Modern SoC Design on Arm
End-of-Chapter Exercises 0.4

Q1 Bus sizes

What is the addressable space of an A32D32 processor in terms of bytes and words?

Answer:

A32D32 means that both the address bus and data bus are 32-bits wide. In theory, 2^{32} 32-bit words could be addressed. However, byte addressing is used in all mainstream processors. There are 4 bytes in a 32-bit word, so it is the low two address bits that are used to index within a word, making the addressable space 2^{30} words which is 2^{32} bytes.

Q2 Address decoding and alignment

Why is the register space of an I/O device typically mapped so that its base address is a multiple of its length?

Answer:

From the point of view of device driver software, this makes little difference, but the address space decoding logic has a complexity issue with unaligned base addresses. As an example, consider a device with 128 bytes of internal address space. This would probably be organised as 32 words of 32 bits. An example addressing slot where the base address is aligned (is a multiple of its length) would be 0xE800_0400 to 0xE800_047F. An example address range where this condition does not hold is 0xE800_0420 to 0xE800_049F (32 bytes have been added on to each end). The aligned range is relatively easy to implement in hardware, requiring the top 32-7=25 address bits to be matched for a single value (using perhaps a 25-input AND gate). The unaligned range is slightly more complex to detect, and for the registers to remain in the same order as documented in the device's data sheet, an address adder has to be used, adding more logic, since the register select bit values are no longer the same as the low-order address bits.

Note, if the device is word-addressed and the processor is byte-addressed (the normal case these days), there will be 7-2=5 address bits selecting between the 32 internal register words.

Q3 What is a microcontroller?

What are the differences between a PC, a microprocessor, a SoC and a microcontroller? Are they clearly distinct?

Answer:

The standard definition of a microcontroller is that it has all parts of a computer, including main memory and some I/O devices all on one piece of silicon. On the other hand, a microprocessor does not have these two items: it just has the execution unit and control unit as defined in

this chapter. The term PC generally refers to a multi-chip computer conforming to the original IBM PC standard and its subsequent redefinitions over the years. The microcontroller is a SoC. Interestingly, the letter M in the Arm AMBA bus standard originally referred to microcontroller (Advanced Microcontroller Bus Architecture).

Q4 Memory Bandwidth

How would you estimate with a spreadsheet the external DRAM bandwidth needed by a SoC?

Answer:

Understanding the likely DRAM bandwidth needs is a very important step in every SoC design. The average bandwidth during heavy use periods is generally the most important statistic. DRAM is nearly always cached and caches can tend to smooth out peak demands, making the average more significant. Data traffic might be estimated to have 95 percent hit ratio in each level of cache. Instruction fetch traffic is likely to hit better, closer to 99 percent. Given the front-side performance needed and cache hit ratio estimates, the DRAM bandwidth need from processor can be estimated. Added on to this needs to be expected traffic level from uncached customers, such as device DMA.

The available DRAM bandwidth from a bank can be estimated from its peak transfer rate, given by the data bus width (e.g., 128 bits) and double data rate (e.g., 2 GHz). The average sustainable rate might be 70 percent of the peak rate but will vary very much according to the locality of reference.

Q5 Address Spaces

How could some peripheral devices be made unaddressable by some cores?

Answer:

A device could be completely isolated by the addressing hardware, meaning there is no address one core can make that will enable it to make a load or store on a particular I/O device. Since the I/O devices are likely to be on different busses, or bus segments, from a processor's connection to its primary storage, isolation would be a matter of making the interconnecting bus bridges not forward the transactions.

Software solutions also exist and are highly feasible in a virtualised/hypervisor environment. But these can also be practical if security is implemented with a trusted operating system. In either case, the VM translation tables are simply not programmed to map the device. Other software solutions rely on bytecoded VMs, like Java/DotNet being trusted. Secure boot is likely to be needed for all software solutions, including those using Trust Zones.