TP3 - Sistemas Integrados em Chip (SoC) na Prática

1 FORMAÇÃO DOS GRUPOS

Formação dos grupos: A Turma toda formará um único grupo e realizará o trabalho começando pela subdivisão do mesmo em três partes ou módulos, os subsistemas processador, memória e periférico. Cada parte será atribuída a um subconjunto de alunos.

Cada subconjunto de alunos formado deve dividir sua parte do trabalho em etapas, de acordo com as características da parte/módulo. Estima-se que esta parte dure duas semanas.

Ao final do desenvolvimento das partes, deverá haver um processo de integração do sistema pelos subconjuntos de alunos que desenvolveram cada uma das partes do trabalho. Estima-se que esta parte dure também duas semanas.

Incentiva-se fortemente que haja pontos de verificação da capacidade de integração das partes, bem como para definir as interfaces entre as partes do sistema. As aulas da disciplina que seguem as da apresentação deste enunciado serão dedicadas para discussões do sistema integrado global e da definição das partes dos trabalho que integram os três módulos.

As notas do trabalho serão individuais, a partir da percepção pelo professor da qualidade do trabalho e do nível de esforço de cada aluno no processo de desenvolvimento da parte que lhe tocou, bem como pela capacidade demonstrada pelo mesmo para operar na evolução de pequenos e grandes grupos, sobretudo na fase de integração dos trabalhos parciais.

2 TRABALHO A SER DESENVOLVIDO E REGRAS DO JOGO

Um SoC para Criptografia

1. A ideia do trabalho é simples, embora sua confecção possa ser algo exigente. São fornecidos dois núcleos de propriedade intelectual (Intellectual Property Cores ou IPs), pré-projetados, pré-validados em simulação e prototipação e se pede para integrá-los.
    a. O primeiro é um sistema processador+memórias que contém uma versão simulável e prototipável do processador MIPS_S e memórias de instruções e dados construídas com BRAMs da Xilinx;
    b. O segundo é um módulo de criptografia DES (um padrão não mais usado por não ser muito seguro, mas muito parecido com versões de algoritmos modernos como o AES). Chamamos este módulo de hardware de um *criptocore*.
2. Os três grupos de trabalho devem se envolver com:
    a. O subsistema de memórias BRAMs, aumentando sua capacidade dos atuais 2Kbytes para instruções e 8Kbytes para dados. Sugere-se aumentar o subsistema para 80Kbytes, sendo 16Kbytes para instruções e 64Kbytes para dados;
    b. O subsistema do processador MIPS_S, sobre o qual deverá ser desenvolvido um software para interagir com o criptocore para enviar e receber dados deste;
    c. O criptocore, que deverá ser integrado ao sistema processador+memória pela criação de uma máquina de estados que se comunique com o software do

processador e acesse a memória de dados quando necessário, para ler ou escrever informações nesta.

3. A aplicação a desenvolver para este sistema integrado é simples:
    a. Inicialmente, existirá um texto carregado na memória de dados. Ele deve ter pelo menos 2Kbytes de tamanho;
    b. Este texto deverá ser criptografado pelo sistema e o resultado, ocupando exatamente o mesmo espaço será colocado na memória após o texto original;
    c. Em seguida, o sistema deverá tomar o texto criptografado e deve descriptografá-lo e colocar na memória o resultado, após o texto criptografado;
    d. Finalmente, o software no processador irá comparar o texto original com o resultado da descriptografia e ambos devem ser absolutamente idênticos.