Hardware Black Magic:

Building devices with FPGAs

Dr. Fouad Kiamilev, Professor
CVORG Labs
Electrical and Computer Engineering
University of Delaware
http://cvorg.ece.udel.edu

Updated Slides and Video

Updated slides as well as video tutorials will be available after the conference on our website at http://www.cvorg.ece.udel.edu

Also during our talk, to keep things interesting during compilation we will be giving away swag in an attempt to keep you interested. See the slides towards the end for details.

What is CVORG?

- From “Dela-where?”
- Operate like a Pirate Ship, sailing where our curious minds take us!
- Interests in reverse engineering, custom hardware, red-teaming, security (especially hardware), networking, high speed communications, you name it, we love doing it!
- The Jack-of-all trades research group!

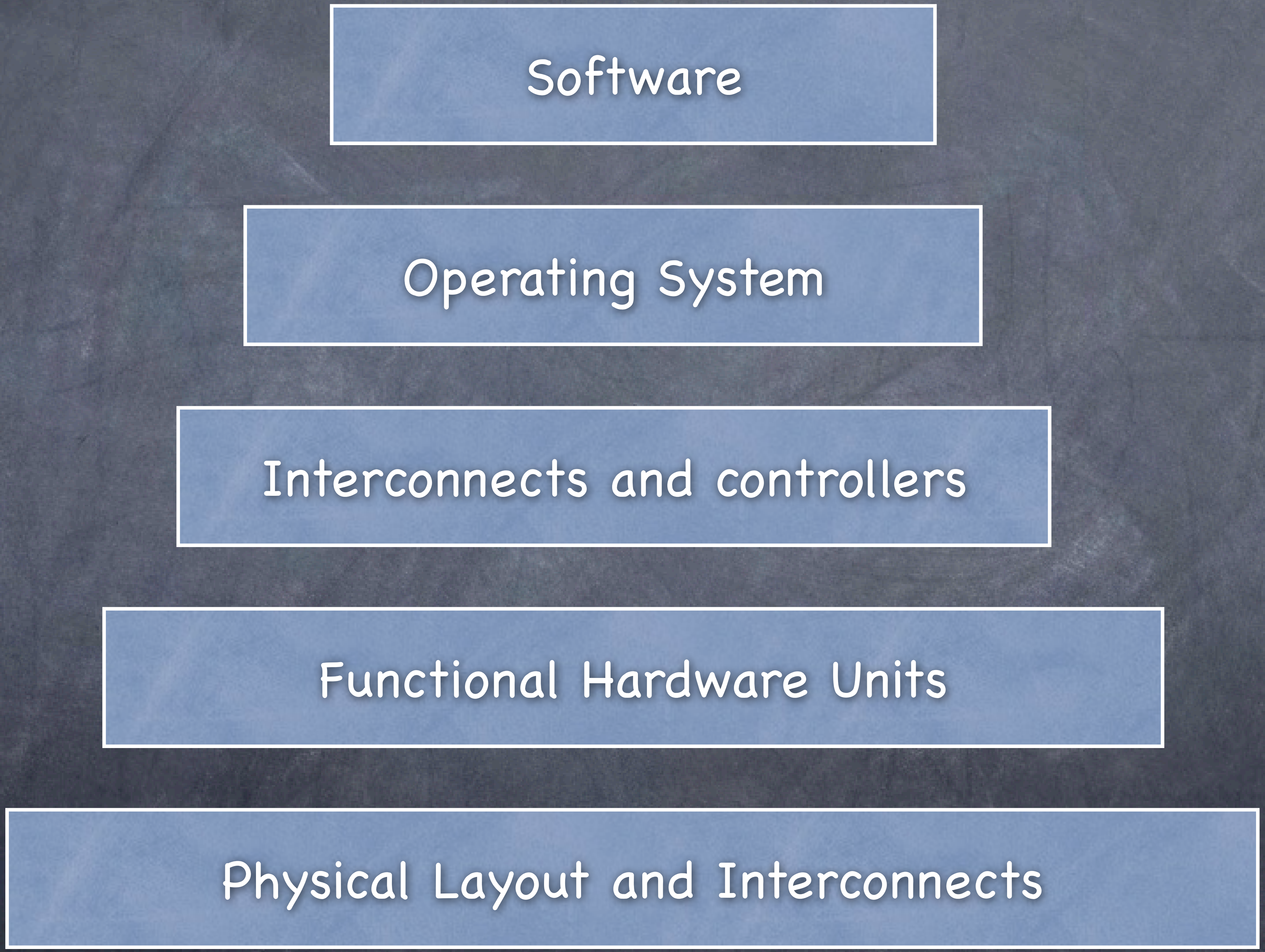
What are FPGAs

- Field-programmable gate arrays contains logic blocks that can reconfigured
- This allows a FPGA to be any moderately complex embedded device
- FPGA design tools cover the entire range of hardware and software design.
- For example, in the Xilinx world the ISE is mainly where you write HDL and the EDK is where you can write C.

Hardware

- While it can be scary, it should be embraced and not avoided
- For every software, there is hardware behind it
- Why spend hours hacking firmware to do what you want - make a device do it for you!

Embedded Design



Software

Operating System

Interconnects and controllers

Functional Hardware Units

Physical Layout and Interconnects

Choices for Digital System Development

- Processor?
  Easy to write code, expensive chips, ok performance, power hungry

- Gate Array (ASIC)?
  Very high performance, low power, very hard to design, expensive to manufacture

- Field-Programmable Gate Array?
  no manufacturing needed (just program), easier to design than ASIC, high performance, lower power

What uses FPGAs?

Printers

Set-Top Boxes

Networking Equipment

Large Integrated Systems

FPGA's Advantage:
Application specific speed
802.11 key cracking

- PC jc-wepcrack
  1.25 GHz G4 150,000/sec
  3.6 GHz P4 300,000/sec

- PS3 cbe-client
  1 SPU 3.2 GHz 241,000/sec
  6 SPU 3.2 GHz 1,446,000/sec

- FPGA pico-wepcrack
  1 Virtex-4 LX-25 12,000,000/sec

- PC wpa-crack
  800 MHz P3 25/sec
  3.6 GHz P4 60/sec
  2.16 GHz Intel Duo 70/sec

- FPGA coWPAtty
  1 Virtex-4 LX-20 380/sec
  1 Virtex-4 LX-25 430/sec
  1 Virtex-4 LX-60 1000/sec

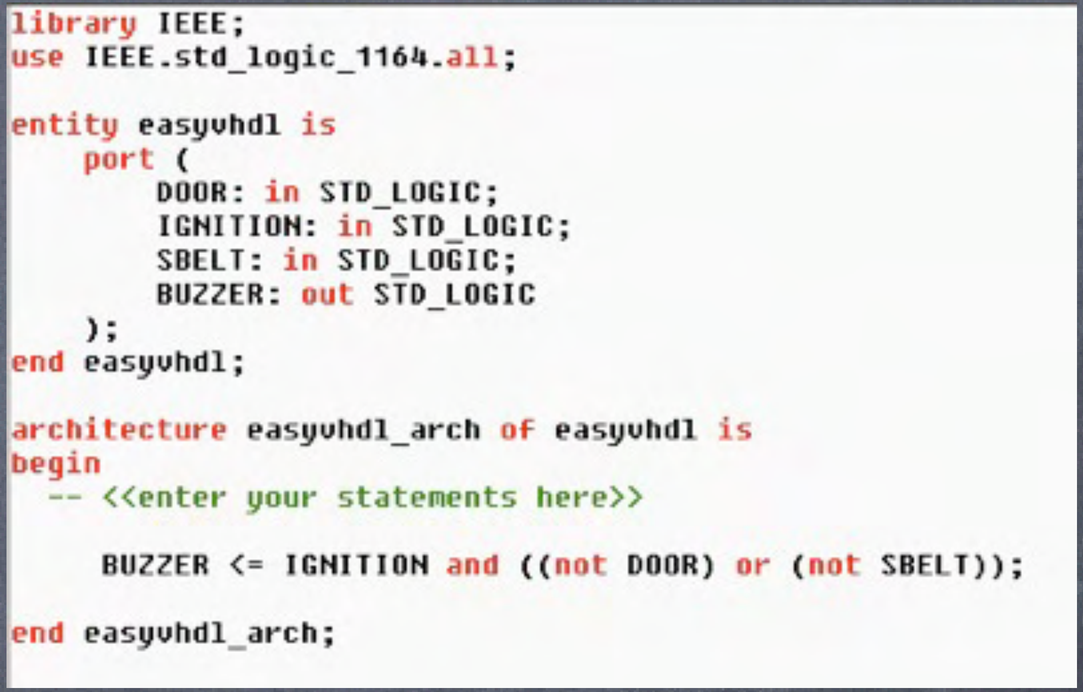
Data from Shmoocon 3 presentation: OpenCiphers by H1kari

Steps in FPGA design

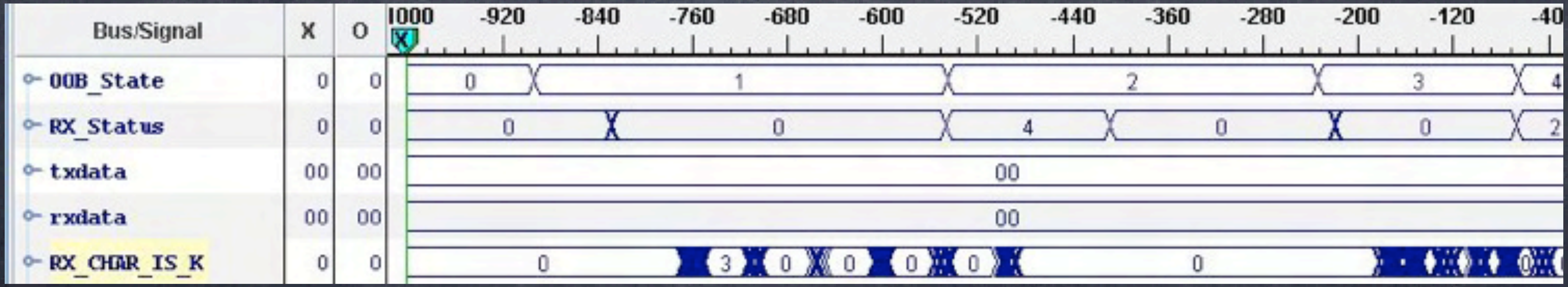
From idea to operation

Designing Logic

- Design Entry
  - Schematic or
  - HDL source code
- Design Entry Tools
  - Internal Logic Analyzer
  - State Diagram
  - Embedded Processor
- Simulation Test Bench
  - VHDL, Verilog and waveform



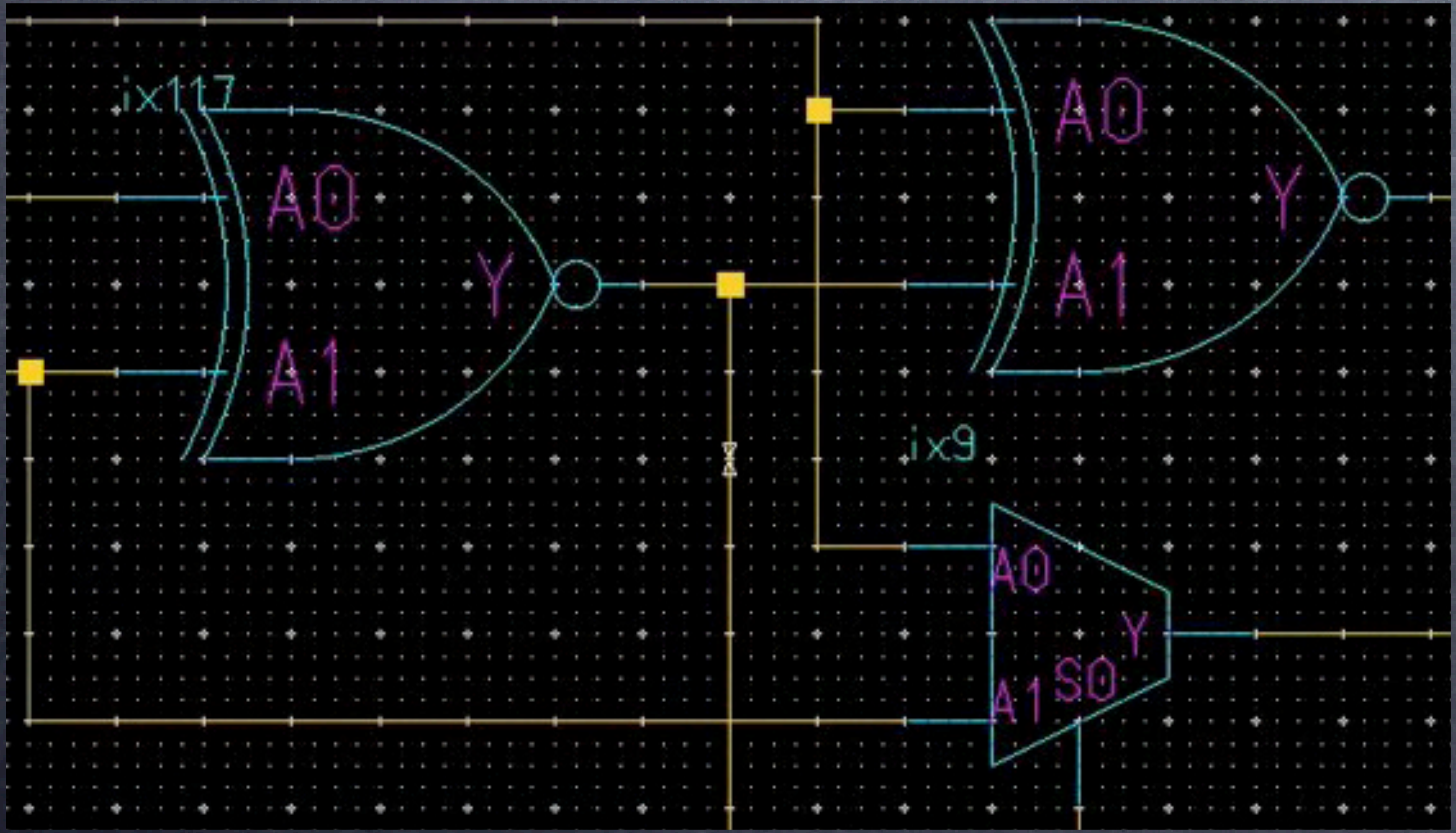
```
library IEEE;
use IEEE.std_logic_1164.all;

entity easyvhdl is
    port (
        DOOR: in STD_LOGIC;
        IGNITION: in STD_LOGIC;
        SBELT: in STD_LOGIC;
        BUZZER: out STD_LOGIC
    );
end easyvhdl;

architecture easyvhdl_arch of easyvhdl is
begin
  -- <<enter your statements here>>

     BUZZER <= IGNITION and ((not DOOR) or (not SBELT));

end easyvhdl_arch;
```

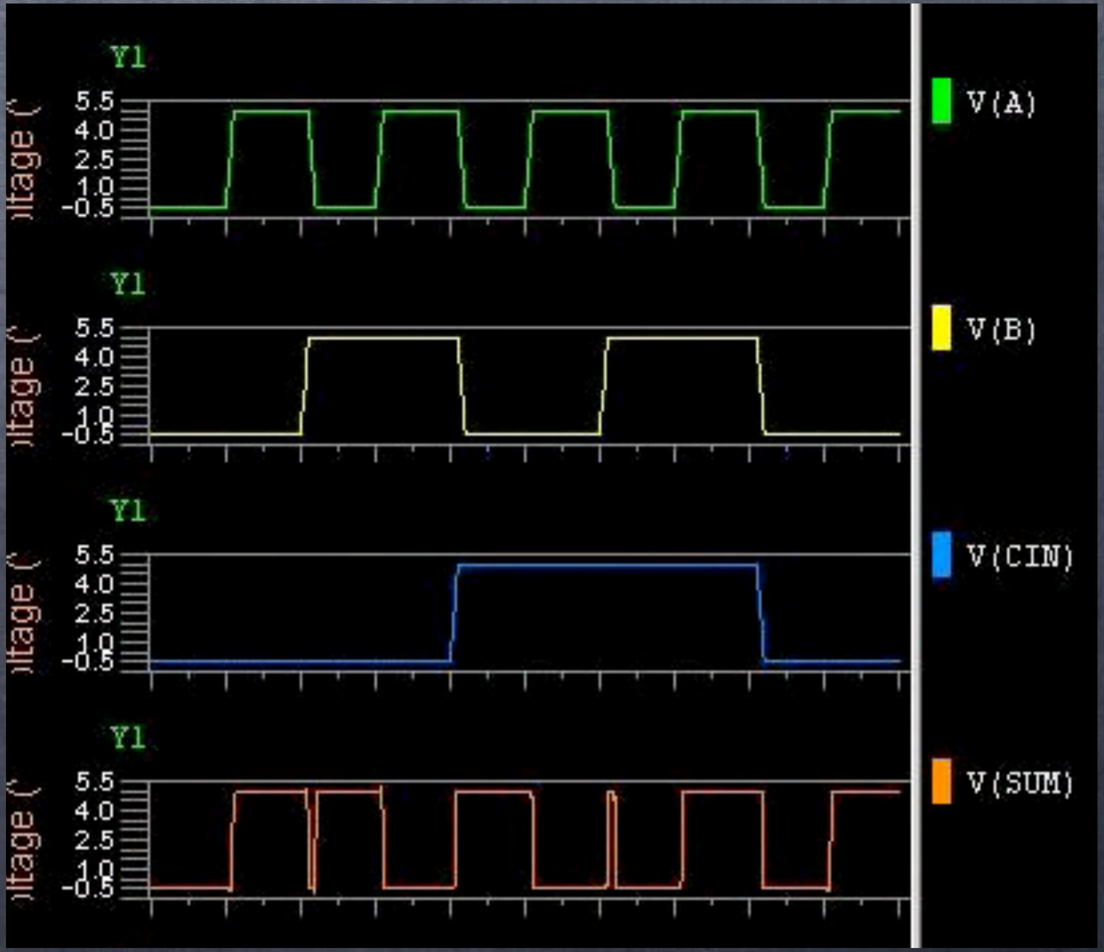


Synthesis
aka compiling your hardware

- Synthesis
  - Check syntax
  - View a schematics
  - Generate post-synthesis simulation model

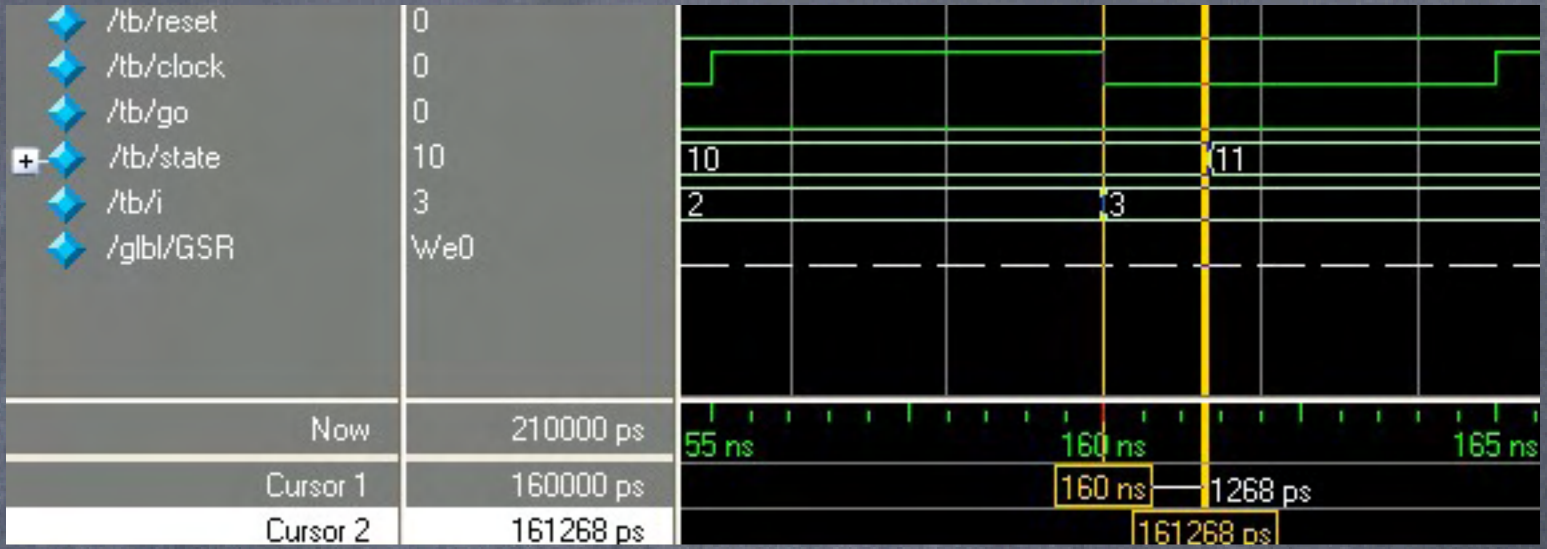
- Netlist
  - Define how your logic blocks connect
  - Internal signal vs external I/O



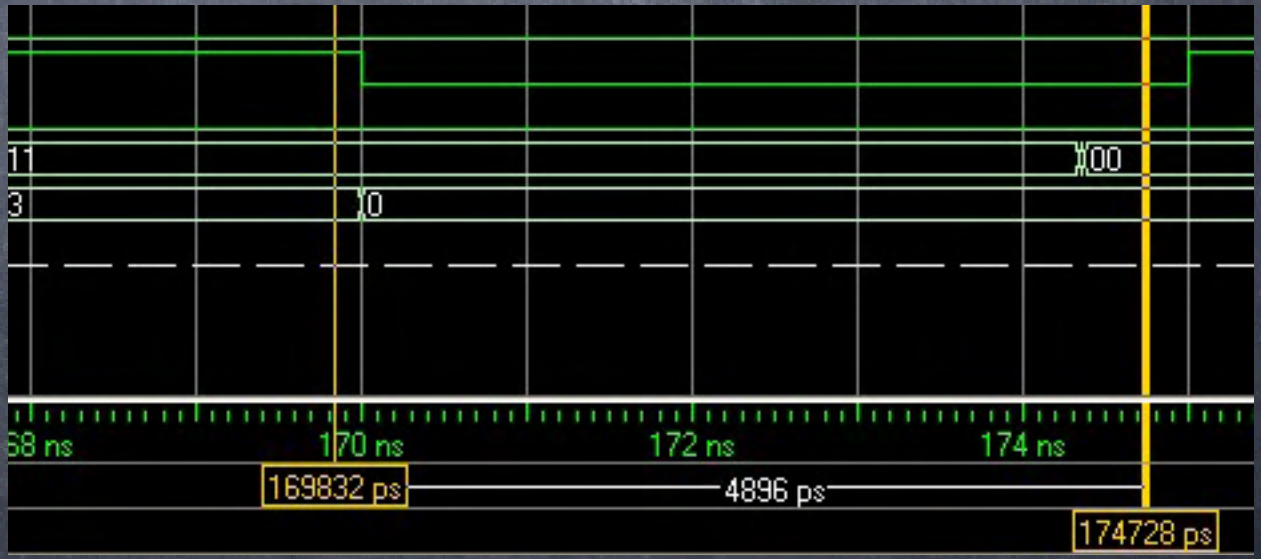


Implementing Designs

- Implement a design
  - Translate
  - Floorplan design
- Map
  - Access reports
  - Analyze timing
  - Manually place components
  - Generate simulation model
- Place & Route
  - Utilization reports
  - Analyze timing
  - Check I/O standards
  - Manually place & route components



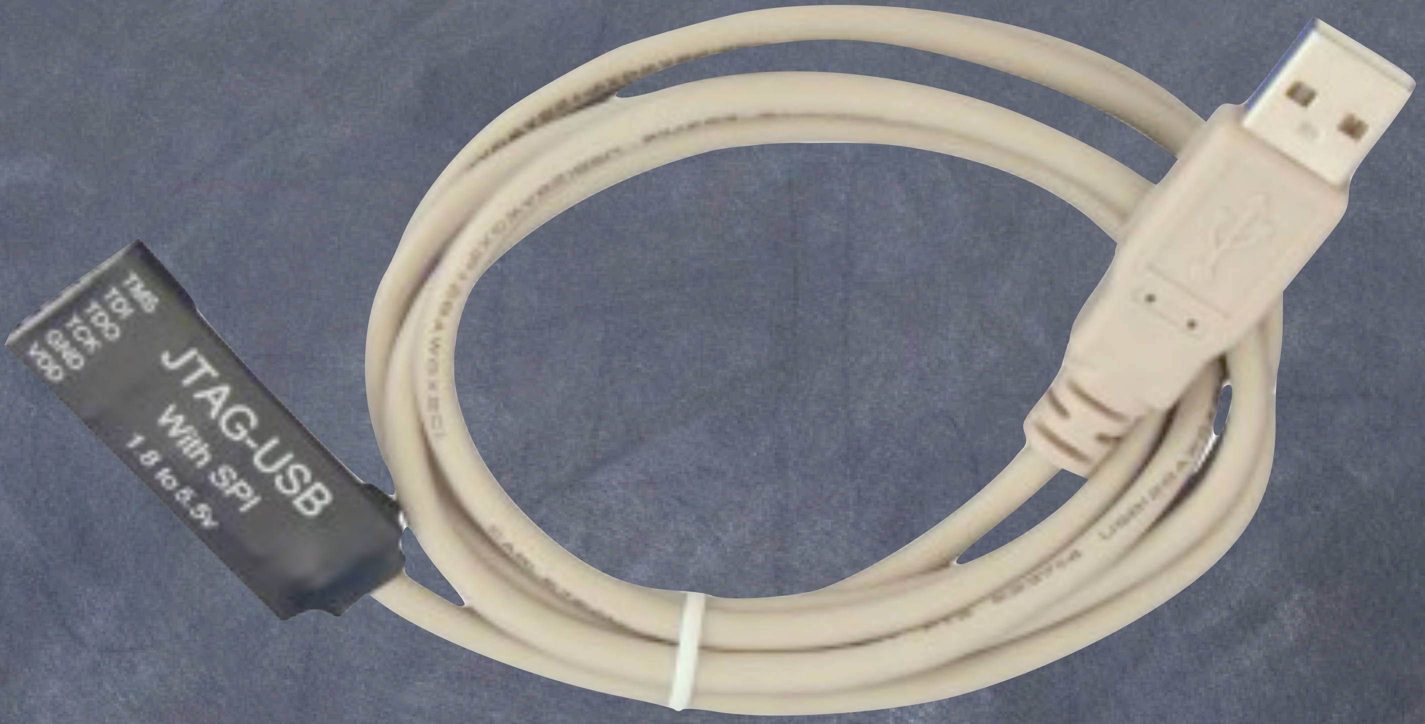
Post-Mapping simulation results.
Note the clock-to-state propagation delay of 1.2ns.



Post-Place and Route simulation results.
Note the clock-to-state propagation delay of 4ns.

Configuring your FPGA

- Ways to program an FPGA
  - JTAG
  - USB
  - SPI Flash
  - SPI PROM
- When is a FPGA programmed
  - On boot
  - On demand



Digilent JTAG programmer --
cheap programmer that works great

The Next ~2.5 Hours

- Explain Xilinx and Altera software
  - Lots of acronyms
- Show step-by-step demos
  - Writing simple VHDL
  - Writing C code for a processor written in HDL
  - Creating high speed interconnects between your functional units
- How far can the demo boards take you
  - Some are less then $100 dollars
  - Another has a touch screen LCD and 5 Megapixel camera
- Free stuff will be given away while we are compiling
  - FPGA Design Kits and other hardware
  - Lots corporate swag
  - A netbook

Thanks!

- Digilent
  Takes FPGAs and makes useful things from them. They make our favorite demo board called the Spartan-3E. Along with cool add-on modules.

- Altera and Xilinx
  The two major FPGA hardware/software manufacturers and other programable logic devices.

- Intel
  Provided lots of toys to give away! Uses FGPAs for design and testing of CPUs. How do you think they get it right one the "first" try!

- Dr. David Sincoskie, Professor, Director, Center on Information and Communications Sciences @ UD
  Donated funds to help make this trip and presentation possible!

If your in the education field, approach these companies to get support to teach FPGAs to your students