS, nem otimizar algumas das funcionalidades já existentes.

Uma possível melhoria é fazer com que o sistema seja capaz de ser executado como um módulo na memória flash da Evaluator-7T. Para fazer isso, no entanto, é preciso que o sistema inteiro torne-se independente do monitor de debug Angel. No sistema implementado, o Angel é responsável pelas interrupções de software (SWI) do sistema. Fazer a migração do Angel para rotinas próprias de SWI não é uma atividade trivial.

Também é possível criar mais funcionalidades para o editor de linha de comando (Shell) do KinOS. No momento, ele faz apenas as atividades essenciais para o gerenciamento de *threads* e comunicação com usuário através de um terminal. Como extensão do shell, pensou-se em permitir a recepção de arquivos executáveis ARM (formato ELF) para serem executados como uma nova *thread* dentro do KinOS.

Adicionalmente, outra melhoria a ser feita no sistema é respeito da técnica usada para comunicação pela porta serial COM0. Atualmente, o envio e a recepção de caracteres é feita pela técnica de *polling*, ou seja, o processador interroga uma variável até que ela contenha o valor desejado. Embora funcional, esse método consome muito tempo de processador. É desejável trocar esse método por interrupções, ou seja, o processador leria os caracteres dos *buffers* de transmissão e de recepção apenas quando o canal serial sinalizasse a ele por meio de uma interrupção de *hardware*.

Por fim, é importante ressaltar que as possíveis melhorias aqui descritas não são as únicas que podem ser realizadas. Há várias outras que passaram despercebidas pelos autores do projeto. Espera-se que, quando o projeto for revisitado, ele passe por uma grande evolução, a fim de torná-lo cada vez mais completo e eficiente.

REFERÊNCIAS BIBLIOGRÁFICAS

- ABDELRAZEK, A. F. M. *Exception and Interrupt Handling in ARM*. [S.l.], Setembro 2006. Disponível em: <http://www.iti.uni-stuttgart.de/radetzki/Seminar06/08_report.pdf>.
- ARCTURUS NETWORKS INC. uclinux - embedded linux microcontroller project. 2008. Disponível em: <<http://www.uclinux.org/>>.
- ARM LIMITED. *ARM7TDMI Data Sheet (ARM DDI 0029E)*. [S.l.], Agosto 1995. Disponível em: <http://www.eecs.umich.edu/panalyzer/pdfs/ARM_doc.pdf>.
- ARM LIMITED. *Application Note 25 - Exception Handling on the ARM (ARM DAI 0025E)*. [S.l.], Setembro 1996. Disponível em: <<http://www.imit.kth.se/courses/2B1445/0304/material/Apps25vE.pdf>>.
- ARM LIMITED. *ARM Evaluator-7T Board User Guide*. [S.l.], Agosto 2000. Disponível em: <http://infocenter.arm.com/help/topic/com.arm.doc.dui0134a/DUI0134A_evaluator7t_ug.pdf>.
- ARM LIMITED. *ARM Developer Suite AXD and armsd Debuggers Guide*. [S.l.], Novembro 2001. Disponível em: <<http://infocenter.arm.com/help/topic/com.arm.doc.dui0066d/DUI0066.pdf>>.
- ARM LIMITED. *ARM7TDMI Technical Reference Manual (ARM DDI 0029G)*. Rev 3. [S.l.], Abril 2001. Disponível em: <<http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0029g/index.html>>.
- ARM LIMITED. *ARM Architecture Reference Manual (ARM DDI 0100I)*. [S.l.], Julho 2005. Disponível em: <<http://www.arm.com/miscPDFs/14128.pdf>>.
- FURBER, S. *ARM System-On-Chip Architecture*. 2. ed. [S.l.]: Addison-Wesley, 2000. ISBN 0-20167-519-6.
- KINOSHITA, C. C. e. A. H. J. *Experiência 5: Interrupções*. [S.l.], 2007. Disponível em: <<http://www.pcs.usp.br/jkinoshi/2007/tomas5.doc>>.
- MEIGNAN, W. Isos - simple multithreading os for the evaluator-7t board. 2003. Disponível em: <<http://wilhem.meignan.free.fr/>>.
- MORROW, M. G. *ARM7TDMI Instruction Set Reference*. [S.l.], Setembro 2008. Disponível em: <http://eceserv0.ece.wisc.edu/morrow/ECE353/arm7tdmi_instruction_set_reference.pdf>.
- RED HAT, INC. ecos - embedded configurable operating system. 2009. Disponível em: <<http://ecos.sourceware.org/>>.
- RYZHYK, L. The arm architecture. Junho 2006. Disponível em: <<http://www.cse.unsw.edu.au/cs9244/06/seminars/08-leonidr.pdf>>.

SAMSUNG ELECTRONICS. *KS32C50100 RISC MicroController User Manual*. [S.l.], Agosto 2007. Disponível em: <<http://www.samsung.com/global/system/business/semiconductor/product/2007/6/11/SystemLSI/I>

SLOSS, A. *Interrupt Handling*. [S.l.], Abril 2001.

SLOSS, A.; SYMES, D.; WRIGHT, C. *ARM System Developer's Guide: designing and optimizing system software*. 1. ed. [S.l.]: Morgan Kauffman, 2004. ISBN 1-55860-874-5.

TANENBAUM, A. S.; WOODHULL, A. S. *Operating Systems: Design and Implementation*. 3rd. ed. [S.l.]: Pearson Prentice Hall, 2006. ISBN 0-13-142938-8.

ZAITSEFF, J. *ELEC2041 Microprocessors - Laboratory Manual*. [S.l.], Junho 2003. Disponível em: <<http://www.zap.org.au/elec2041-cdrom/unsw/elec2041/README.html>>.

Apêndice A – PESQUISAS INICIAIS

Antes da decisão pela implementação de um *microkernel* próprio, foram feitas uma série de pesquisas sobre Sistemas Operacionais já existentes para sistemas embarcados, categoria da qual o processador ARM7TDMI e a placa Evaluator-7T fazem parte. Dentre os resultados encontrados, dois Sistemas Operacionais chamaram mais a atenção do grupo: o *eCos* e o *uCLinux*. Esses dois sistemas estão descritos nas seções seguintes.

Além disso, cogitou-se o uso de um ambiente de desenvolvimento baseado no Sistema Operacional GNU/Linux e na ferramenta GNUARM, uma *toolchain* para compilação, embarque e depuração de código em processadores ARM. No entanto, a falta de familiaridade do grupo com ambas as ferramentas e as dificuldades encontradas para configurá-las e executá-las de maneira adequada resultou na escolha do ambiente Windows com desenvolvimento pelo CodeWarrior, uma vez que, para o primeiro, o grupo já possuía conhecimentos avançados e, para o segundo, a existência de uma documentação mais precisa fez com que a curva de aprendizado da ferramenta diminuísse consideravelmente.

A.1 O Sistema Operacional eCos

Este sistema operacional para sistemas embarcados é de código aberto, e portanto, e não cobra royalties pelo seu uso (RED HAT, INC., 2009). Porém, trata-se de um sistema não relacionado ao Linux. Um ponto pelo qual ele se destaca, é seu sistema de configuração. Esse sistema permite a imposição de requisitos bem definidos dos componentes de tempo de execução. Essas ferramentas são distribuídas conjuntamente com o código-fonte do eCos. Dessa forma, dadas as restrições de hardware da Evaluator-7T, o porte dessa sistema operacional é simples de ser feito.

Existem versões desse SO para diversas arquiteturas, inclusive a ARM. O trabalho residiria na adaptação à placa Evaluator-7T.

Com o avanço das pesquisas sobre o eCos, descobriu-se que já havia um porte para a placa

Evaluator-7T. Com isso, o esforço do projeto seria concentrado apenas em realizar a instalação correta do código já existente para placa. Essa abordagem, porém, não era a idealizada pelo projeto, tendo em vista, principalmente, seus objetivos didáticos. A simples instalação de um projeto já pronto não agregaria tanto valor educacional ao projeto quanto a realização das próprias funções básicas de um sistema operacional.

Por esses motivos, então, decidiu-se que o eCos não seria utilizado no projeto, pois não cumpriria um dos objetivos que motivaram a escolha do tema deste projeto: o estudo aprofundado e o consequente aprendizado avançado sobre Sistemas Operacionais.

A.2 O Sistema Operacional uCLinux

Este sistema operacional é um porte do Linux para sistemas sem uma unidade de gerenciamento de memória (MMU) (ARCTURUS NETWORKS INC., 2008), que é o caso da placa Evaluator-7T. Assim como o eCos, há portes dele para diversas arquiteturas, assim como diversas ferramentas que, assim como o Linux, são softwares livres. Tal fato torna interessante para tornar a placa independente de licenças. O que torna este sistema interessante é a existência de uma comunidade entusiasta com este sistema, fazendo com que exista muito material para estudo e assim reduzir a complexidade do porte pretendido.

Assim como o eCos, as pesquisas para se obter mais detalhes sobre este sistema operacional e sobre a viabilidade de utilizá-lo na placa Evaluator-7T prosseguiram. Embora existisse na página do projeto guias básicos para a compilação do código, estes se mostraram insuficientes para a total compreensão do que deveria ser feito. Além disso, não havia instruções sobre como proceder em caso de erros, sendo necessário recorrer às listas de discussão sobre o projeto. Nessas listas, já que a informação é proveniente de uma quantidade muito grande de fontes, a busca pela solução dos eventuais erros encontrados se torna excessivamente lenta, consumindo muito tempo para um problema que, aparentemente, seria de simples resolução.

Além disso, o uCLinux necessita da ferramenta GNUARM para a compilação e embarque do código na placa, a qual requer um ambiente GNU/Linux para sua utilização. Como mencionado anteriormente, a falta de familiaridade do grupo com esses ambientes fez com que o tempo gasto para a realização de tarefas simples e para a resolução de pequenos problemas fosse muito grande. Dessa forma, decidiu-se também por não realizar o porte do uCLinux para a Evaluator-7T.

A decisão final para o projeto foi, então, a criação de um *microkernel* próprio, baseado nos conceitos básicos aprendidos na disciplina de Sistemas Operacionais.

Apêndice B – ARQUIVOS FONTE

B.1 cinit.h

```

1  /*****
2  *  IMPORT
3  *****/
4
5  #include "constants.h"
6  #include "terminal.h"
7  #include "irq.h"
8  #include "button.h"
9  #include "segment.h"
10 #include "timer.h"
11 #include "tictactoe.h"
12
13
14 /*****
15 *  EXTERN
16 *****/
17
18 extern void handler_board_angel(void);
19 extern void handler_board_no_angel(void);
20 extern void handler_swi(void);
21 extern void handler_emulator(void);

```

B.2 cinit.c

```

1  /*****
2  KinOS – Microkernel for ARM Evaluator 7-T
3  Seniors project – Computer Engineering
4  Escola Politecnica da USP, 2009
5  *****/

```

```

6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9   */
10
11  /*
12   The program was based on the mutex program by ARM – Strategic Support
13   Group,
14   contained on the ARM Evaluator 7–T example CD, under the folder /
15   Evaluator7–T/
16   source/examples/mutex/
17   *****
18
19  /* Initialization code in C */
20
21  #include "cinit.h"
22
23  /* Entry point for C part */
24  int C_Entry (void) {
25      /* Initialize 7-segment display */
26      segment_init();
27      /* Initialize timer */
28      timer_init();
29      /* Initialize button */
30      button_init();
31      /* Install hardware interruption handler */
32      if (emulator == 1) {
33          install_handler ((unsigned)handler_emulator, (unsigned *)IRQVector);
34      }
35      else if (emulator == 0) {
36          install_handler ((unsigned)handler_board_angel, (unsigned *)IRQVector);
37      }
38      else {
39          install_handler ((unsigned)handler_board_no_angel, (unsigned *)
40                          IRQVector);
41      }
42      /* Install software interruption handler */
43      install_handler ((unsigned)handler_swi, (unsigned *)SWIVector);
44      /* Start timer */
45      timer_start();
46      /* Enabling IRQ interruption and changing to user mode */
47      __asm {
48          MOV    r1, #0x40|0x10

```

```

46     MSR    CPSR_c, r1
47 }
48 /* Start with shell */
49 shell();
50
51 /* The return below should not be reachable */
52 return 0;
53 }

```

B.3 constants.h

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7–T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13   Group,
14  contained on the ARM Evaluator 7–T example CD, under the folder /
15   Evaluator7–T/
16   source/examples/mutex/
17  *****/
18 /***** GENERAL VARIABLES *****/
19 /* Defines if the program is running on: */
20 /* 0 – Evaluator 7–T board with Angel */
21 /* 1 – CodeWarrior ARMulator */
22 /* 2 – Evaluator 7–T board no Angel */
23 #define emulator 0
24 /* The number of the operating system software interrupt */
25 #define OS_SWI 0
26 /* Interrupt table SWI instruction position */
27 #define SWIVector (unsigned *) 0x08
28 /* Interrupt table IRQ instruction position */

```

```

29 #define IRQVector (unsigned *) 0x18
30 /* Time set for the timer */
31 #define COUNTDOWN 0x001ffff0
32
33 /***** EMULATOR VARIABLES *****/
34 /* Timer interrupt ID */
35 #define IRQTimer      0x0010
36 /* IRQ interrupt controller addresses */
37 #define IRQEnableSet   (volatile unsigned *) 0x0A000008
38 #define IRQEnableClear (volatile unsigned *) 0x0A00000C
39 /* Timer registers */
40 #define EmulatorIRQTimerLoad (volatile unsigned *) 0x0A800000
41 #define EmulatorIRQTimerControl (volatile unsigned *) 0x0A800008
42 #define IRQTimerClear   (volatile unsigned *) 0x0A80000C
43
44 /***** BOARD VARIABLES *****/
45 /* Input/output data address */
46 #define IOData          (volatile unsigned *) 0x03ff5008
47 /* IRQ interrupt controller addresses */
48 #define IRQStatus       (volatile unsigned *) 0x03ff4004
49 /* Timer registers */
50 #define TimerEnableSet   (volatile unsigned *) 0x03ff6000
51 #define EvaluatorIRQTimerLoad (volatile unsigned *) 0x03ff6004
52 #define EvaluatorIRQTimerControl (volatile unsigned *) 0x03ff4008
53 /* Button addresses */
54 #define IRQButtonControl (volatile unsigned *) 0x03ff5004
55 /* Segment addresses */
56 #define IOPMod           (volatile unsigned *) 0x03ff5000
57 /* The bits taken up by the display in IOData register */
58 #define Segment_mask    0x1FC00
59 /* Define segments in terms of IO lines */
60 #define SEG_A    (1<<10)
61 #define SEG_B    (1<<11)
62 #define SEG_C    (1<<12)
63 #define SEG_D    (1<<13)
64 #define SEG_E    (1<<14)
65 #define SEG_F    (1<<16)
66 #define SEG_G    (1<<15)
67 #define DISP_0    (SEG_A|SEG_B|SEG_C|SEG_D|SEG_E|SEG_F)
68 #define DISP_1    (SEG_B|SEG_C)
69 #define DISP_2    (SEG_A|SEG_B|SEG_D|SEG_E|SEG_G)
70 #define DISP_3    (SEG_A|SEG_B|SEG_C|SEG_D|SEG_G)
71 #define DISP_4    (SEG_B|SEG_C|SEG_F|SEG_G)

```

```

72 #define DISP_5    (SEG_A|SEG_C|SEG_D|SEG_F|SEG_G)
73 #define DISP_6    (SEG_A|SEG_C|SEG_D|SEG_E|SEG_F|SEG_G)
74 #define DISP_7    (SEG_A|SEG_B|SEG_C)
75 #define DISP_8    (SEG_A|SEG_B|SEG_C|SEG_D|SEG_E|SEG_F|SEG_G)
76 #define DISP_9    (SEG_A|SEG_B|SEG_C|SEG_D|SEG_F|SEG_G)
77 #define DISP_A    (SEG_A|SEG_B|SEG_C|SEG_E|SEG_F|SEG_G)
78 #define DISP_B    (SEG_C|SEG_D|SEG_E|SEG_F|SEG_G)
79 #define DISP_C    (SEG_A|SEG_D|SEG_E|SEG_F)
80 #define DISP_D    (SEG_B|SEG_C|SEG_D|SEG_E|SEG_G)
81 #define DISP_E    (SEG_A|SEG_D|SEG_E|SEG_F|SEG_G)
82 #define DISP_F    (SEG_A|SEG_E|SEG_F|SEG_G)

```

B.4 startup.s

```

1  ;*****
2  ; KinOS – Microkernel for ARM Evaluator 7–T
3  ; Seniors project – Computer Engineering
4  ; Escola Politecnica da USP, 2009
5  ;
6  ; Felipe Giunte Yoshida
7  ; Mariana Ramos Franco
8  ; Vinicius Tosta Ribeiro
9  ;
10 ;
11 ;
12 ; The program was based on the mutex program by ARM – Strategic Support
    Group,
13 ; contained on the ARM Evaluator 7–T example CD, under the folder /
    Evaluator7–T/
14 ; source/examples/mutex/
15 ;*****
16
17
18 ; Startup assembly code
19 ; Obs.: This code was built supposing that the generated assembly is ARM
20 ; assembly, not THUMB!!!
21
22 IMPORT current_thread_id
23 IMPORT thread_array
24 IMPORT C_Entry
25

```

```

26 ; Identifying that from below on it is assembly code (readable only)
27 AREA asm_init, CODE
28
29 ; Entry point of the program
30 ENTRY
31
32 ; Beginning assembly initialization
33 start
34 ; Changing to IRQ mode and disabling interruptions, then setting up
35 ; IRQ stack pointer to 0x8000
36 MOV r0, #0xC0|0x12 ; r0 = 0xC0 or 0x12 (0xC0 = IRQ disabled,
37 ; 0x12 = IRQ mode)
38 MSR CPSR_c, r0 ; status_register = r0
39 MOV sp, #0x8000 ; stack pointer = 0x8000
40
41 ; Changing to system mode and disabling interruptions, then setting up
42 ; user stack pointer to 0x20000
43 MOV r0, #0xC0|0x1F ; r0 = 0xC0 or 0x1F (0xC0 = IRQ disabled,
44 ; 0x1F = system mode)
45 MSR CPSR_c, r0 ; status_register = r0
46 MOV sp, #0x20000 ; stack pointer = 0x20000
47
48 ; Changing to SVC mode and disabling interruptions, then setting up
49 ; SVC stack pointer to 0x8000 - 128
50 MOV r0, #0xC0|0x13 ; r0 = 0xC0 or 0x13 (0xC0 = IRQ disabled,
51 ; 0x13 = SVC mode)
52 MSR CPSR_c, r0 ; status_register = r0
53 MOV r0, #0x8000 ; r0 = 0x8000
54 SUB r0, r0, #128 ; r0 = r0 - 128
55 MOV sp, r0 ; stack pointer = r0
56
57 ; Initializes the thread array with zeros (0 = thread disabled,
58 ; 1 = thread enabled)
59 LDR r0, =thread_array ; r0 = thread_array start address
60 MOV r1, #1 ; r1 = 1
61 STR r1, [r0] ; address(r0) = r1
62 MOV r1, #0 ; r1 = 0 (disabled)
63 MOV r2, #0 ; r2 = 0
64 init_thread_array_loop
65 ADD r2, r2, #4 ; r2 = r2 + 4
66 CMP r2, #36 ; r2 = 36?
67 BEQ set_active_thread ; if yes, go to set_active_thread
68 ADD r3, r0, r2 ; r3 = r0 + r2

```

```

69  STR    r1, [r3]          ; address(r3) = r1
70  B      init_thread_array_loop ; return to init_thread_array_2
71
72  ; Setting the thread id to 1
73  set_active_thread
74  LDR    r0, =current_thread_id ; r0 = current thread id address
75  MOV    r1, #1              ; r1 = 1
76  STR    r1, [r0]            ; current thread id = 1
77
78  ; Pass control to C_Entry
79  LDR    lr, =C_Entry         ; link register = C entry
80  MOV    pc, lr               ; process counter = C entry
81
82  ; End of assembly code
83  END

```

B.5 apps/tasks.h

```

1  /*****
2  * IMPORT
3  *****/
4
5  #include "segment.h"
6  #include "swi.h"
7  #include "mutex.h"
8  #include "led.h"
9  #include "serial.h"
10 #include "irq.h"
11 #include "dips.h"
12 #include "tictactoe.h"
13
14
15 /*****
16 * EXTERN
17 *****/
18
19 extern int current_thread_id;
20
21
22 /*****
23 * DEFINES

```

```

24  *****/
25
26  struct name_address {
27      char* name;          // The task name
28      void (*task_ptr)(int); // Pointer to the task
29  };
30
31
32  /*****
33   * ROUTINES
34   *****/
35
36  int strcmp (char* str1, char* str2);
37  pt2Task get_task_addr(char* name);
38  int get_state(int pid);
39  int get_task_name_size(void);
40  char* get_task_name(int index);
41
42  void display_pid(int);
43  void mutex_test (int);
44  void fork_test (int);
45  void set_segment(int);
46  void set_led(int);
47  void malicious_handler(int);
48  void security_flaw (int);
49  void dips_to_leds (int);
50  void dips_to_segments (int);
51  void play_tictactoe(int);

```

B.6 apps/tasks.c

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7-T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */
10

```

```

11  /*
12     The program was based on the mutex program by ARM – Strategic Support
13     Group,
14     contained on the ARM Evaluator 7–T example CD, under the folder /
15     Evaluator7–T/
16     source/examples/mutex/
17     *****/
18  /******
19  * IMPORT
20  *****/
21  #include "tasks.h"
22  #include "terminal.h"
23
24
25  /******
26  * EXTERN
27  *****/
28
29  extern int thread_array [];
30
31
32  /******
33  * GLOBAL VARIABLES
34  *****/
35
36  // The number which is showed in the display
37  int displayNumber;
38
39  // Struct which saves the task name and task address
40  struct name_address tasks_name [] = {
41      {"display_pid", &display_pid},
42      {"set_led", &set_led},
43      {"set_segment", &set_segment},
44      {"mutex_test", &mutex_test},
45      {"fork_test", &fork_test},
46      {"dips_to_leds", &dips_to_leds},
47      {"dips_to_segments", &dips_to_segments},
48      {"malicious_handler", &malicious_handler},
49      {"tictactoe", &play_tictactoe}
50  };
51

```

```

52 /*****
53  * MACRO
54  *****/
55
56 // The number of tasks in the struct tasks_name
57 #define tasks_name_size 9
58
59
60 /*****
61  * ROUTINES
62  *****/
63
64 // Compare two strings
65 int strcmpper (char* str1, char* str2){
66     int i;
67     for (i = 0; str1[i] == str2[i]; i++){
68         if (str1[i] == '\0'){
69             return 0;
70         }
71     }
72     return str1[i] - str2[i];
73 }
74
75 // Get the task address
76 pt2Task get_task_addr(char* name){
77     int i;
78     for(i=0; i < tasks_name_size; i++){
79         if(strcmpper(tasks_name[i].name, name)==0){
80             return tasks_name[i].task_ptr;
81         }
82     }
83     return 0;
84 }
85
86 // Get the thread state (active/inactive)
87 int get_state(int pid){
88     if (pid > 9 || pid < 0){
89         return 0;
90     }else{
91         return thread_array[pid];
92     }
93 }
94

```

```

95 // Get the size of the struct task_name
96 int get_task_name_size(){
97     return tasks_name_size;
98 }
99
100 // Get the task name from the struct task_name
101 char* get_task_name(int index){
102     return tasks_name[index].name;
103 }
104
105
106 /*****
107  * TASKS
108  *****/
109
110
111 // Show in the LEDs the value passed as argument
112 void set_led(int value){
113     switch (value) {
114         case 0:
115             LED_1_OFF;
116             LED_2_OFF;
117             LED_3_OFF;
118             LED_4_OFF;
119             break;
120         case 1:
121             LED_1_OFF;
122             LED_2_OFF;
123             LED_3_OFF;
124             LED_4_ON;
125             break;
126         case 2:
127             LED_1_OFF;
128             LED_2_OFF;
129             LED_3_ON;
130             LED_4_OFF;
131             break;
132         case 3:
133             LED_1_OFF;
134             LED_2_OFF;
135             LED_3_ON;
136             LED_4_ON;
137             break;

```

```
138  case 4:
139      LED_1_OFF;
140      LED_2_ON;
141      LED_3_OFF;
142      LED_4_OFF;
143      break;
144  case 5:
145      LED_1_OFF;
146      LED_2_ON;
147      LED_3_OFF;
148      LED_4_ON;
149      break;
150  case 6:
151      LED_1_OFF;
152      LED_2_ON;
153      LED_3_ON;
154      LED_4_OFF;
155      break;
156  case 7:
157      LED_1_OFF;
158      LED_2_ON;
159      LED_3_ON;
160      LED_4_ON;
161      break;
162  case 8:
163      LED_1_ON;
164      LED_2_OFF;
165      LED_3_OFF;
166      LED_4_OFF;
167      break;
168  case 9:
169      LED_1_ON;
170      LED_2_OFF;
171      LED_3_OFF;
172      LED_4_ON;
173      break;
174  case 10:
175      LED_1_ON;
176      LED_2_OFF;
177      LED_3_ON;
178      LED_4_OFF;
179      break;
180  case 11:
```

```

181     LED_1_ON;
182     LED_2_OFF;
183     LED_3_ON;
184     LED_4_ON;
185     break;
186 case 12:
187     LED_1_ON;
188     LED_2_ON;
189     LED_3_OFF;
190     LED_4_OFF;
191     break;
192 case 13:
193     LED_1_ON;
194     LED_2_ON;
195     LED_3_OFF;
196     LED_4_ON;
197     break;
198 case 14:
199     LED_1_ON;
200     LED_2_ON;
201     LED_3_ON;
202     LED_4_OFF;
203     break;
204 case 15:
205     LED_1_ON;
206     LED_2_ON;
207     LED_3_ON;
208     LED_4_ON;
209     break;
210 }
211 set_state(current_thread_id , 0);
212 exit(current_thread_id);
213 while(1);
214 }
215
216
217 // Set in the display the value passed as argument
218 void set_segment(int value){
219     while (1) {
220         if (displayNumber != value) {
221             segment_set(value);
222             displayNumber = value;
223         }

```

```

224     }
225 }
226
227
228 // Set in the display the thread's pid
229 void display_pid(int trash){
230     while (1) {
231         if (displayNumber != current_thread_id) {
232             segment_set(current_thread_id);
233             displayNumber = current_thread_id;
234         }
235     }
236 }
237
238
239 // The tictactoe program
240 void play_tictactoe(int trash) {
241
242     WAIT_SHELL;
243     tictactoe();
244     SIGNAL_SHELL;
245
246     set_state(current_thread_id , 0);
247     exit(current_thread_id);
248     while(1){}
249 }
250
251
252 // Exemple of fork/exec
253 void fork_test(int trash){
254     int a = 0;
255     char pid[1];
256
257     pid[0] = current_thread_id + 48;
258     print("\r\nparent = ");
259     print(pid);
260     print(".\r\n");
261
262     a = fork();
263     if(a != -1 && a != 0){
264         pid[0] = a + 48;
265         print("child = ");
266         print(pid);

```

```

267     print(".\r\n");
268     exit(a);
269 }
270
271 while(1){
272
273 }
274 }
275
276
277 // Example of mutex
278 void mutex_test (int led) {
279
280     if (led >= 1 && led <= 4) {
281
282         while (1) {
283             int delay;
284             /* Set display as 3 */
285             if (displayNumber != current_thread_id) {
286                 segment_set(current_thread_id);
287                 displayNumber = current_thread_id;
288             }
289             /* Wait if mutex is on, if it is not, set it */
290             WAIT_EXAMPLE;
291             /* Turn on LED 1 */
292             switch (led) {
293                 case 1:
294                     LED_1_ON;
295                     break;
296                 case 2:
297                     LED_2_ON;
298                     break;
299                 case 3:
300                     LED_3_ON;
301                     break;
302                 case 4:
303                     LED_4_ON;
304                     break;
305             }
306
307             /* Wait 20 ffff*/
308             for (delay=0; delay<0xffff; delay++) {}
309             /* Turn off LED 1 */

```

```

310     switch (led) {
311         case 1:
312             LED_1_OFF;
313             break;
314         case 2:
315             LED_2_OFF;
316             break;
317         case 3:
318             LED_3_OFF;
319             break;
320         case 4:
321             LED_4_OFF;
322             break;
323     }
324     /* Turn mutex off */
325     SIGNAL_EXAMPLE;
326     /* Wait */
327     for (delay=0; delay<0xffff; delay++) {}
328 }
329 }
330 else {
331     // kills the process if it received invalid parameters
332     print("Invalid parameter for mutex_test\r\n\n");
333
334     set_state(current_thread_id, 0);
335     exit(current_thread_id);
336     while(1){}
337 }
338 }
339
340
341 // Malicious program wich install a handler
342 // Attention!! This program will lock the system
343 void malicious_handler (int trash) {
344     LED_1_OFF;
345     LED_2_OFF;
346     LED_3_OFF;
347     LED_4_OFF;
348     displayNumber = 0;
349     install_handler ((unsigned)security_flaw, (unsigned *)IRQVector);
350     while (1) {}
351 }
352

```

```

353
354 // Routine used in the malicious_handler
355 void security_flaw (int trash) {
356     int delay;
357     while (1) {
358         switch (displayNumber) {
359             case 0:
360                 LED_1_ON;
361                 LED_2_ON;
362                 LED_3_ON;
363                 LED_4_ON;
364                 displayNumber = 15;
365                 break;
366             case 15:
367                 LED_1_OFF;
368                 LED_2_OFF;
369                 LED_3_OFF;
370                 LED_4_OFF;
371                 displayNumber = 0;
372                 break;
373         }
374         for (delay = 0; delay <= 0x001ffff0; delay++) {};
375     }
376 }
377
378
379 // Set in the LEDs the value give in the switches
380 void dips_to_leds (int trash) {
381     set_led(dips_read());
382 }
383
384
385 // Set in the display the value give in the switches
386 void dips_to_segments (int trash) {
387
388     int setvalue;
389
390     setvalue = (int)(dips_read());
391     segment_set(setvalue);
392     print("DIP value succesfully setted on the display!\r\n\n");
393
394     set_state(current_thread_id, 0);
395     exit(current_thread_id);

```

```

396  while(1){}
397  }

```

B.7 apps/terminal.h

```

1  /*****
2   * ROUTINES
3   *****/
4
5  /* Reads a string from the COM0 port */
6  void getcommand(char *cmd, int length);
7
8  /* The shell routine */
9  void shell (void);
10
11 /* Kills a running process */
12 void run_end(char *arg);
13
14 /* Sets the state (active or inactive) in the tasks struct */
15 void set_state(int pid, int state);

```

B.8 apps/terminal.c

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7–T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13  Group,
14  contained on the ARM Evaluator 7–T example CD, under the folder /
15  Evaluator7–T/
16  source/examples/mutex/
17  *****/

```

```

16
17 /*****
18  * IMPORT
19  *****/
20
21 #include "serial.h"
22 #include "tasks.h"
23 #include <string.h>
24
25
26 /*****
27  * MACROS
28  *****/
29
30 #define angel_SWI 0x123456
31 #define MAX_CMD_LENGTH 80
32 #define MAX_TASK_NAME 20
33
34 #define ISALPHA(c) ((c >= 65 && c <= 90) || (c >= 97 && c <= 192))
35 #define ISDIGIT(c) ((c >= 48 && c <= 57))
36
37
38 struct pid_name {char* pid; char name[MAX_TASK_NAME]; int state;} tasks[] =
39     {
40     {"1", "shell", 1},
41     {"2", "", 0},
42     {"3", "", 0},
43     {"4", "", 0},
44     {"5", "", 0},
45     {"6", "", 0},
46     {"7", "", 0},
47     {"8", "", 0},
48     {"9", "", 0}
49 };
50
51 /*****
52  * MISC
53  *****/
54
55 __swi (angel_SWI) void _Exit(unsigned op, unsigned except);
56 #define Exit() _Exit(0x18,0x20026)
57

```

```

58 __swi (angel_SWI) void _WriteC(unsigned op, const char *c);
59 #define WriteC(c) _WriteC (0x3,c)
60
61
62 /*****
63  * ROUTINES
64  *****/
65
66 /* — comm_print —————
67  *
68  * Description : write a string via the Angel SWI call WriteC
69  *
70  * Parameters : const char *string — string to be written
71  * Return : none...
72  * Notes : none...
73  *
74  */
75
76 void comm_print (const char *string)
77 {
78     int pos = 0;
79     while (string[pos] != 0) WriteC(&string[pos++]);
80 }
81
82 /* — comm_init —————
83  *
84  * Description : initialize the COM0 port and set to 9600 baud.
85  *
86  * Parameters : none...
87  * Return : none...
88  * Notes : none...
89  *
90  */
91
92 void comm_init (void)
93 {
94     serial_initcom0user (BAUD_9600);
95 }
96
97 /* — comm_banner —————
98  *
99  * Description : print out standard banner out of the COM0 port
100  *

```

```

101  * Parameters : none...
102  * Return    : none...
103  * Notes     : none...
104  *
105  */
106
107  void comm_banner (void)
108  {
109      print ("\n** Welcome to KinOS!!");
110      print (" - Version 0.1 **\n\r");
111  }
112
113  /* — comm_getkey —————
114  *
115  * Description : wait until a key is press from the host PC.
116  *
117  * Parameters : none...
118  * Return     : none...
119  * Notes      : none...
120  *
121  */
122
123  void comm_getkey (void)
124  {
125      serial_getkey();
126  }
127
128  // Fills an entire string str of length 'length' with null characters
129  void clearstring(char *str, int length) {
130
131      int i;
132
133      for (i = 0; i < length; i++) {
134          str[i] = 0;
135      }
136
137  }
138
139  // Sets the state (active or inactive) in the tasks struct
140  void set_state(int pid, int state){
141      tasks[pid-1].state = state;
142
143  }

```

```

144
145 // Runs start command with arguments arg and num
146 void run_start(char *arg, int num) {
147     int a = 0;
148     int count = 0;
149     int i;
150
151     // Checks if the typed program name is in the tasks list
152     if (get_task_addr(arg) == 0){
153         print("\nProgram not found.\r\n\n");
154         return;
155     }
156
157     for(i=0; i< 9; i++){
158         count = count + tasks[i].state;
159     }
160
161     if(count==9){
162         print("\nImpossible to run more than 9 programs.\r\n\n");
163         return;
164     }
165
166     else{
167
168         // Forks the shell process and executes the new process with the user-
169         // supplied arguments
170         a = fork();
171         if(a != -1 && a != 0){
172             print("\nProgram started.\r\n\n");
173             exec(a ,get_task_addr(arg), num);
174             memcpy(tasks[a - 1].name, arg, sizeof(char)*MAX_TASK_NAME);
175             tasks[a - 1].state = 1;
176         }
177     }
178 }
179
180 }
181
182
183 // Kills a running process
184 void run_end(char *arg) {
185     int i;

```

```

186
187 // arg = all
188 if(strcmp(arg, "all")==0) {
189     SIGNAL_SHELL;
190     SIGNAL_EXAMPLE;
191     for(i=1; i < 9; i++){
192         exit(i+1);
193         tasks[i].state = 0;
194     }
195     print("\nFinished all programs.\r\n\n");
196 }
197 // arg = task name
198 else{
199     for(i=1; i < 9; i++){
200         if(tasks[i].state == 1){
201             if(strcmp(tasks[i].name, arg) == 0){
202                 exit(i+1);
203                 tasks[i].state = 0;
204                 print("\nProgram finished.\r\n\n");
205                 return;
206             }
207         }
208     }
209     print("\nThe selected program has not yet been started.\r\n\n");
210 }
211
212 }
213
214 // Kills a process using its PID as an argument
215 void run_end_pid(int pid) {
216
217     if(pid == 1){
218         print("\nNot possible to kill the shell program.\r\n\n");
219     }else if(pid < 2 || pid > 9){
220         print("\nIncorrect PID.\r\n\n");
221     }else{
222         exit(pid);
223         tasks[pid - 1].state = 0;
224         print("\nProgram finished.\r\n\n");
225     }
226
227 }
228

```

```

229 // Lists all available programs in the tasks list
230 void run_listtasks() {
231     int i;
232     print("\nTasks Name: \r\n\n");
233     for(i=0; i<get_task_name_size(); i++){
234         print(get_task_name(i));
235         print("\r\n");
236     }
237     print("\r\n\n");
238 }
239
240
241 // Lists all currently active threads in the system
242 // This is done by consulting the tasks list (defined above)
243 void run_ps() {
244
245     int i, j, k;
246     char blankstr[MAX_TASK_NAME];
247
248     print("\nCurrently active threads:\r\n");
249     print("\n");
250     print("Name:                PID:\r\n");
251
252     for(i=0; i < 9; i++) {
253         if(tasks[i].state == 1){
254
255             j = 0;
256             while (tasks[i].name[j] != 0 && j < MAX_TASK_NAME)
257                 j++;
258
259             clearstring(blankstr, MAX_TASK_NAME);
260
261             for(k = 0; k < MAX_TASK_NAME - j; k++)
262                 blankstr[k] = 32; // blank
263
264             print(tasks[i].name);
265             print(blankstr);
266             print( tasks[i].pid);
267             print("\r\n");
268         }
269     }
270     print("\r\n\n");
271

```

```

272 }
273
274
275 // Lists all available commands for kinoshell
276 void run_help() {
277     print("\nOther available commands for kinoshell:\r\n\n");
278     print("                ps : Lists all currently active threads in KinOS
                \r\n");
279     print("                start <name> : Starts a new thread with the program
                specified in <name>\r\n");
280     print("start <name> [<arg>] : Starts a new thread with the program
                specified in <name>\r\n");
281     print("                                and the argument in <arg>\r\n");
282     print("                end <name> : Kills the first threads named <name>\r\n");
283     print("                end pid <num> : Kills the threads with the pid <num>\r\n");
284     print("                end all : Kills all threads\r\n");
285     print("                about : Displays additional information about the
                KinOS project\r\n");
286     print("                listtasks : Displays a list of available programs for
                execution\r\n");
287     print("\n");
288 }
289
290
291 // Additional information about the project
292 void run_about() {
293     print("\nAbout KinOS v1.0 (December 2009)\r\n\n");
294     print("Authors: Felipe Giunte Yoshida\r\n");
295     print("                Mariana Ramos Franco\r\n");
296     print("                Vinicius Tosta Ribeiro\r\n");
297     print("Project advisor: Prof. Dr. Jorge Kinoshita\r\n\n");
298 }
299
300
301
302 /* — getcommand —————
303 *
304 * Reads a string from the COM0 port
305 *
306 */
307 void getcommand(char *cmd, int length) {
308
309     int i, c;

```

```

310
311 c=0; i=0;
312
313 clearstring(cmd, length);
314
315 while (c != '\r' && i < length) {
316     c = serial_getchar();
317     if (c == 8) { // backspace
318         if (i>0) {
319             i--;
320         }
321     }
322     else {
323         cmd[i++] = c;
324     }
325 }
326 }
327
328
329 /* — getcommand —————
330 *
331 * Runs a finite state machine in order to parse user input (char *cmd)
332 *
333 */
334 void parsecommand(char *cmd) {
335
336     int i, state, iw1, iw2, error;
337     char c;
338     char *reservedwords[] = { "ps", "start", "end", "help", "about", "
        listtasks", "pid" };
339     char word1[MAX_CMD_LENGTH], word2[MAX_CMD_LENGTH], word3[2];
340
341     error = 0;
342     state = 0;
343     iw1 = 0;
344     iw2 = 0;
345
346     clearstring(word1, MAX_CMD_LENGTH);
347     clearstring(word2, MAX_CMD_LENGTH);
348     clearstring(word3, 2);
349
350     // sweeps the entire cmd string
351     for (i = 0; i < MAX_CMD_LENGTH; i++) {

```

```

352
353 c = cmd[i];
354
355 // this finite state mamchine is designed to find up to two words (
    letter{letter|digit}) and one hex number ([0-9][A-F][a-f])
356 // it ignores excessive blanks between each word
357 switch (state) {
358
359     case 0:
360         if(c == ' ' || c == '\t')
361             state = 0;
362         else if (ISALPHA(c) || c == '-') {
363             state = 1;
364             word1[iw1] = c;
365             iw1++;
366         }
367         else
368             state = 666;
369         break;
370
371     case 1:
372         if(c == ' ' || c == '\t')
373             state = 2;
374         else if (c == '\r')
375             state = 5;
376         else if (ISALPHA(c) || ISDIGIT(c) || c == '-') {
377             state = 1;
378             word1[iw1] = c;
379             iw1++;
380         }
381         else
382             state = 666;
383         break;
384
385     case 2:
386         if(c == ' ' || c == '\t')
387             state = 2;
388         else if (c == '\r')
389             state = 5;
390         else if (ISALPHA(c) || c == '-') {
391             state = 3;
392             word2[iw2] = c;
393             iw2++;

```

```

394     }
395     else
396         state = 666;
397     break;
398
399 case 3:
400     if(ISALPHA(c) || ISDIGIT(c) || c == '_') {
401         state = 3;
402         word2[iw2] = c;
403         iw2++;
404     }
405     else if(c == ' ' || c == '\t')
406         state = 4;
407     else if(c == '\r')
408         state = 5;
409     else
410         state = 666;
411     break;
412
413 case 4:
414     if(c == ' ' || c == '\t')
415         state = 4;
416     else if(c == '\r')
417         state = 5;
418     else if(ISDIGIT(c) || (c >= 65 && c <= 70) || (c >= 97 && c <=
419         102)) {
420         state = 6;
421         word3[0] = c;
422     }
423     else
424         state = 666;
425     break;
426
427 case 5:
428     // acceptance state
429     state = 5;
430     break;
431
432 case 6:
433     if(c == ' ' || c == '\t')
434         state = 6;
435     else if(c == '\r')
436         state = 5;

```

```

436         else
437             state = 666;
438         break;
439
440     case 666:
441         // error state
442         break;
443     }
444
445
446 }
447
448 if(state == 5) {
449     // checks if word1 is one of the reserved words
450     // and if the command's syntax is respected
451     if(strcmp(reservedwords[0], word1) == 0 && iw2 == 0 && word3[0] == 0)
452         run_ps();
453
454     else if(strcmp(reservedwords[1], word1) == 0 && iw2 != 0 && word3[0] !=
455              0){
456         //numbers
457         if(word3[0] > 47 && word3[0] < 58){
458             run_start(word2, word3[0] - 48);
459         }
460         // a, b, c, d, e, f
461         else if(word3[0] > 96 && word3[0] < 103){
462             run_start(word2, word3[0] - 87);
463         }
464         // A B C D E F
465         else if(word3[0] >= 65 && word3[0] <= 70){
466             run_start(word2, word3[0] - 55);
467         }
468     }
469
470     else if(strcmp(reservedwords[1], word1) == 0 && iw2 != 0 && word3[0] ==
471              0)
472         run_start(word2, 0);
473
474     else if(strcmp(reservedwords[2], word1) == 0 && iw2 != 0 && word3[0] ==
475              0)
476         run_end(word2);

```

```

475     else if(strcmp(reservedwords[2], word1) == 0 && strcmp(reservedwords
476         [6], word2) == 0 && word3[0] != 0){
477         //numbers
478         if(word3[0]>49 && word3[0]<58){
479             run_end_pid(word3[0] - 48);
480         }else{
481             print("\nThe pid must be a number between 2 and 9.\r\n\n");
482         }
483     }
484     else if(strcmp(reservedwords[3], word1) == 0 && iw2 == 0 && word3[0] ==
485         0)
486         run_help();
487     else if(strcmp(reservedwords[4], word1) == 0 && iw2 == 0 && word3[0] ==
488         0)
489         run_about();
490     else if(strcmp(reservedwords[5], word1) == 0 && iw2 == 0 && word3[0] ==
491         0)
492         run_listtasks();
493     else
494         print("\nInvalid command.\r\n\n");
495 }
496 else {
497     print("\nInvalid command.\r\n\n");
498 }
499 }
500 }
501
502
503 /* Print the KiOS banner */
504 void printbanner() {
505
506     print("Welcome to\r\n");
507     print("_____ \r\n
508 ");
509     print("88      a8P      88      ,ad8888ba ,      ad88888ba      \r\n
510 ");
511     print("88      ,88\ '      \""      d8\""\ '      '\ "8b      d8\ "
512         "\"8b      \r\n");

```

```

510     print("88  ,88\"
           \"n");
511     print("88,d88'      88 8b,dPPYba,  88      88  'Y8aaaaa,  \"r\\n
           ");
512     print("88888\\\"88,      88 88P\\'  '\\\"8a 88      88  '\\\"\"\"\"\"\"\"8
           b,  \"r\\n");
513     print("88P  Y8b      88 88      88 Y8,      ,8P      '8b  \"r\\n
           ");
514     print("88      \\\"88,  88 88      88  Y8a.  .a8P  Y8a      a8P  \"r\\
           n");
515     print("88      Y8b 88 88      88  '\\\"Y8888Y\\\"\\'  '\\\"Y88888P\\\"
           \"r\\n");
516     print("-----\"r\\n
           \"n");
517     print("Type '\\help\\' for a list of available commands\\r\\n\\n");
518
519 }
520
521 /* The shell routine */
522 void shell (void)
523 {
524     char cmd[MAX_CMD_LENGTH];
525
526     comm_init();
527     printbanner();
528
529     while (1) {
530
531         WAIT_SHELL;
532
533         print("kinoshell> ");
534
535         getcommand(cmd, MAX_CMD_LENGTH);
536
537         parsecommand(cmd);
538
539         SIGNAL_SHELL;
540
541         switch_thread();
542
543     }
544
545     Exit();

```

```

546 }
547
548
549 /*****
550  * END OF comm.c
551  *****/

```

B.9 apps/tictactoe.h

```

1  /*****
2  * IMPORT
3  *****/
4
5  #include "serial.h"
6  #include "terminal.h"
7
8  #include "../mutex/mutex.h"
9  #include "../interrupt/swi.h"
10
11
12 /*****
13  * ROUTINES
14  *****/
15
16 /* Entry point of the game */
17 void tictactoe(void);

```

B.10 apps/tictactoe.c

```

1  /*****
2  KinOS – Microkernel for ARM Evaluator 7–T
3  Seniors project – Computer Engineering
4  Escola Politecnica da USP, 2009
5
6  Felipe Giunte Yoshida
7  Mariana Ramos Franco
8  Vinicius Tosta Ribeiro
9  */
10
11 /*

```

```

12  The program was based on the mutex program by ARM – Strategic Support
    Group,
13  contained on the ARM Evaluator 7-T example CD, under the folder /
    Evaluator7-T/
14  source/examples/mutex/
15  *****/
16
17
18  /******
19  * IMPORT
20  *****/
21
22  #include "tictactoe.h"
23
24
25  /******
26  * MACROS
27  *****/
28
29  #define ISDIGIT(c) ((c >= 48 && c <= 57))
30  #define MAX 3
31
32  /******
33  * GLOBAL VARIABLES
34  *****/
35
36  // global variable
37  char grid[3][3];
38
39
40  /******
41  * ROUTINES
42  *****/
43
44  // prints the game grid
45  // Example:
46  //
47  // X |  |
48  // —+—+—
49  // O | X |
50  // —+—+—
51  // O | O | X
52  //

```

```

53 void printgrid(void) {
54
55     char str[MAX];
56
57     str[1] = 0;
58
59     print("\r\n\n 0  1  2\r\n\n");
60
61     print("0  ");
62     str[0] = grid[0][0];
63     print(str);
64     print(" | ");
65     str[0] = grid[0][1];
66     print(str);
67     print(" | ");
68     str[0] = grid[0][2];
69     print(str);
70     print("\r\n");
71
72     print("  —+—+—\r\n");
73
74     print("1  ");
75     str[0] = grid[1][0];
76     print(str);
77     print(" | ");
78     str[0] = grid[1][1];
79     print(str);
80     print(" | ");
81     str[0] = grid[1][2];
82     print(str);
83     print("\r\n");
84
85     print("  —+—+—\r\n");
86
87     print("2  ");
88     str[0] = grid[2][0];
89     print(str);
90     print(" | ");
91     str[0] = grid[2][1];
92     print(str);
93     print(" | ");
94     str[0] = grid[2][2];
95     print(str);

```

```

96     print("\r\n\n");
97
98 }
99
100 // Puts a game token in the grid at the position specified by the player
101 int placetoken(char token, int i, int j) {
102
103     if ((grid[i][j] == 0 || grid[i][j] == 32) && (i >= 0 || i < 3 || j >= 0
104         || j < 3)) {
105         grid[i][j] = token;
106         return 1;
107     }
108     else {
109         print("\r\nInvalid move!\r\n\n");
110         return 0;
111     }
112 }
113
114 // Checks if one of the players has won
115 int isgameover(void) {
116
117     int i;
118
119     for (i = 0; i < 3; i++) {
120
121         if (
122             (grid[i][0] == grid[i][1] && grid[i][1] == grid[i][2] && (grid[i]
123                 ][0] != 32 && grid[i][0] != 0)) || // lines
124             (grid[0][i] == grid[1][i] && grid[1][i] == grid[2][i] && (grid
125                 ][0][i] != 32 && grid[0][i] != 0)) // columns
126         ) {
127             return 1;
128         }
129     }
130
131     // diagonals
132     if (((grid[0][0] == grid[1][1] && grid[1][1] == grid[2][2]) ||
133         (grid[0][2] == grid[1][1] && grid[1][1] == grid[2][0])) &&
134         (grid[1][1] != 32 && grid[1][1] != 0)) {
135         return 1;
136     }
137     else {

```

```

136         return 0;
137     }
138
139 }
140
141 // Returns the game symbol for each player
142 char getplayertoken(int player) {
143
144     if (player == '0') return 'X';
145     else return 'O';
146
147 }
148
149 // Alternates between Player 1 and Player 2
150 char changeplayer(char player) {
151
152     if (player == '0')
153         return '1';
154     else
155         return '0';
156
157 }
158
159 void banner() {
160
161     print("Tic Tac Toe for KinOS v0.1 (December 2009)\r\n\n");
162     print("Type 'q' in both Row and Column fields anytime to quit\r\n\n");
163
164 }
165
166 // Entry point of the game
167 // (The commented-out sections regarding random numbers are for automatic
playing)
168 void tictactoe(void) {
169
170     int i, j, victory, okmove = 0;
171     int freespaces;
172     char playerstr[2], rowstr[MAX], columnstr[MAX], player;
173
174     for (i = 0; i < 3; i++) {
175         for (j = 0; j < 3; j++) {
176             grid[i][j] = 32;
177         }

```

```

178     }
179
180     banner();
181
182     //srand(time(NULL));
183
184     printgrid();
185
186     freespaces = 9;
187     victory = 0;
188     player = '0';
189
190     // Gets moves from both players until a win condition or tied game is
191     found
192     while(victory == 0 && freespaces > 0) {
193
194         playerstr[0] = player+1;
195         playerstr[1] = 0;
196         okmove = 0;
197
198         while (okmove != 1) {
199             print("Player ");
200             print(playerstr);
201             print("\'s move:\r\n\n");
202
203
204             print("    Row: ");
205             getcommand(rowstr, MAX);
206
207             i = (int)(rowstr[0] - 48);
208             //i = rand()%3;
209
210             print("\n    Column: ");
211             getcommand(columnstr, MAX);
212             j = (int)(columnstr[0] - 48);
213             //j = rand()%3;
214
215             if(rowstr[0] == 'q' && columnstr[0] == 'q') {
216                 print("\n\nQuitting Tic Tac Toe\r\n\n");
217                 return;
218             }
219

```

```

220         okmove = placetoken(getplayertoken(player), i, j);
221     }
222
223
224     print("\r\n");
225
226     freespaces--;
227
228     victory = isgameover();
229
230     printgrid();
231
232     player = changeplayer(player);
233
234 }
235
236
237 if (victory == 1) {
238     playerstr[0] = changeplayer(player)+1;
239     print("A winner is Player ");
240     print(playerstr);
241     print(" !\r\n\n");
242 }
243 else {
244     print("Tied game!\r\n\n");
245 }
246
247 }

```

B.11 interrupt/handler_irq.s

```

1  ;*****
2  ; KinOS – Microkernel for ARM Evaluator 7–T
3  ; Seniors project – Computer Engineering
4  ; Escola Politecnica da USP, 2009
5  ;
6  ; Felipe Giunte Yoshida
7  ; Mariana Ramos Franco
8  ; Vinicius Tosta Ribeiro
9  ;
10 ;

```

```

11 ;
12 ; The program was based on the mutex program by ARM – Strategic Support
    Group,
13 ; contained on the ARM Evaluator 7–T example CD, under the folder /
    Evaluator7–T/
14 ; source/examples/mutex/
15 ;*****
16
17
18
19 ; Hardware interrupt handling code
20
21 IMPORT  button_irq
22 IMPORT  timer_irq
23
24 EXPORT  Angel_IRQ_Address
25 EXPORT  current_thread_id
26 EXPORT  handler_board_angel
27 EXPORT  handler_board_no_angel
28 EXPORT  handler_emulator
29 EXPORT  process_control_block
30 EXPORT  thread_array
31 EXPORT  force_next_thread
32
33 ; Beginning handler code
34 AREA  handler_irq, CODE
35
36 force_next_thread
37     ADD r14, r14, #4 ; Add 4 to the returning address in case it was not
38                     ; called from a interruption (forced switching)
39 ; Routine designed to the emulator, all the hardware IRQ is caused by the
    timer
40 handler_emulator
41     STMFD sp!, {r0 – r3, lr} ; Stacking r0 to r3 and the link register
42     B    handler_timer ; Branch to handler_timer
43
44 ; Routine designed to the board, have the Angel handler routine, button and
    timer
45 handler_board_angel
46     ; Save current context for APCS
47     STMFD sp!, {r0 – r3, lr} ; Stacking r0 to r3 and the link register
48     LDR  r0, IRQStatus ; r0 = irq type address
49     LDR  r0, [r0] ; r0 = irq type

```

```

50  TST    r0, #0x0400      ; irq type == 0x0400?
51  BNE    handler_timer   ; If yes, go to handler_timer
52  TST    r0, #0x0001     ; irq type = 0x0001?
53  BNE    handler_button  ; If yes, go to handler_button
54  LDMFD  sp!, {r0 - r3, lr} ; If it is not any of them, restore r0-r3 and
    lr
55  LDR    pc, Angel_IRQ_Address ; and branch to the Angel routine
56
57  ; Routine designed to the board, not have the Angel handler routine, button
    and timer
58  handler_board_no_angel
59      ; Save current context for APCS
60      STMFD sp!, {r0 - r3, lr} ; Stacking r0 to r3 and the link register
61      LDR    r0, IRQStatus    ; r0 = irq type address
62      LDR    r0, [r0]         ; r0 = irq type
63      TST    r0, #0x0400     ; irq type == 0x0400?
64      BNE    handler_timer   ; If yes, go to handler_timer
65      TST    r0, #0x0001     ; irq type = 0x0001?
66      BNE    handler_button  ; If yes, go to handler_button
67      LDMFD  sp!, {r0 - r3, lr} ; If it is not any of them, restore r0-r3
    and lr
68      B      end_handler     ; and return
69
70  ; handler routine for the button interruption
71  handler_button
72      BL    button_irq       ; C routine for the button
73      B    no_thread_switch  ; End the handler
74
75  ; Timer interruption handler routine
76  handler_timer
77      STMFD  sp!, {r4 - r12}   ; Stack the rest of the registers (r4-r12)
78      BL    timer_irq         ; Clear timer interruption
79      LDMFD  sp!, {r4 - r12}   ; Load r4-12 registers again
80      LDR    r0, =current_thread_id ; r0 = current_thread_id address
81      LDR    r0, [r0]         ; r0 = current_thread_id
82                          ; Send to the next step r0 as the current
83                          ; thread ID
84
85  ; Finds out the next active thread id (send result in r1)
86  get_next_taskid_loop
87      CMP    r0, #9           ; r0 == 9? (it is the last thread?)
88      BEQ    last_thread      ; If yes, branch last_thread
89      ADD    r1, r0, #1       ; If not, r1 = r0 + 1

```

```

90  B    next_thread          ; and branch to next_thread
91  last_thread
92  MOV   r1, #1              ; r1 = 1
93  next_thread
94  SUB   r2, r1, #1          ; r2 = r1 - 1
95  MOV   r3, #4              ; r3 = 4
96  MUL   r2, r3, r2          ; r2 = r2 * r3
97  LDR   r3, =thread_array   ; r3 = thread_array bottom address
98  ADD   r2, r2, r3          ; r2 = r3 + r2
99  LDR   r2, [r2]            ; r2 = thread array content
100  CMP   r2, #1              ; thread array content = 1?
101  BEQ   set_addresses       ; If yes, branch to set_addresses
102                      ; Send to the next step the next active
103                      ; thread in r1
104  MOV   r0, r1              ; If not, r0 = r1
105  B     get_next_taskid_loop ; and loop to get_next_taskid_loop
106
107 ; Sets current and next thread PCB addresses
108 set_addresses
109  LDR   r2, =current_thread_id ; r2 = current thread id address
110  LDR   r2, [r2]              ; r2 = current thread id
111  CMP   r2, r1              ; Is r2 = current thread id ==
112                      ; next thread id
113  BEQ   no_thread_switch     ; If yes, branch to no_thread_switch
114 ; Setting current_task_addr
115  MOV   r0, #68              ; Else start thread switch. r0 = 68
116  MUL   r0, r2, r0          ; r0 = current thread id * 68
117  LDR   r2, =process_control_block ; r2 = PCB bottom
118  ADD   r0, r0, r2          ; r0 = PCB bottom + id * 68
119  LDR   r2, =current_task_addr ; r2 = current task addr addr
120  STR   r0, [r2]            ; current_task_addr = r0
121 ; Setting next_task_addr
122  MOV   r0, #68              ; r0 = 68
123  MUL   r0, r1, r0          ; r0 = next thread id * 68
124  LDR   r2, =process_control_block ; r2 = PCB_bottom
125  ADD   r0, r2, r0          ; r0 = PCB bottom + next id * 68
126  LDR   r2, =next_task_addr   ; r2 = next_task_addr addr
127  STR   r0, [r2]            ; next_task_addr = r0
128
129 ; Setting new current_thread_id
130  LDR   r0, =current_thread_id ; r0 = current_thread_id
131  STR   r1, [r0]            ; current_thread_id = next thread id
132

```

```

133 ; Carry out process switch
134 ; Reset and save IRQ stack
135 LDR    r0, =irq_stack_pointer    ; r0 = irq_stack_pointer addr
136 MOV    r1, sp                    ; r1 = irq stack pointer
137 ADD    r1, r1, #5*4              ; r1 = irq stack pointer + 5 (# of data in
138                                     ; the stack, r0-r3, lr) * 4 (size of a word)
139 STR    r1, [r0]                  ; irq_stack_pointer = irq stack pointer
140                                     ; without the data that will be removed next
141 LDMFD   sp!, {r0-r3, lr}          ; Restore the remaining registers
142 ; Load and position r13 to point into current PCB
143 LDR    r13, =current_task_addr    ; r13 = current task PCB bottom address
144                                     address
145 LDR    r13, [r13]                 ; r13 = current task PCB bottom address
146 SUB    r13, r13, #60              ; r13 = current task PCB bottom address - 60
147                                     ; to point to the right place for the stacking
148                                     ; (next step)
149 ; Store the current user registers in current PCB
150 STMIA   r13, {r0-r14}^            ; Stacks the r0-r14 registers in the PCB
151 MRS     r0, SPSR                  ; r0 = status register
152 STMDB   r13, {r0, r14}            ; Stacks r0 and r14
153 ; Load and position r13 to point into next PCB
154 LDR    r13, =next_task_addr       ; r13 = next task PCB bottom address
155                                     address
156 LDR    r13, [r13]                 ; r13 = next task PCB bottom address
157 SUB    r13, r13, #60              ; r13 = next task PCB bottom address - 60
158                                     ; to point to the right place for the stacking
159                                     ; (next step)
160 ; Load the next task and setup PSR
161 LDMNEDB r13, {r0, r14}            ; Restore r0 and r14 (IRQ mode)
162 MSRNE   spsr_cxsf, r0             ; Restore status register
163 LDMNEIA r13, {r0-r14}^            ; Restore r0-r14 for the user mode
164 NOP                                           ; NOP! (required for the above instruction)
165 ; Load the IRQ stack into r13_irq
166 LDR    r13, =irq_stack_pointer    ; r13 = stack pointer address address
167 LDR    r13, [r13]                 ; Restore previous stack pointer
168 B      end_handler                ; Go to the end
169
170 no_thread_switch
171 LDMFD   sp!, {r0-r3, lr}          ; Restore the remaining registers
172
173 end_handler
174 SUBS    pc, r14, #4               ; Process counter = IRQ mode link register - 4
175                                     ; (-4 is required for the pipeline)

```

```

174
175 ; Data area
176 AREA irq_vars, DATA
177
178 IRQStatus ; IRQ interrupt type address
179 DCD 0x03ff4004
180 Angel_IRQ_Address ; Reserved space for the Angel IRQ Interrupt address
181 DCD 0x00000000
182 current_thread_id ; Context task ID
183 DCD 0x0
184 current_task_addr ; Address of the PCB for the current Task
185 DCD 0x0
186 next_task_addr ; Address of the PCB for the next Task
187 DCD 0x0
188 irq_stack_pointer ; Copy of the IRQ stack
189 DCD 0x0
190 process_control_block ; PCB for all the tasks (each size = 68) Offsets =
    bottom +
191 % 612 ; 68 * process#
192 thread_array ; Thread status array, where each thread has one word to
    indicate
193 % 36 ; if it is active (1) or inactive (0). Offset = bottom + 4 *
    thread#
194
195 ; End of assembly code
196 END

```

B.12 interrupt/handler_swi.s

```

1 ;*****
2 ; KinOS – Microkernel for ARM Evaluator 7–T
3 ; Seniors project – Computer Engineering
4 ; Escola Politecnica da USP, 2009
5 ;
6 ; Felipe Giunte Yoshida
7 ; Mariana Ramos Franco
8 ; Vinicius Tosta Ribeiro
9 ;
10 ;
11 ;

```

```

12 ; The program was based on the mutex program by ARM — Strategic Support
    Group,
13 ; contained on the ARM Evaluator 7-T example CD, under the folder /
    Evaluator7-T/
14 ; source/examples/mutex/
15 ;*****
16
17
18 ; Software interrupt handling code
19
20 IMPORT routine_fork
21 IMPORT routine_exec
22 IMPORT routine_exit
23 IMPORT routine_print
24 IMPORT handler_emulator
25 IMPORT force_next_thread
26
27 EXPORT Angel_SWI_Address
28 EXPORT handler_swi
29
30 ; Beginning handler code
31 AREA handler, CODE
32
33 ; Software interruption routine handler
34 handler_swi
35     STMFD sp!,{r0-r12,lr}      ; Stack registers r0-12 and link register
36     LDR r0,[lr,#-4]            ; Calculate address of SWI instruction (r0 = lr
    -4)
37     BIC r0,r0,#0xff000000      ; Mask off top 8 bits of instruction to give
    SWI
38                               ; number
39     LDR r1, Angel_SWI_Number    ; r1 = Angel SWI Number
40     CMP r0, r1                 ; Compare SWI number to angel interrupt number
41     BEQ goto_angel             ; If it is angel interrupt, branch to goto_angel
42     MOV r1, #0                 ; r1 = 0
43     CMP r0, r1                 ; Compare SWI number to r1
44     BEQ os_swi                 ; If it is OS SWI, branch to os_swi
45
46 ; Go to Angel routine
47 goto_angel
48     LDMFD sp!,{r0-r12,lr}      ; Restore registers r0-12 and link register
49     LDR pc, Angel_SWI_Address ; Branch to the Angel
50

```

```

51 ; Operating system SWI handler, identify the routine
52 os_swi
53     LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers
54     STMFD  sp!,{r0-r12,lr} ; and stores them again (in order to clean the
        registers)
55     MOV    r1, #0          ; r1 = 0
56     CMP    r0, r1          ; Compare the first parameter to 0
57     BEQ    pre_routine_fork ; If it is equal, branch to the fork
58     MOV    r1, #1          ; r1 = 1
59     CMP    r0, r1          ; Compare the first parameter to 1
60     BEQ    pre_routine_exec ; If it is equal, branch to the exec
61     MOV    r1, #2          ; r1 = 2
62     CMP    r0, r1          ; Compare the first parameter to 2
63     BEQ    pre_routine_exit ; If it is equal, branch to the exit
64     MOV    r1, #3          ; r1 = 3
65     CMP    r0, r1          ; Compare the first parameter to 3
66     BEQ    pre_routine_print ; If it is equal, branch to the print
67     MOV    r1, #4          ; r1 = 4
68     CMP    r0, r1          ; Compare the first parameter to 4
69     BEQ    pre_routine_switch ; If it is equal, branch to the switch
70
71     LDMFD sp!,{r0-r12,pc}^ ; If it is an unidentified syscall, go back to
        the program,
72                             ; restoring the registers and putting the return address in
73                             ; the process counter
74
75 ; Fork caller
76 pre_routine_fork
77     LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers
78     STMFD  sp!,{r0-r12,lr} ; and stores them again (in order to clean the
        registers)
79     B routine_fork        ; Branch to the fork C routine
80
81 ; Exec caller
82 pre_routine_exec
83     LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers
84     STMFD  sp!,{r0-r12,lr} ; and stores them again (in order to clean the
        registers)
85     B routine_exec        ; Branch to the exec C routine
86
87 ; Exit caller
88 pre_routine_exit
89     LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers

```

```

90  STMFD    sp!,{r0-r12,lr} ; and stores them again (in order to clean the
    registers)
91  B routine_exit      ; Branch to the exit C routine
92
93  ; Print caller
94  pre_routine_print
95  LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers
96  STMFD    sp!,{r0-r12,lr} ; and stores them again (in order to clean the
    registers)
97  MOV     r0, r2      ; r0 = r2
98  BL  routine_print   ; Branch to the print C routine
99  LDMFD sp!,{r0-r12,pc}^; Return to the original function
100
101 ; Switch caller
102 pre_routine_switch
103 LDMFD sp!,{r0-r12,lr} ; Restore r0-r12 registers and link registers
104 B force_next_thread ; Branch to the switch routine
105
106 ; Data area
107 AREA swi_vars, DATA
108
109 Angel_SWI_Number      ; Identification number for the Angel SWI
110     DCD 0x00123456
111 Angel_SWI_Address     ; Reserved space for the Angel SWI Interrupt address
112     DCD 0x00000000
113
114 ; End of assembly code
115 END

```

B.13 interrupt/irq.h

```

1  /*****
2  *  IMPORT
3  *****/
4
5  #include "timer.h"
6
7
8  /*****
9  *  ROUTINES
10 *****/

```

```

11 |
12 | /* Installs a handler branch on the interrupt vector */
13 | void install_handler (unsigned handler_routine_address, unsigned *
    |     vector_address);

```

B.14 interrupt/irq.c

```

1 | /******
2 | KinOS – Microkernel for ARM Evaluator 7–T
3 | Seniors project – Computer Engineering
4 | Escola Politecnica da USP, 2009
5 |
6 | Felipe Giunte Yoshida
7 | Mariana Ramos Franco
8 | Vinicius Tosta Ribeiro
9 | */
10 |
11 | /*
12 | The program was based on the mutex program by ARM – Strategic Support
13 | Group,
14 | contained on the ARM Evaluator 7–T example CD, under the folder /
15 | Evaluator7–T/
16 | source/examples/mutex/
17 | *****
18 | /******
19 | * IMPORT
20 | *****
21 | /* C functions for hardware interruptions */
22 |
23 | #include "irq.h"
24 |
25 | /******
26 | * EXTERN
27 | *****
28 |
29 | /* Reserved spaces where the Angel IRQ/SWI addressess will be stored */
30 | extern int Angel_IRQ_Address;
31 | extern int Angel_SWI_Address;
32 |

```

```

33
34 /*****
35  * ROUTINES
36  *****/
37
38 /* Installs a handler branch on the interrupt vector */
39 void install_handler (unsigned handler_routine_address, unsigned *
    vector_address) {
40
41     /* Case it is running in the emulator or without angel */
42     if (emulator == 1 || emulator == 2) {
43         /* The instruction that will be put in the IRQ vector */
44         unsigned branch_to_handler_instruction;
45         /* Handler relative address */
46         unsigned offset;
47         /* -0x8 due to the pipeline, >> 2 due to the word alignment */
48         offset = ((handler_routine_address - (unsigned)vector_address - 0x8) >>
            2);
49         /* Add to the address, the branch instruction */
50         branch_to_handler_instruction = 0xea000000 | offset;
51         /* Put the instruction in the vector */
52         *vector_address = branch_to_handler_instruction;
53     }
54     /* Case it is running with the angel */
55     else {
56         /* Angel branch instruction */
57         unsigned Angel_branch_instruction;
58         /* Angel instruction */
59         unsigned *Angel_address;
60         /* Getting Angel branch instruction */
61         Angel_branch_instruction = *vector_address;
62         /* Separate the instruction from the address */
63         Angel_branch_instruction ^= 0xe59ff000;
64         /* Calculating absolute address */
65         Angel_address = (unsigned *) ((unsigned)vector_address +
            Angel_branch_instruction + 0x8);
66         /* Store address in the proper position */
67         if ((unsigned)vector_address == 0x18) {
68             Angel_IRQ_Address = *Angel_address;
69         }
70         else {
71             Angel_SWI_Address = *Angel_address;
72         }

```

```

73     /* Inserting handler instruction in the vector table */
74     *Angel_address = handler_routine_address;
75 }
76 }

```

B.15 interrupt/swi.h

```

1  /******
2  *  IMPORT
3  *  *****/
4
5  #include "constants.h"
6
7
8  /******
9  *  TYPEDEF
10 *  *****/
11
12 typedef void (*pt2Task)(int);
13
14
15 /******
16 *  MISC
17 *  *****/
18
19 /* SWI routine syscall */
20 __swi(OS_SWI) int syscall(int, int, pt2Task, int);
21
22
23 /* SWI routine syscall_print */
24 __swi(OS_SWI) int syscall_print(int, int, char*, int);
25
26
27 /******
28 *  ROUTINES
29 *  *****/
30
31 /* Calls the fork system call and return the child id or zero */
32 int fork (void);
33
34 /* Calls the exec system call */

```

```

35 void exec (int, pt2Task, int);
36
37 /* Calls the exit system call */
38 void exit (int);
39
40 /* Calls the print system call */
41 void print(char *str);
42
43 /* Calls the switch_thread system call */
44 void switch_thread (void);

```

B.16 interrupt/swi.c

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7–T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13   Group,
14  contained on the ARM Evaluator 7–T example CD, under the folder /
15   Evaluator7–T/
16   source/examples/mutex/
17  *****/
18
19 /*****
20  * IMPORT
21  *****/
22 #include "swi.h"
23
24
25 /*****
26  * ROUTINES

```

```

27  *****/
28
29  /* Calls the fork system call and return the child id or zero */
30  int fork(){
31      int pid = 0;
32      pid = syscall(0, 0, 0, 0);
33      return pid;
34  }
35
36  /* Calls the exec system call */
37  void exec(int process_id , pt2Task process_addr , int arg1){
38      syscall(1, process_id , process_addr , arg1);
39  }
40
41  /* Calls the exit system call */
42  void exit(int process_id){
43      syscall(2, process_id , 0, 0);
44  }
45
46  /* Calls the print system call */
47  void print(char *str) {
48      syscall_print(3, 0, str , 0);
49  }
50
51  /* Calls the switch_thread system call */
52  void switch_thread (void) {
53      syscall(4, 0, 0, 0);
54  }

```

B.17 mutex/mutex.h

```

1  *****
2  * EXTERNAL
3  *****/
4
5  extern unsigned volatile int semaphore_shell; // do not access directly
6  extern unsigned volatile int semaphore_example; // do not access directly
7
8  *****
9  * MACROS
10 *****/

```

```

11
12 #define WAIT_SHELL    while (semaphore_shell==1) {} mutex_lock_shell();
13 #define SIGNAL_SHELL  mutex_unlock_shell();
14
15 #define WAIT_EXAMPLE  while (semaphore_example==1) {} mutex_lock_example();
16 #define SIGNAL_EXAMPLE mutex_unlock_example();
17
18
19 /*****
20  * ROUTINES
21  *****/
22
23 /* Locks the shell semaphore */
24 void mutex_lock_shell (void);
25
26 /* Unlocks the shell semaphore */
27 void mutex_unlock_shell (void);
28
29 /* Locks the example semaphore */
30 void mutex_lock_example (void);
31
32 /* Unlocks the example semaphore */
33 void mutex_unlock_example (void);

```

B.18 mutex/mutex.c

```

1 /*****
2  KinOS – Microkernel for ARM Evaluator 7–T
3  Seniors project – Computer Engineering
4  Escola Politecnica da USP, 2009
5
6  Felipe Giunte Yoshida
7  Mariana Ramos Franco
8  Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13  Group,
14  contained on the ARM Evaluator 7–T example CD, under the folder /
15  Evaluator7–T/

```

```

14  source/examples/mutex/
15  *****/
16
17  /******
18  *  STATICS
19  *****/
20
21  unsigned volatile int semaphore_shell = 2; // this is a start value
22  unsigned volatile int semaphore_example = 2; // this is a start value
23
24
25  /******
26  *  ROUTINES
27  *****/
28
29  /* Locks the shell semaphore */
30  void mutex_lock_shell (void) {
31
32      __asm {
33          spin:
34          mov    r1, &semaphore_shell
35          mov    r2, #1
36          swp    r3, r2, [r1]
37          cmp    r3, #1
38          beq    spin
39      }
40  }
41
42  /* Unlocks the shell semaphore */
43  void mutex_unlock_shell (void) {
44      __asm {
45          mov    r1, &semaphore_shell
46          mov    r2, #0
47          swp    r0, r2, [r1]
48      }
49  }
50
51  /* Locks the example semaphore */
52  void mutex_lock_example (void) {
53
54      __asm {
55          spin:
56          mov    r1, &semaphore_example

```

```

57     mov    r2, #1
58     swp    r3, r2, [r1]
59     cmp    r3, #1
60     beq    spin
61 }
62 }
63
64 /* Unlocks the example semaphore */
65 void mutex_unlock_example (void) {
66     __asm {
67         mov    r1, &semaphore_example
68         mov    r2, #0
69         swp    r0, r2, [r1]
70     }
71 }

```

B.19 peripherals/button.h

```

1  /* *****
2   * IMPORT
3   ***** */
4
5  #include "constants.h"
6  #include "terminal.h"
7  #include "tasks.h"
8
9
10 /* *****
11  * ROUTINES
12  ***** */
13
14 /* Initializes the button */
15 void button_init (void);
16
17 /* Handles a button interruption */
18 void button_irq (void);

```

B.20 peripherals/button.c

```

1  /* *****

```

```

2  KinOS – Microkernel for ARM Evaluator 7-T
3  Seniors project – Computer Engineering
4  Escola Politecnica da USP, 2009
5
6  Felipe Giunte Yoshida
7  Mariana Ramos Franco
8  Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13   Group,
14   contained on the ARM Evaluator 7-T example CD, under the folder /
15   Evaluator7-T/
16   source/examples/mutex/
17   *****/
18 /******
19  * IMPORT
20   *****/
21
22 /* This file contains routines to initialize and handle button
23   interruptions */
24
25 #include "button.h"
26
27 /******
28  * ROUTINES
29   *****/
30
31 /* Initializes the button */
32 void button_init (void) {
33     /* Force global disable off */
34     *(volatile int*)EvaluatorIRQTimerControl &= ~((1 << 21) | (1<<10) |
35         (1<<0));
36     /* Enable int0 */
37     *(unsigned *)IRQButtonControl |= 1 << 4;
38     /* Set as active high */
39     *(unsigned *)IRQButtonControl |= 1 << 3;
40     /* Allow for rising edge */
41     *(unsigned *)IRQButtonControl|= 1;

```

```

41 }
42
43 /* Handles a button interruption */
44 void button_irq (void) {
45     *(unsigned *) IRQStatus |= 1;
46
47     /* Do something */
48
49     /* Call the function to kill all tasks with pid > 1 */
50     print("\r\n");
51     run_end("all");
52
53 }

```

B.21 peripherals/dips.h

```

1  /* *****
2   * IMPORT
3   *****
4
5  #include "constants.h"
6
7
8  /* *****
9   * ROUTINES
10  *****
11
12 /* Return the value of the dip switches */
13 unsigned dips_read (void);

```

B.22 peripherals/dips.c

```

1  /* *****
2   KinOS – Microkernel for ARM Evaluator 7–T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro

```

```

9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
    Group,
13  contained on the ARM Evaluator 7–T example CD, under the folder /
    Evaluator7–T/
14  source/examples/mutex/
15  *****/
16
17
18 /******
19  * IMPORT
20  *****/
21
22 /* This file contains routines to initialize and handle DIPS interruptions
    */
23
24 #include "dips.h"
25
26
27 /******
28  * ROUTINES
29  *****/
30
31 /* Return the value of the dip switches */
32 unsigned dips_read (void)
33 {
34     /* 0xf = switch mask */
35     return 0xF & *IOData;
36 }

```

B.23 peripherals/led.h

```

1  /******
2  * MACROS
3  *****/
4
5  /* LED changing functions */
6
7  #define LEDBANK    *((unsigned *)0x03ff5008)

```

```

8
9 #define LED_4_ON      (LEDBANK=LEDBANK|0x00000010)
10 #define LED_3_ON      (LEDBANK=LEDBANK|0x00000020)
11 #define LED_2_ON      (LEDBANK=LEDBANK|0x00000040)
12 #define LED_1_ON      (LEDBANK=LEDBANK|0x00000080)
13 #define LED_4_OFF      (LEDBANK=LEDBANK&~0x00000010)
14 #define LED_3_OFF      (LEDBANK=LEDBANK&~0x00000020)
15 #define LED_2_OFF      (LEDBANK=LEDBANK&~0x00000040)
16 #define LED_1_OFF      (LEDBANK=LEDBANK&~0x00000080)

```

B.24 peripherals/segment.h

```

1  /*****
2   * IMPORT
3   *****/
4
5  #include "constants.h"
6
7
8  /*****
9   * ROUTINES
10  *****/
11
12  /* Initialize 7-segment display */
13  void segment_init (void);
14
15  /* Set number on the display */
16  void segment_set (int seg);

```

B.25 peripherals/segment.c

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7-T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */

```

```

10
11  /*
12   The program was based on the mutex program by ARM – Strategic Support
13   Group,
14   contained on the ARM Evaluator 7–T example CD, under the folder /
15   Evaluator7–T/
16   source/examples/mutex/
17   *****/
18   /******
19   * IMPORT
20   * *****/
21   /* This file contains routines to initialize and handle the 7 segment
22   display */
23   #include "segment.h"
24
25   /******
26   * STATICS
27   * *****/
28
29   /* Calculates the proper display addresses value according to the number */
30   static unsigned int numeric_display [16] = {
31     DISP_0,
32     DISP_1,
33     DISP_2,
34     DISP_3,
35     DISP_4,
36     DISP_5,
37     DISP_6,
38     DISP_7,
39     DISP_8,
40     DISP_9,
41     DISP_A,
42     DISP_B,
43     DISP_C,
44     DISP_D,
45     DISP_E,
46     DISP_F
47   };
48
49

```

```

50  /*****
51  *  ROUTINES
52  *****/
53
54  /* Set number on the display */
55  void segment_set (int seg) {
56      if ( seg >= 0 & seg <= 0xf ) {
57          *IOWData    &= ~Segment_mask;
58          *IOWData    |= numeric_display[seg];
59      }
60  }
61
62  /* Initialize 7-segment display */
63  void segment_init (void) {
64      *IOPMod |= Segment_mask;
65      *IOWData |= Segment_mask;
66  }

```

B.26 peripherals/serial.h

```

1  /*****
2  *
3  *  ARM Strategic Support Group
4  *
5  *****/
6
7  /*****
8  *
9  *  Module      : serial.h
10 *  Description : simple code to drive the serial port on the
11 *               Evaluator7T.
12 *  Tool Chain  : ARM Developer Suite 1.0
13 *  Platform    : Evaluator7T
14 *  History     :
15 *
16 *    2000-3-29 Andrew N. Sloss
17 *    - started serial module
18 *
19 *****/
20
21 /*****

```

```

22  * IMPORT
23  *****/
24
25  // none...
26
27  /**
28  * MACROS
29  *****/
30
31  #define BAUD_9600      (162 << 4)
32
33  #define COM1DEBUG      (1)
34  #define COM0_USER      (0)
35
36  /**
37  * DATATYPES
38  *****/
39
40  // none...
41
42  /**
43  * STATICS
44  *****/
45
46  // none...
47
48  /**
49  * ROUTINES
50  *****/
51
52  /* — serial_initcom0user —————
53  *
54  * Description : initializes the USER/COM0 serial port.
55  *
56  * Parameters : unsigned baudrate — baudrate i.e. 9600
57  * Return      : none...
58  * Notes       : none...
59  *
60  */
61
62  void serial_initcom0user (unsigned baudrate);
63
64

```

```

65  /* — serial_initcom1debug —————
66  *
67  * Description : initializes the DEBUG/COM1 serial port.
68  *
69  * Parameters : unsigned baudrate — baudrate i.e. 9600
70  * Return : none...
71  * Notes : none...
72  *
73  */
74
75  void serial_initcom1debug (unsigned baudrate);
76
77
78  /* — serial_print —————
79  *
80  * Description : print out a string through the com port
81  *
82  * Parameters : unsigned port — USER/DEBUG
83  *               : char *s — string to be printed out.
84  * Return : none...
85  * Notes : none...
86  *
87  */
88
89  void serial_print (unsigned port, char *s);
90
91
92  /* — serial_getkey —————
93  *
94  * Description : standard implementation of getkey.
95  *
96  * Parameters : none...
97  * Return : none...
98  * Notes :
99  *
100  *      waits until a key is pressed then echo's back.
101  *
102  */
103
104  void serial_getkey (void);
105
106
107  /* — serial_getkey —————

```

```

108  *
109  * Description : standard implementation of getkey.
110  *
111  * Parameters : none...
112  * Return : none...
113  * Notes :
114  *
115  *      waits until a key is pressed then echoes back.
116  *
117  */
118  char serial_getchar(void);
119
120
121
122  /*****
123  * END OF serial.h
124  *****/

```

B.27 peripherals/serial.c

```

1  /*****
2  *
3  * ARM Strategic Support Group
4  *
5  *****/
6
7  /*****
8  *
9  * Module : serial.c
10 * Description : simple code to drive the serial port on the
11 *      Evaluator7T.
12 * Tool Chain : ARM Developer Suite 1.0
13 * Platform : Evaluator7T
14 * History :
15 *
16 *      2000-3-29 Andrew N. Sloss
17 *      - started serial module
18 *
19 *****/
20
21 /*****

```

```

22  * IMPORT
23  *****/
24
25  // none...
26
27  /* *****/
28  * MACROS
29  *****/
30
31  #define SYSCFG      (0x03ff0000)
32  #define UART0_BASE  (SYSCFG + 0xD000)
33  #define UART1_BASE  (SYSCFG + 0xE000)
34
35  /*
36  * Serial settings .....
37  */
38
39  #define ULCON 0x00
40  #define UCON  0x04
41  #define USTAT 0x08
42  #define UTXBUF 0x0C
43  #define URXBUF 0x10
44  #define UBRDIV 0x14
45
46  /*
47  * Line control register bits .....
48  */
49
50  #define ULCR8bits  (3)
51  #define ULCRS1StopBit (0)
52  #define ULCRNoParity (0)
53
54  /*
55  * UART Control Register bits .....
56  */
57
58  #define UCRRxM  (1)
59  #define UCRRxSI (1 << 2)
60  #define UCRTxM  (1 << 3)
61  #define UCRLPB  (1 << 7)
62
63  /*
64  * UART Status Register bits

```

```

65  */
66
67  #define USROverrun      (1 << 0)
68  #define USRParity      (1 << 1)
69  #define USRFraming     (1 << 2)
70  #define USRBreak      (1 << 3)
71  #define USRDTR         (1 << 4)
72  #define USRRxData      (1 << 5)
73  #define USRTxHoldEmpty (1 << 6)
74  #define USRTxEmpty     (1 << 7)
75
76  /* default baud rate value */
77
78  #define BAUD_9600      (162 << 4)
79
80  // UART registers are on word aligned, D8
81
82  /* UART primitives */
83
84  #define GET_STATUS(p) (*(volatile unsigned *)((p) + USTAT))
85  #define RX_DATA(s)    ((s) & USRRxData)
86  #define GET_CHAR(p)   (*(volatile unsigned *)((p) + URXBUF))
87  #define TX_READY(s)   ((s) & USRTxHoldEmpty)
88  #define PUT_CHAR(p,c) (*(unsigned *)((p) + UTXBUF) = (unsigned )(c))
89
90  #define COMLDEBUG (1)
91  #define COM0_USER (0)
92
93  /* — serial_init —————
94  *
95  * Description : wait until a key is press from the host PC.
96  *
97  * Parameters : unsigned int port — com port either USER/DEBUG
98  *              : unsigned int baud — baud rate i.e. 9600
99  * Return      : none...
100 * Notes       : none...
101 *
102 */
103
104 void serial_init (unsigned int port, unsigned int baud)
105 {
106     /* Disable interrupts */
107     *(volatile unsigned *) (port + UCON) = 0;

```

```

108
109  /* Set port for 8 bit, one stop, no parity */
110  *(volatile unsigned *) (port + ULCON) = (ULCR8bits);
111
112  /* Enable interrupt operation on UART */
113  *(volatile unsigned *) (port + UCON) = UCRRxM | UCRTxM;
114
115  /* Set baud rate */
116  *(volatile unsigned *) (port + UBRDIV) = baud;
117
118 }
119
120 /* — serial_initcom0user —————
121  *
122  * Description : initializes the USER/COM0 serial port.
123  *
124  * Parameters : unsigned baudrate — baudrate i.e. 9600
125  * Return    : none...
126  * Notes     : none...
127  *
128  */
129
130 void serial_initcom0user (unsigned baudrate)
131 {
132     serial_init(UART0_BASE, baudrate);
133 }
134
135 /* — serial_initcom1debug —————
136  *
137  * Description : initializes the DEBUG/COM1 serial port.
138  *
139  * Parameters : unsigned baudrate — baudrate i.e. 9600
140  * Return    : none...
141  * Notes     : none...
142  *
143  */
144
145 void serial_initcom1debug (unsigned baudrate)
146 { serial_init(UART1_BASE, baudrate); }
147
148 /* — serial_print —————
149  *
150  * Description : print out a string through the com port

```

```

151  *
152  * Parameters : unsigned port – USER/DEBUG
153  *       : char *s – string to be printed out.
154  * Return    : none...
155  * Notes     : none...
156  *
157  */
158
159 void serial_print (unsigned port, char *s)
160 {
161     while ( *s != 0 || *s != '\0' ) {
162         switch (port) {
163             case COM0_USER:
164                 while ( TX_READY(GET_STATUS(UART0_BASE))==0);
165                 PUT_CHAR(UART0_BASE,*s++);
166                 break;
167             case COM1_DEBUG:
168                 while ( TX_READY(GET_STATUS(UART1_BASE))==0);
169                 PUT_CHAR(UART1_BASE,*s++);
170                 break;
171         }
172     }
173 }
174
175 /* — serial_getkey —————
176  *
177  * Description : standard implementation of getkey.
178  *
179  * Parameters : none...
180  * Return    : none...
181  * Notes     :
182  *
183  *       waits until a key is pressed then echoes back.
184  *
185  */
186
187 void serial_getkey (void)
188 {
189     char c;
190
191     while ( (RX_DATA(GET_STATUS(UART0_BASE)))==0 );
192
193     c = GET_CHAR(UART0_BASE);

```

```

194
195     while ( TX_READY(GET_STATUS(UART0_BASE))==0);
196     PUT_CHAR(UART0_BASE, c);
197 }
198
199
200
201 /* — serial_getkey —————
202  *
203  * Description : standard implementation of getkey.
204  *
205  * Parameters : none...
206  * Return : none...
207  * Notes :
208  *
209  *     waits until a key is pressed then echoes back.
210  *
211  */
212
213 char serial_getchar(void)
214 {
215     char c;
216
217     while ( (RX_DATA(GET_STATUS(UART0_BASE)))==0 );
218
219     c = GET_CHAR(UART0_BASE);
220
221     while ( TX_READY(GET_STATUS(UART0_BASE))==0);
222     PUT_CHAR(UART0_BASE, c);
223
224     return c;
225 }
226
227
228
229 /*****
230  * END OF serial.c
231  *****/

```

B.28 peripherals/timer.h

```

1  /*****
2   * IMPORT
3   *****/
4
5  #include "constants.h"
6
7
8  /*****
9   * ROUTINES
10  *****/
11
12 /* Initiate timer settings */
13 void timer_init (void);
14
15 /* Restart timer interrupt */
16 void timer_irq (void);
17
18 /* Start timer */
19 void timer_start (void);

```

B.29 peripherals/timer.c

```

1  /*****
2   KinOS – Microkernel for ARM Evaluator 7–T
3   Seniors project – Computer Engineering
4   Escola Politecnica da USP, 2009
5
6   Felipe Giunte Yoshida
7   Mariana Ramos Franco
8   Vinicius Tosta Ribeiro
9  */
10
11 /*
12  The program was based on the mutex program by ARM – Strategic Support
13   Group,
14   contained on the ARM Evaluator 7–T example CD, under the folder /
15   Evaluator7–T/
16   source/examples/mutex/
17  *****/

```

```

18  * IMPORT
19  *****/
20
21  /* This file contains routines to initialize and handle timer interruptions
    */
22
23  #include "timer.h"
24
25  /******
26  * ROUTINES
27  *****/
28
29  /* Initiate timer settings */
30  void timer_init (void) {
31      /* Case it's from the emulator */
32      if (emulator == 1) {
33          /* Clear/disable all interrupts */
34          *IRQEnableClear = ~0;
35          /* Disable counters by clearing the control bytes */
36          *EmulatorIRQTimerControl = 0;
37          /* Clear counter/timer interrupts */
38          *IRQTimerClear = 0 ;
39      }
40      /* Case it's the board */
41      else {
42          /* Disable interrupt */
43          *TimerEnableSet = 0;
44          /* Clear pending interrupts */
45          *IRQStatus = 0x00000000;
46      }
47  }
48
49  /* Restart timer interrupt */
50  void timer_irq(void) {
51      if (emulator == 1) {
52          /* Clear the interrupt */
53          *IRQTimerClear = 0;
54      }
55      else {
56          /* Clear pending interrupts */
57          *IRQStatus = 1 << 10;
58          /* Load counter values */
59          *EvaluatorIRQTimerLoad = COUNTDOWN;

```

```

60      /* Unmask the interrupt source */
61      *(volatile int*)EvaluatorIRQTimerControl &= ~((1<<21) | (1<<10) |
62      (1<<0));
63  }
64  }
65  /* Start timer */
66  void timer_start (void) {
67      if (emulator == 1) {
68          /* Load counter values */
69          *EmulatorIRQTimerLoad = COUNTDOWN;
70          /* Enable the Timer | Periodic Timer producing interrupt | Set Maximum
71             Prescale - 8 bits */
72          *EmulatorIRQTimerControl = (0x80 | 0x40 | 0x08 );
73          /* Enable interrupt */
74          *IRQEnableSet = IRQTimer;
75      }
76      else {
77          /* Load counter values */
78          *EvaluatorIRQTimerLoad = COUNTDOWN;
79          /* Enable interrupt */
80          *TimerEnableSet |= 0x1;
81          /* Unmask the interrupt source */
82          *(volatile int*)EvaluatorIRQTimerControl &= ~((1 << 21) | (1 << 10) |
83          (1 << 0));
84      }
85  }

```

B.30 syscalls/exec.s

```

1  ;*****
2  ; KinOS - Microkernel for ARM Evaluator 7-T
3  ; Seniors project - Computer Engineering
4  ; Escola Politecnica da USP, 2009
5  ;
6  ; Felipe Giunte Yoshida
7  ; Mariana Ramos Franco
8  ; Vinicius Tosta Ribeiro
9  ;
10 ;
11 ;

```

```

12 ; The program was based on the mutex program by ARM – Strategic Support
    Group,
13 ; contained on the ARM Evaluator 7–T example CD, under the folder /
    Evaluator7–T/
14 ; source/examples/mutex/
15 ;*****
16
17
18 ; Exec system call
19
20 EXPORT routine_exec
21
22 IMPORT process_control_block
23
24 ; Beginning fork code
25 AREA exec, CODE
26
27 ; From the call of the function: r1 = task id, r2 = task address
28 routine_exec
29 ; Store variables
30 STMFD sp!,{r0–r12,lr} ; Push r0–12 in the stack
31
32 MOV r6, r3 ; r6 = value of the first argument
33
34 ; Put the task address in task_pcb_address – 4 (Process counter)
35
36 MOV r0, r2 ; r0 = task address
37 ADD r0, r0, #4 ; r0 = task address + 4 (+4 due to the pipeline
    )
38 LDR r3, =process_control_block ; r3 = PCB bottom
39 MOV r4, #68 ; r4 = 68
40 MUL r5, r1, r4 ; r5 = (task id) * 68
41 ADD r3, r3, r5 ; r3 = PCB bottom + (task id) * 68
42 SUB r3, r3, #4 ; r3 = r3 – 4
43 STR r0, [r3] ; MEM[r3] = r0
44
45 ; Set up user stack for the task
46 SUB r3, r3, #4 ; r3 = r3 – 4 (stack pointer)
47 MOV r4, #0x20000 ; r4 = SP_USER_BOTTOM
48 loop
49 SUB r1, r1, #1 ; r1 = task id – 1
50 CMP r1, #0 ; r1 = 0 ?
51 BEQ end_loop ; if equal, end_loop

```

```

52 SUB    r4, r4, #4048      ; r0 = r4 - 4048 (next stack)
53 B      loop              ; Go to next stack
54 end_loop
55 STR    r4,[r3]            ; MEM[r3] = r4 (the process stack pointer)
56
57 ; Set up the r0
58 SUB    r3,r3,#52          ; r3 = r3 - 52
59 STR    r6,[r3]
60
61 ; Set up link register
62 SUB    r3, r3, #4          ; r3 = r3 - 4 (link register)
63 MOV    r0, r2              ; r0 = task address
64 ADD    r0, r0, #4          ; r0 = r0 - 4
65 STR    r0, [r3]           ; MEM[r3] = r0
66
67 ; Set up SPSR
68 SUB    r3, r3, #4          ; r3 = r3 - 4
69 MOV    r0, #0x10          ; r0 = 0x10 (user mode)
70 STR    r0, [r3]           ; MEM[r3] = r0
71
72 ; Return
73 LDMFD  sp!, {r0-r12,pc}^ ; Pop r0-r12 and link register to process counter
74
75 ; End of assembly code
76 END

```

B.31 syscalls/exit.s

```

1  ;*****
2  ; KinOS – Microkernel for ARM Evaluator 7-T
3  ; Seniors project – Computer Engineering
4  ; Escola Politecnica da USP, 2009
5  ;
6  ; Felipe Giunte Yoshida
7  ; Mariana Ramos Franco
8  ; Vinicius Tosta Ribeiro
9  ;
10 ;
11 ;
12 ; The program was based on the mutex program by ARM – Strategic Support
    Group,

```

```

13 ; contained on the ARM Evaluator 7-T example CD, under the folder /
    Evaluator7-T/
14 ; source/examples/mutex/
15 ;*****
16
17
18 ; Exec system call
19
20 EXPORT routine_exit
21
22 IMPORT thread_array
23
24 ; Beginning fork code
25 AREA exit, CODE
26
27 ; r1 comes as task id
28 routine_exit
29 STMFd sp!,{r0-r12, lr} ; save registers
30 MOV r2, r1 ; r2 = task id
31 LDR r0, =thread_array ; r0 = thread_array
32 MOV r1, #0 ; r1 is the state value = inactive
33 SUB r2, r2, #1 ; r2 = task id - 1
34 MOV r3, #4 ; r3 = 4
35 MUL r4, r2, r3 ; r4 = (task id - 1) * 4
36 ADD r4, r0, r4 ; r4 = thread_array + (task id - 1) * 4
37 STR r1, [r4] ; Mem[r4] = r1 (inactive)
38
39 LDMFD sp!,{r0-r12, pc}^ ; return
40
41 ; End of assembly code
42 END

```

B.32 syscalls/fork.s

```

1 ;*****
2 ; KinOS - Microkernel for ARM Evaluator 7-T
3 ; Seniors project - Computer Engineering
4 ; Escola Politecnica da USP, 2009
5 ;
6 ; Felipe Giunte Yoshida
7 ; Mariana Ramos Franco

```

```

8 ; Vinicius Tosta Ribeiro
9 ;
10 ;
11 ;
12 ; The program was based on the mutex program by ARM – Strategic Support
    Group,
13 ; contained on the ARM Evaluator 7-T example CD, under the folder /
    Evaluator7-T/
14 ; source/examples/mutex/
15 ;*****
16
17
18 ; Fork system call
19
20 IMPORT  thread_array
21 IMPORT  process_control_block
22 IMPORT  current_thread_id
23
24 EXPORT  routine_fork
25
26 ; Beginning fork code
27 AREA  fork, CODE
28
29 ; Routine to duplicate a process code
30 routine_fork
31 ; Stacks current state twice
32 STMFD  sp!,{r1-r12,lr} ; Stacks the link register and r1-r12
33 STMFD  sp!,{r0-r12} ; Stacks r0-r12
34 STMFD  sp!,{lr} ; Stacks the link register (In a separate
    instruction
35 ; to stack it in the top)
36
37 ; Finds the first available space in the process table (return id in r0 and
    its address in r1)
38 LDR  r1, =thread_array ; r1 = bottom of the thread array address
39 MOV  r0, #1 ; r0 = 1
40 routine_fork_loop
41 LDR  r2, [r1] ; r2 = thread array position
42 CMP  r2, #0 ; r2 = 0?
43 BEQ  pcb_bottom ; If the position is available (r2 = 0), go to
    pcb_bottom
44 ADD  r0, r0, #1 ; r0 = r0 + 1 (next id)
45 CMP  r0, #10 ; Is this the last thread slot being checked?

```

```

46  BEQ   fork_fail      ; if it is, there is no available slot, go to
    fork_fail
47  ADD   r1, r1, #4      ; r1 = r1 + 4 (next address)
48  B     routine_fork_loop ; Check next slot (go to routine_fork_loop)
49
50 ; Get the PCB bottom of the new process (return it in r2)
51 pcb_bottom
52  LDR   r2, =process_control_block ; r2 = pcb_bottom
53  MOV   r3, #68          ; r3 = 68
54  MUL   r3, r0, r3        ; r3 = 68 * available thread id
55  ADD   r2, r2, r3        ; r2 = pcb bottom + (thread id * 68)
56
57 ; Retrieves user mode stack pointer (returns it in r3)
58  SUB   r13, r13, #4     ; Opens a space in the stack
59  STMIA r13, {r13}^      ; Store user mode stack pointer in the SVC stack
60  NOP                      ; No operation (necessary for the above instruction)
61  LDMFD sp!, {r3}        ; r3 = user mode stack pointer
62
63 ; Retrieves user mode stack base (returns in r4)
64  MOV   r4, #0x20000      ; r4 = 0x20000 (User mode stack pointer base)
65  MOV   r6, #4048         ; r6 = 4048 (Distance between each thread stack)
66  LDR   r5, =current_thread_id ; r5 = current thread id address
67  LDR   r5, [r5]          ; r5 = current thread id
68  SUB   r5, r5, #1        ; r5 = current thread id - 1
69  MUL   r6, r5, r6        ; r6 = (current thread id - 1) * 4048
70  SUB   r4, r4, r6        ; r4 = 0x20000 - (current thread id - 1) * 4048
71                      ; (this is the base of the current thread stack)
72
73 ; Retrieves new thread stack base (returns in r5)
74  MOV   r5, #0x20000      ; r5 = 0x20000 (User mode stack pointer base)
75  MOV   r6, #4048         ; r6 = 4048 (Distance between each thread stack)
76  SUB   r7, r0, #1        ; r7 = new thread id - 1
77  MUL   r6, r7, r6        ; r6 = (new thread id - 1) * 4048
78  SUB   r5, r5, r6        ; r5 = 0x20000 - ((new thread id - 1) * 4048)
79
80 ; Duplicates stack
81 loop_stack_copy
82  LDR   r6, [r4]          ; r6 = original stack data
83  STR   r6, [r5]          ; Stores data in new stack (stack_top = r6)
84  CMP   r4, r3            ; Is this the top of the stack? (r4 == r3?)
85  BEQ   build_new_pcb     ; if it is, branch to build_new_pcb
86  SUB   r5, r5, #4        ; if not, go to next space in the new stack (r5 =
    r5 - 4)

```

```

87 SUB    r4, r4, #4      ; and next data in the original stack (r4 = r4 - 4)
88 B      loop_stack_copy ; restart sequence (go to loop_stack_copy)
89
90 build_new_pcb
91 ; Store SPSR
92 SUB    r2, r2, #68 ; r2 = r2 - 68 (r2 = PCB[-68] address)
93 MOV    r3, #0x10     ; r3 = #0x10 (User mode)
94 STR    r3, [r2]      ; PCB[-68] = #0x10
95
96 ; Store stack pointer
97 ADD    r2, r2, #60 ; r2 = r2 + 60 (r2 = PCB[-8] address)
98 STR    r5, [r2]      ; PCB[-8] = new stack pointer
99
100 ; Stores r14 and LR
101 ADD    r2, r2, #4 ; r2 = r2 + 4 (r2 = PCB[-4] address)
102 LDMFD  sp!, {r3} ; Restore link register from the stack to r3
103 ADD    r3, r3, #4 ; r3 = r3 + 4 (due to the pipeline)
104 STR    r3, [r2] ; PCB[-4] = return address
105 SUB    r2, r2, #60 ; r2 = r2 - 60 (r2 = PCB[-64] address)
106 STR    r3, [r2] ; PCB[-64] = return address
107
108 ; Copy registers
109 MOV    r3, #0 ; r3 = 0
110 MOV    r4, #12 ; r4 = 12
111 registers_loop
112 ADD    r2, r2, #4 ; r2 = r2 + 4 (Next PCB register space)
113 LDMFD  sp!, {r5} ; Restore register from the stack to r5
114 STR    r5, [r2] ; Store register in the PCB
115 CMP    r3, r4 ; r12 was copied? (r3 == r4?)
116 BEQ    enable_thread ; If yes, go to enable_thread
117 ADD    r3, r3, #1 ; r3 = r3 + 1 (Next register)
118 B      registers_loop ; Copy next register
119
120 ; Enable thread in the thread vector
121 enable_thread
122 MOV    r2, #1 ; r2 = 1
123 STR    r2, [r1] ; New process in thread array = 1
124 LDMFD  sp!, {r1-r12,pc}^ ; Restore all the registers but r0
125 ; (it contains the new process id)
126
127 ; Case when there is no thread space
128 fork_fail
129 LDMFD  sp!, {lr} ; Restore link register

```

```

130  LDMFD sp!, {r0-r12} ; Restore r0-r12
131  LDMFD sp!, {r1-r12} ; Restore r1-r12
132  MOV   r0, #0xFFFFFFFF ; r0 = -1 (r0 is the return value)
133  LDMFD sp!, {pc}^      ; Restore return address to the process counter
134
135  ; End of assembly code
136  END

```

B.33 syscalls/routine_print.h

```

1  /*****
2  * IMPORT
3  *****/
4
5  #include "serial.h"
6
7
8  /*****
9  * ROUTINES
10 *****/
11
12 /* print out a string through the user com port */
13 void routine_print(char *str);

```

B.34 syscalls/routine_print.c

```

1  /*****
2  KinOS – Microkernel for ARM Evaluator 7-T
3  Seniors project – Computer Engineering
4  Escola Politecnica da USP, 2009
5
6  Felipe Giunte Yoshida
7  Mariana Ramos Franco
8  Vinicius Tosta Ribeiro
9  */
10
11 /*
12 The program was based on the mutex program by ARM – Strategic Support
   Group,

```

```

13   contained on the ARM Evaluator 7-T example CD, under the folder /
14   Evaluator7-T/
15   source/examples/mutex/
16   *****/
17   /******
18   *  MACROS
19   *****/
20
21   #define SYSCFG    (0x03ff0000)
22   #define UART0_BASE (SYSCFG + 0xD000)
23   #define UART1_BASE (SYSCFG + 0xE000)
24
25   /*
26   *  Serial settings .....
27   */
28
29   #define ULCON 0x00
30   #define UCON  0x04
31   #define USTAT 0x08
32   #define UTXBUF 0x0C
33   #define URXBUF 0x10
34   #define UBRDIV 0x14
35
36   /*
37   *  Line control register bits .....
38   */
39
40   #define ULCR8bits  (3)
41   #define ULCRS1StopBit (0)
42   #define ULCRNoParity (0)
43
44   /*
45   *  UART Control Register bits .....
46   */
47
48   #define UCRRxM  (1)
49   #define UCRRxSI (1 << 2)
50   #define UCRTxM  (1 << 3)
51   #define UCRLPB  (1 << 7)
52
53   /*
54   *  UART Status Register bits

```

```

55  */
56
57 #define USROverrun      (1 << 0)
58 #define USRParity      (1 << 1)
59 #define USRFraming     (1 << 2)
60 #define USRBreak       (1 << 3)
61 #define USRDTR         (1 << 4)
62 #define USRRxData      (1 << 5)
63 #define USRTxHoldEmpty (1 << 6)
64 #define USRTxEmpty     (1 << 7)
65
66 /* default baud rate value */
67
68 #define BAUD_9600      (162 << 4)
69
70 // UART registers are on word aligned, D8
71
72 /* UART primitives */
73
74 #define GET_STATUS(p) (*(volatile unsigned *)((p) + USTAT))
75 #define RX_DATA(s)    ((s) & USRRxData)
76 #define GET_CHAR(p)   (*(volatile unsigned *)((p) + URXBUF))
77 #define TX_READY(s)   ((s) & USRTxHoldEmpty)
78 #define PUT_CHAR(p,c) (*(unsigned *)((p) + UTXBUF) = (unsigned )(c))
79
80 #define COM1DEBUG (1)
81 #define COM0_USER (0)
82
83 /*****
84  * ROUTINES
85  *****/
86
87 /* print out a string through the user com port */
88 void routine_print(char *str) {
89
90     while ( *str != 0 || *str != '\0' ) {
91         while ( TX_READY(GET_STATUS(UART0_BASE))==0);
92         PUT_CHAR(UART0_BASE,*str++);
93     }
94
95 }

```