:)

Your PC ran into a problem and needs to restart. I've already captured your screen contents, so there's nothing to worry about. Trust me. I'm the BSODomizer HD, a mischievous FPGA and HDMI platform for the (m)asses!

For more information about this issue and possible fixes, visit http://bsodomizer.com/hd

If you call a support person, give them this info:
Stop code: IVE_BEEN_BSODOMIZED

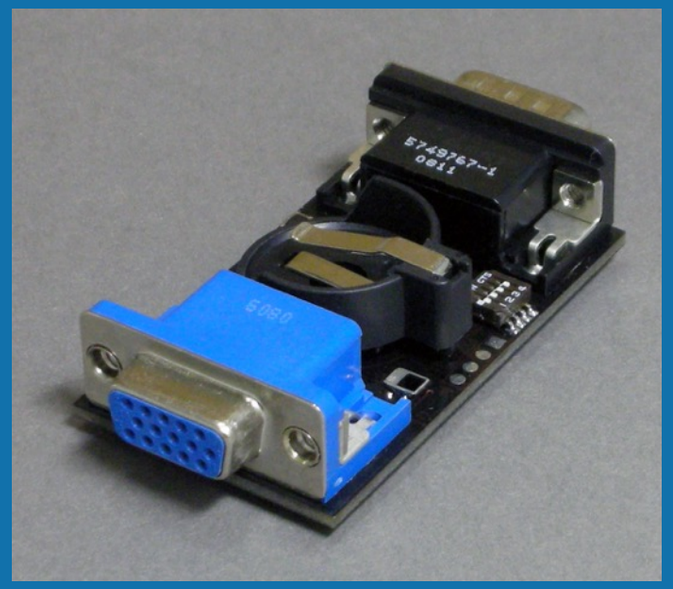
In Debt to Our Friends

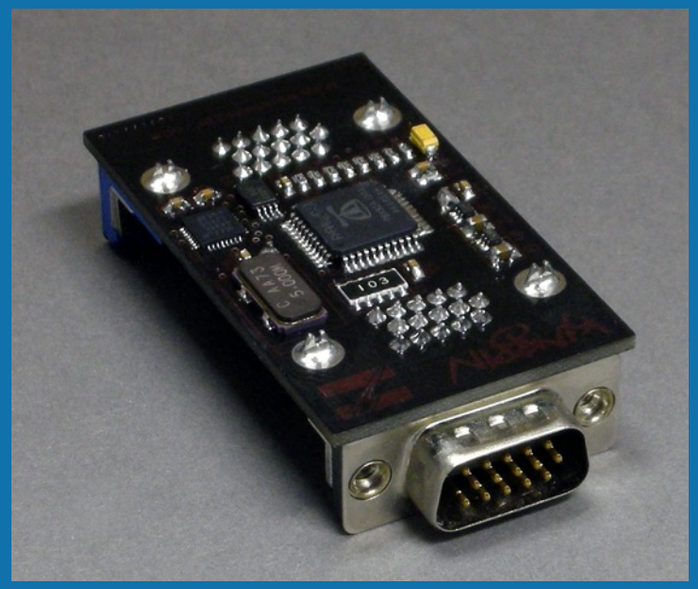
This project would not have happened without the help, support, and patience of...

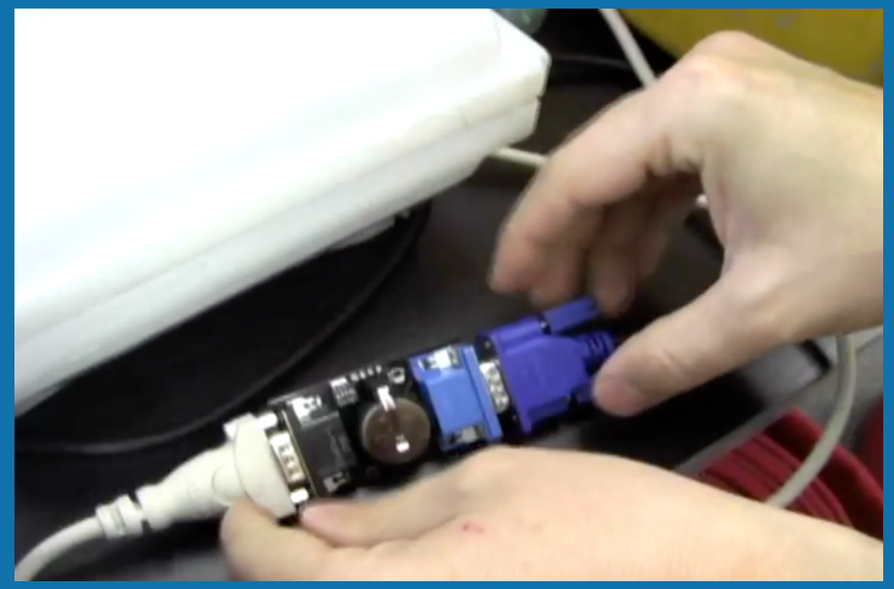
- Kris Bahnsen (l33tbunni)
- Raivis Rengelis (RaivisR)
- Parker Dillmann (LonghornEngineer)
- #tymkrs

The Original B50Domizer

- Released at DEFCON 16 (2008)
- XGA (1024 x 768) w/ text only
- Parallax Propeller, reprogrammable w/ PropClip
- 2x CR2032 Lithium coin cells
- Fully open source





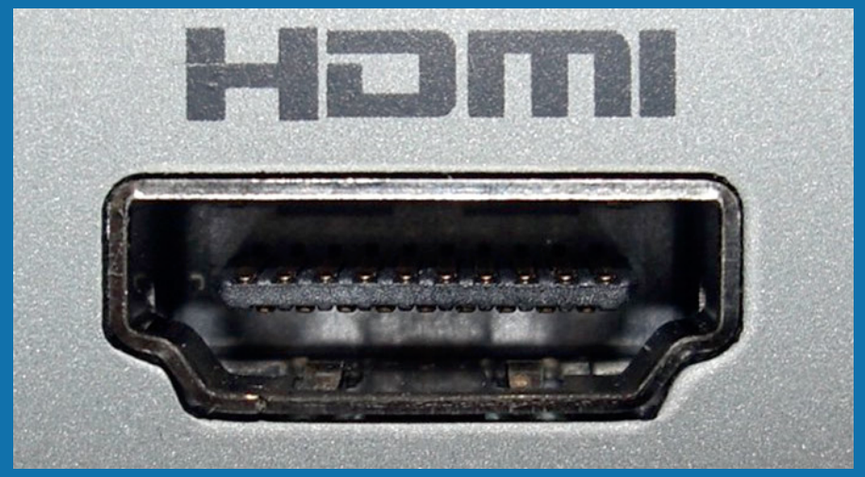


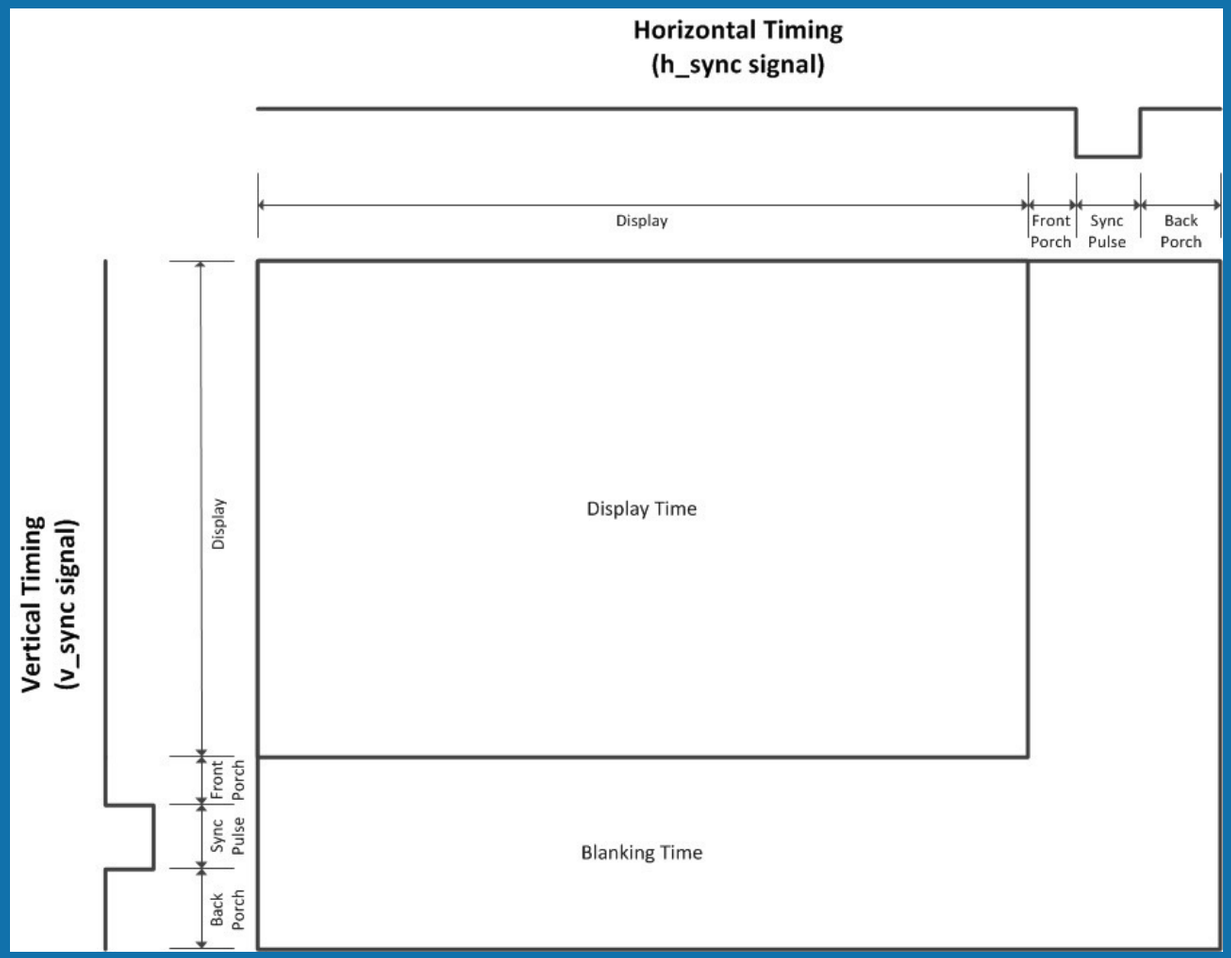
Desired Features

- Mischief
  - Full color, 1080p graphic capability
  - User-loadable images from SD card
  - Animated screens
- Legit
  - Screen capture (for pentesting)
  - Video display calibration
  - Open source FPGA tool/reference design

HDMI 101

- High speed, differential signalling
  - TMDS: 3 DATA + 1 CLK
- 1080p @ 60Hz is hard and fast
  - Bit rate: ~3.6GHz
  - Pixel clock: 148.5MHz
- Try doing that with a microcontroller!
- High speed processing more efficiently handled by FPGA

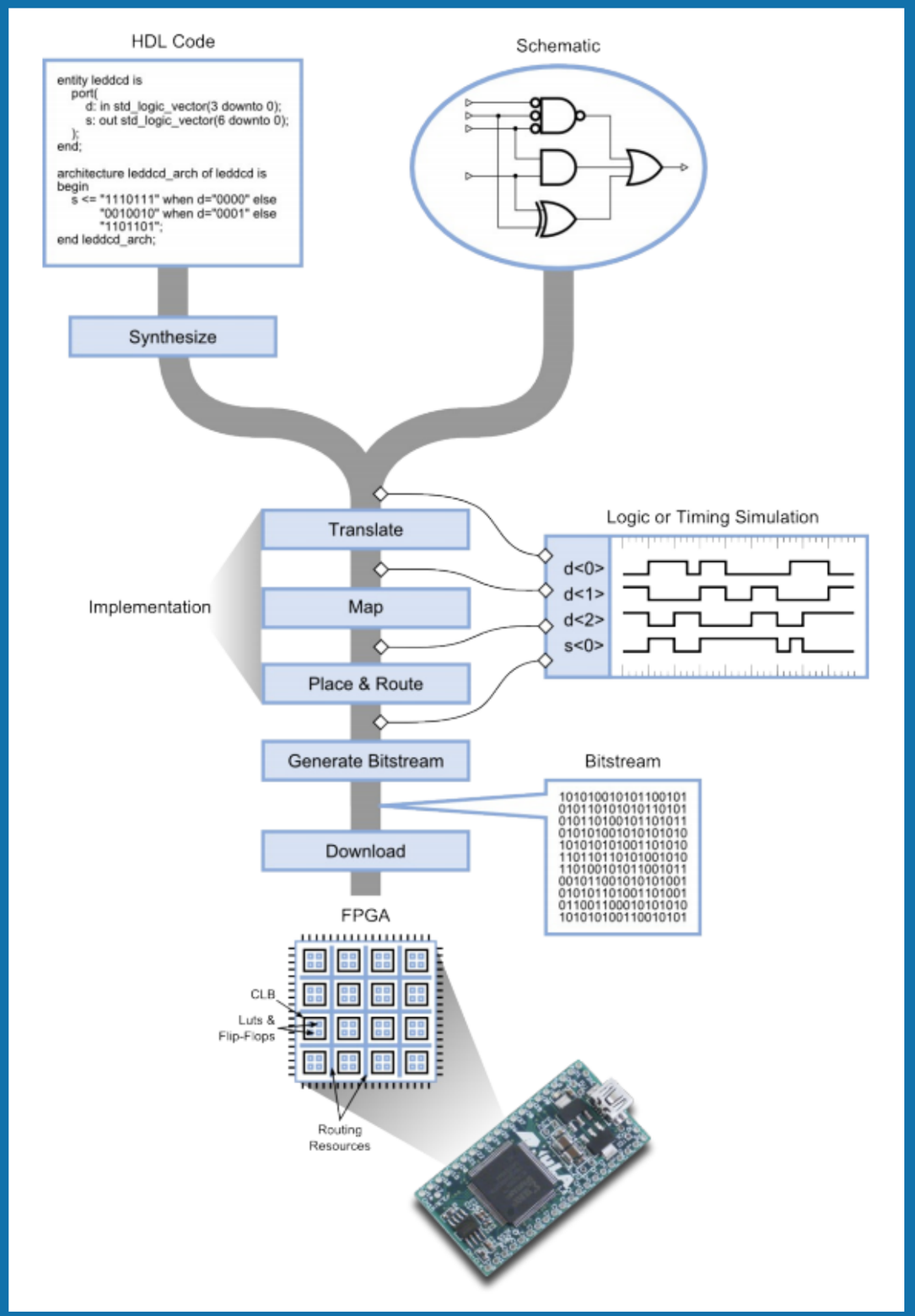




FPGA: WTF?!

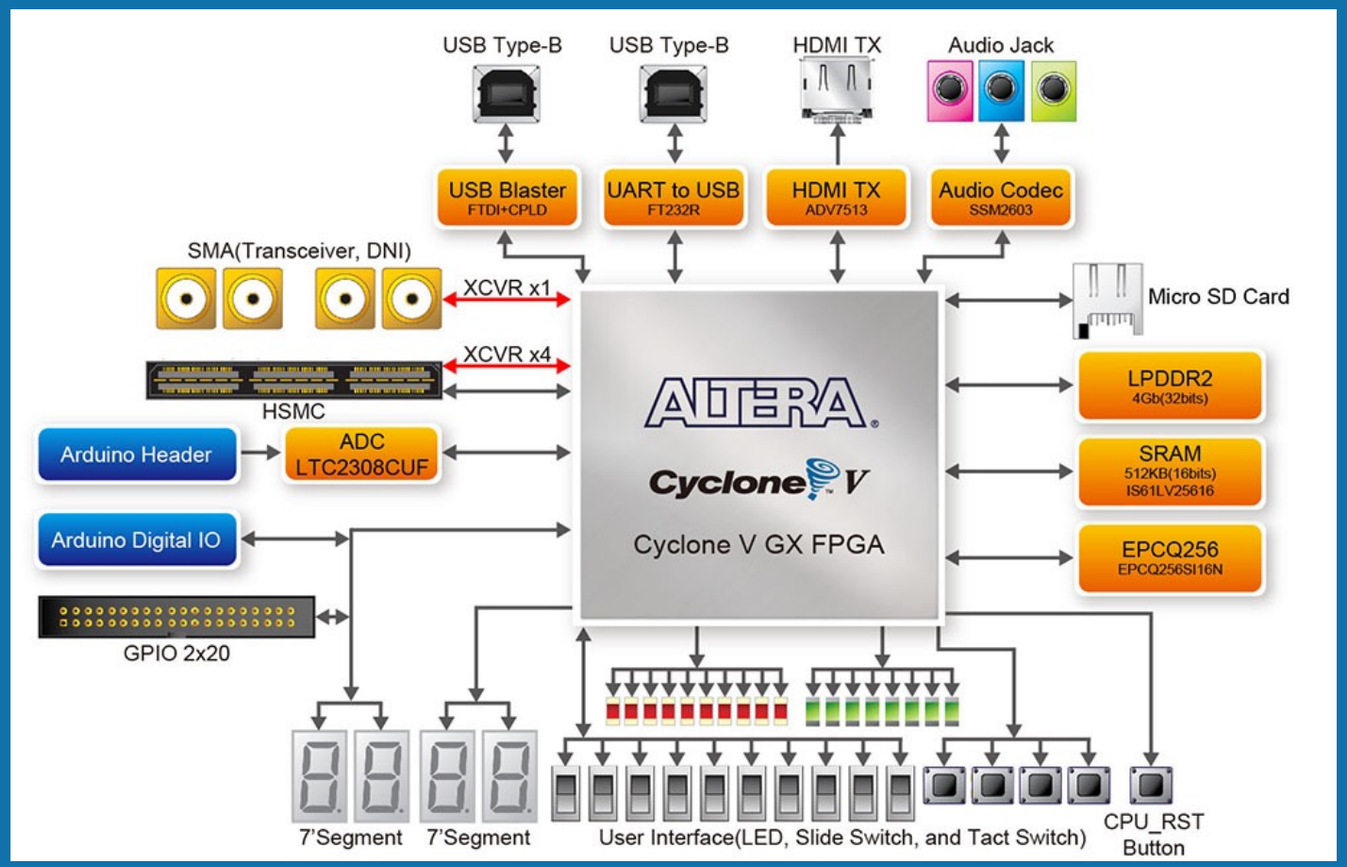
- Blank slate of digital logic
- Configurable blocks/ connections
- Behavior defined w/ schematic or HDL

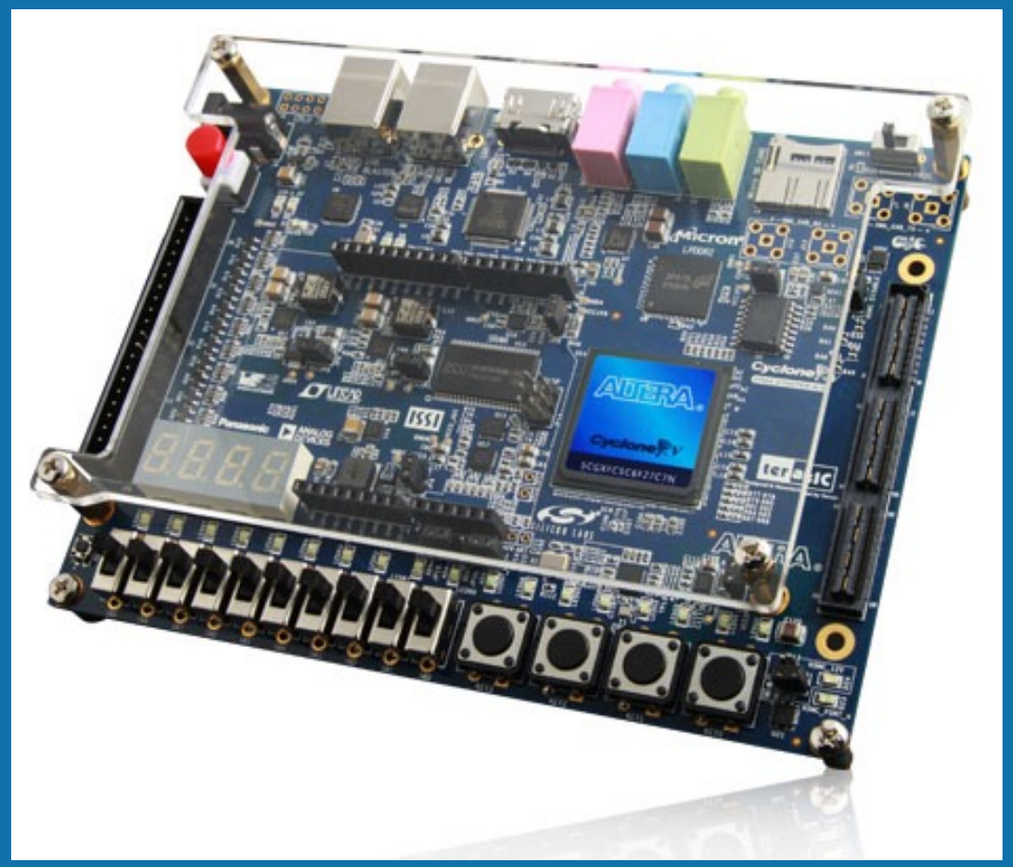
- Design/purchase IP modules to create hardware
- System operates in parallel, synchronized to clock(s)
- Danger and confusion abounds!



FPGA: Cyclone V GX Starter Kit

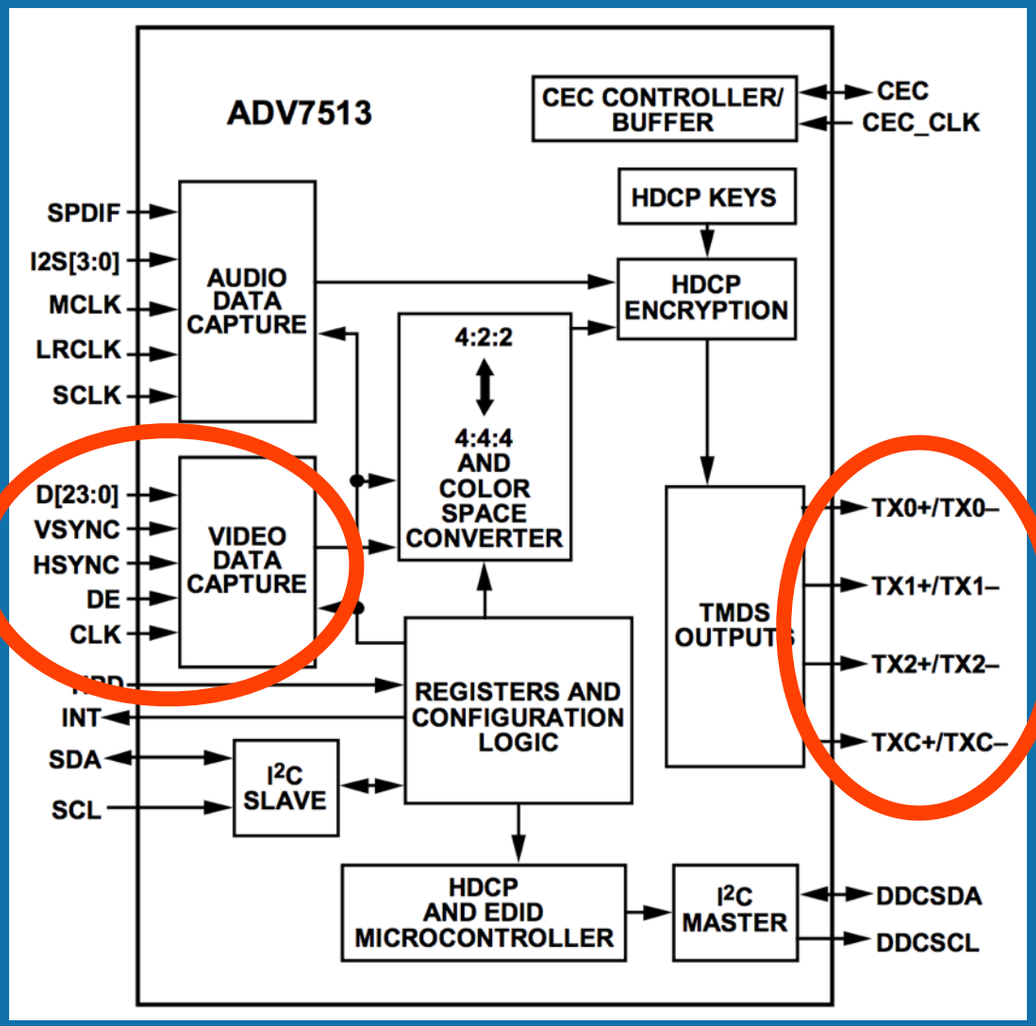
- Cyclone 5CGXFC5C6F27C7N, $179 USD
- Performance v. power v. cost
- Got up and running in minimal time (~2 days)
- Terasic does not provide schematics or PCB layout in native format :(



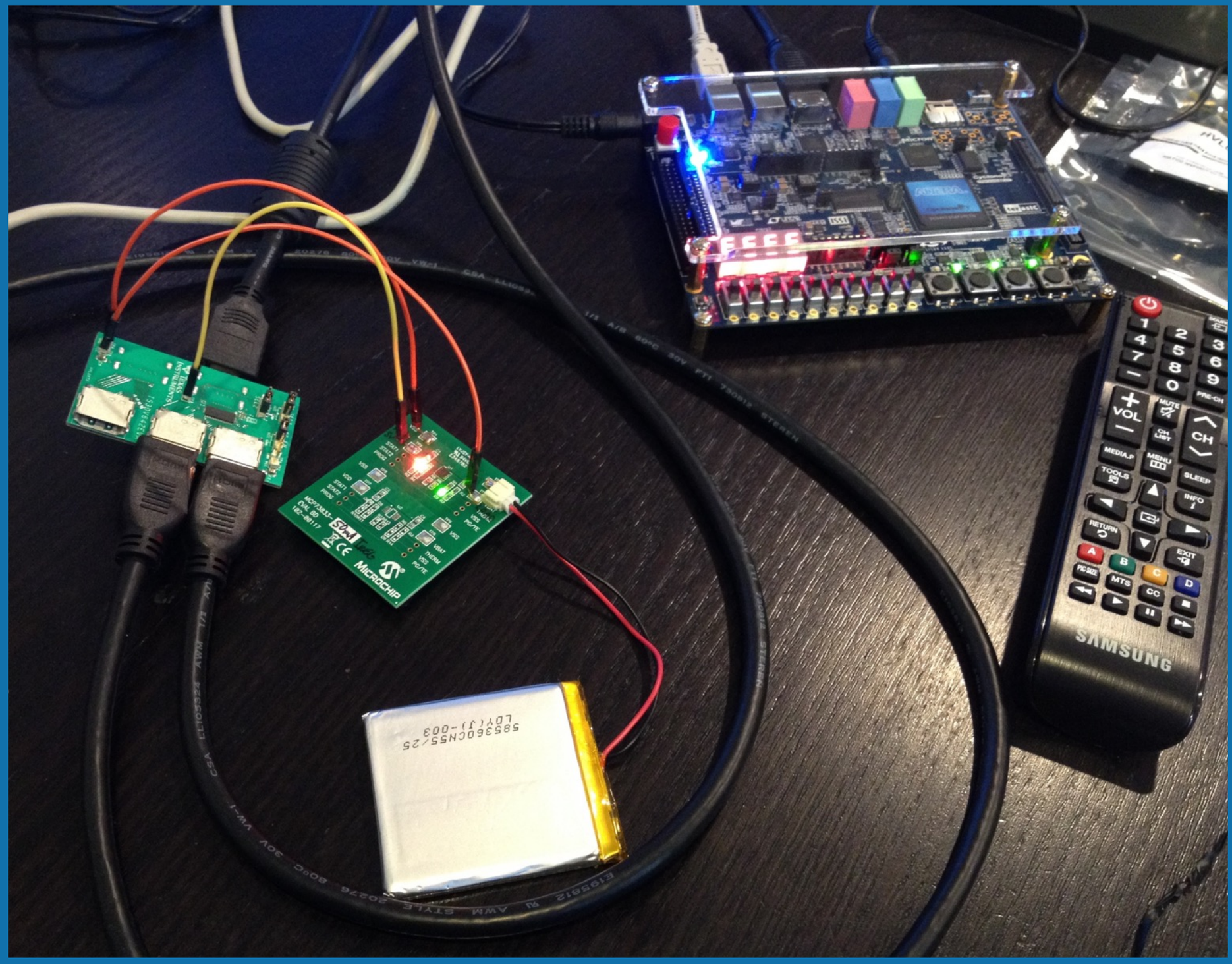


HDMI TX: ADV7513

- Serialization converter to reduce resources of FPGA
- Included on the C5G dev. kit
- We provide RGB + control signals, it magically provides HDMI-compliant TMDS outputs



Early Proof of Concept

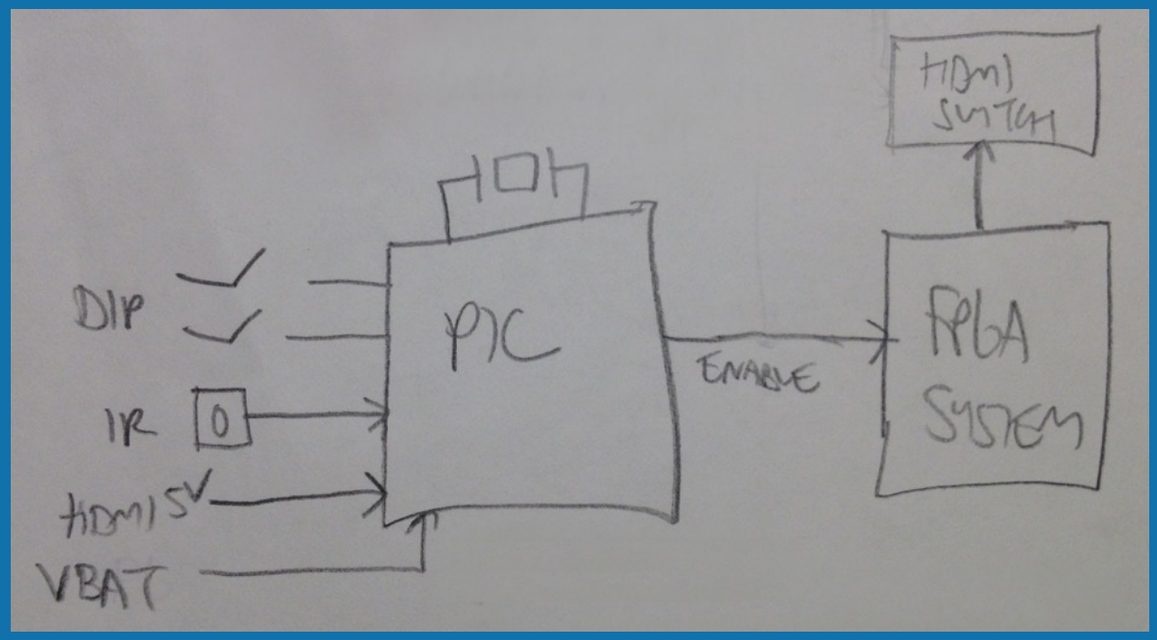


Refinements

- Block RAM too small for full 1080p color image
  - We need 1920 * 1080 * 24bpp = ~5.93MB
- External LPDDR2 SDRAM
  - Micron MT42L128M32D1: 512MB @ 400MHz
- MicroSD card interface
  - Want to store screen captures & user-defined images
- Need to implement the rest of the circuitry, too!
- Combine everything into a functional demo

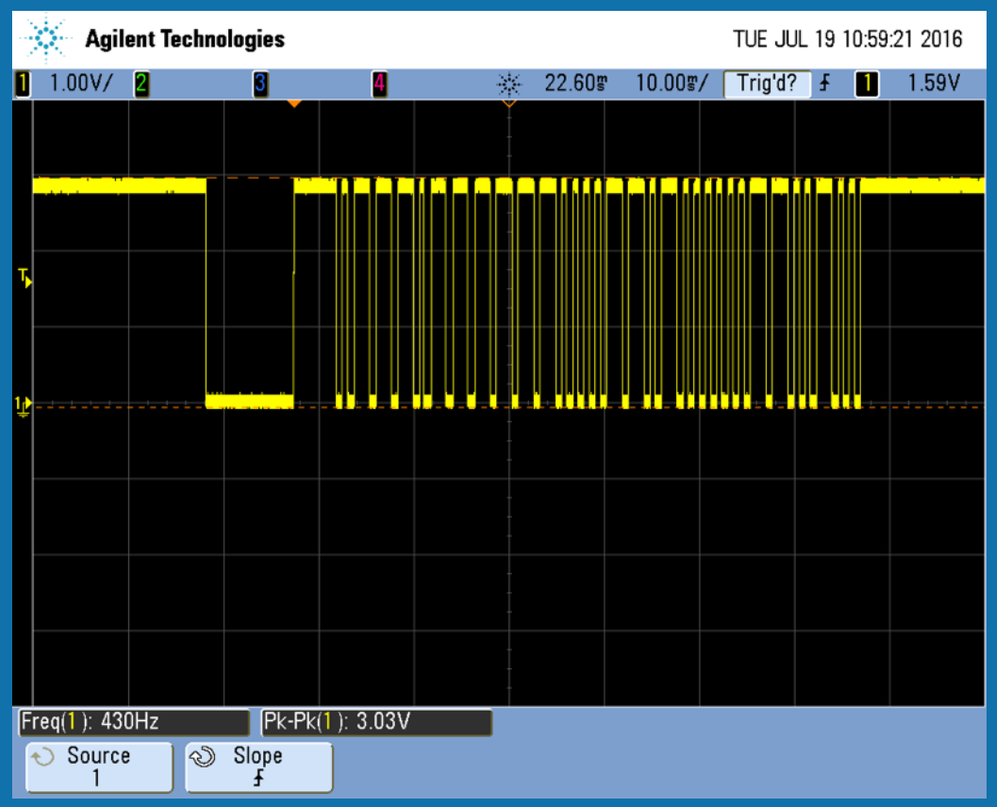
PIC Front End

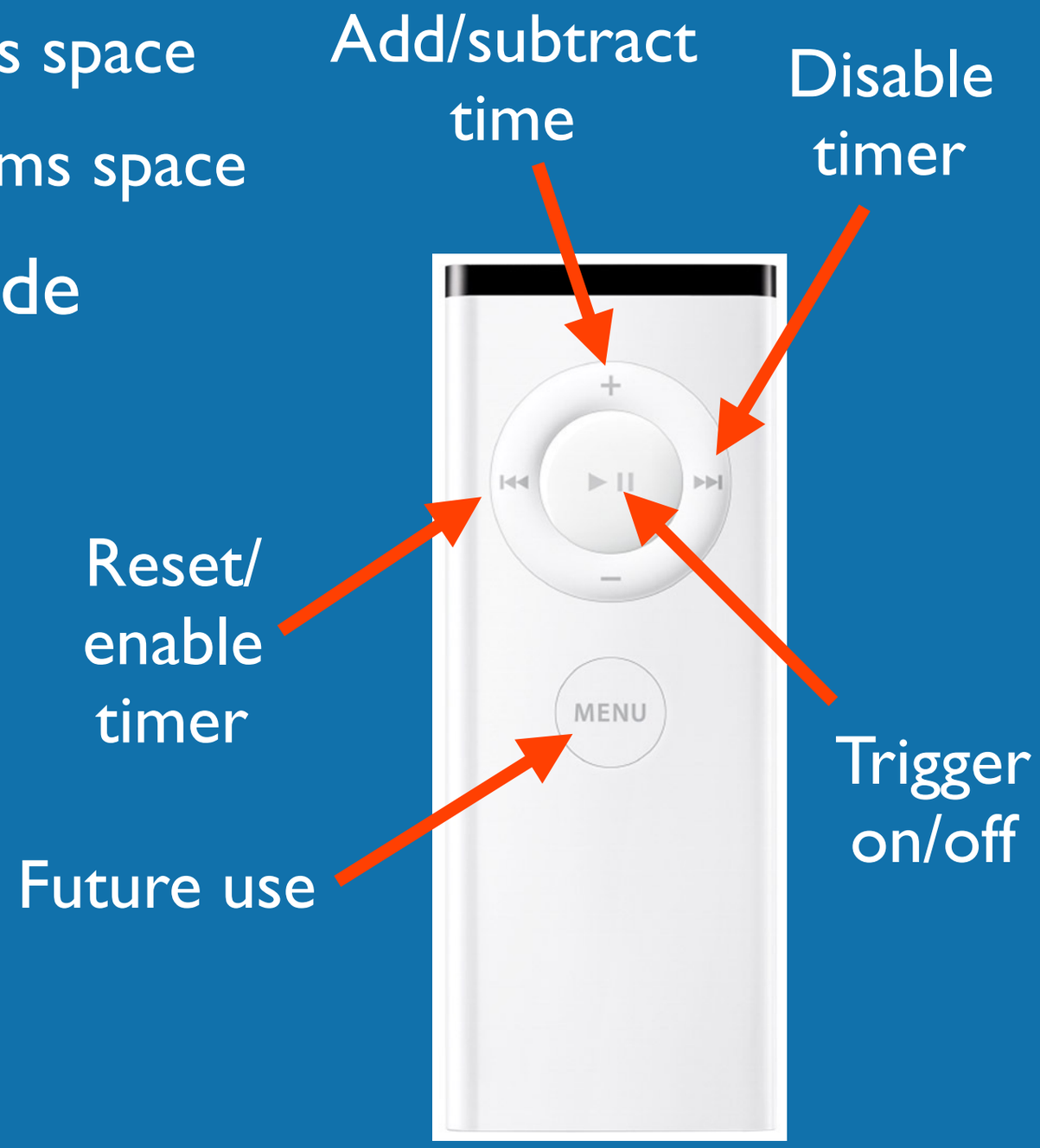
- Microchip PIC16LF1829
- Control power to FPGA subsystem
- External triggering via IR (Sharp GP1US301XP 38kHz)
- Timer to delay BSOD (user configurable)
- A/D to monitor battery level
- Can be replaced with whatever your heart desires



Apple IR Remote

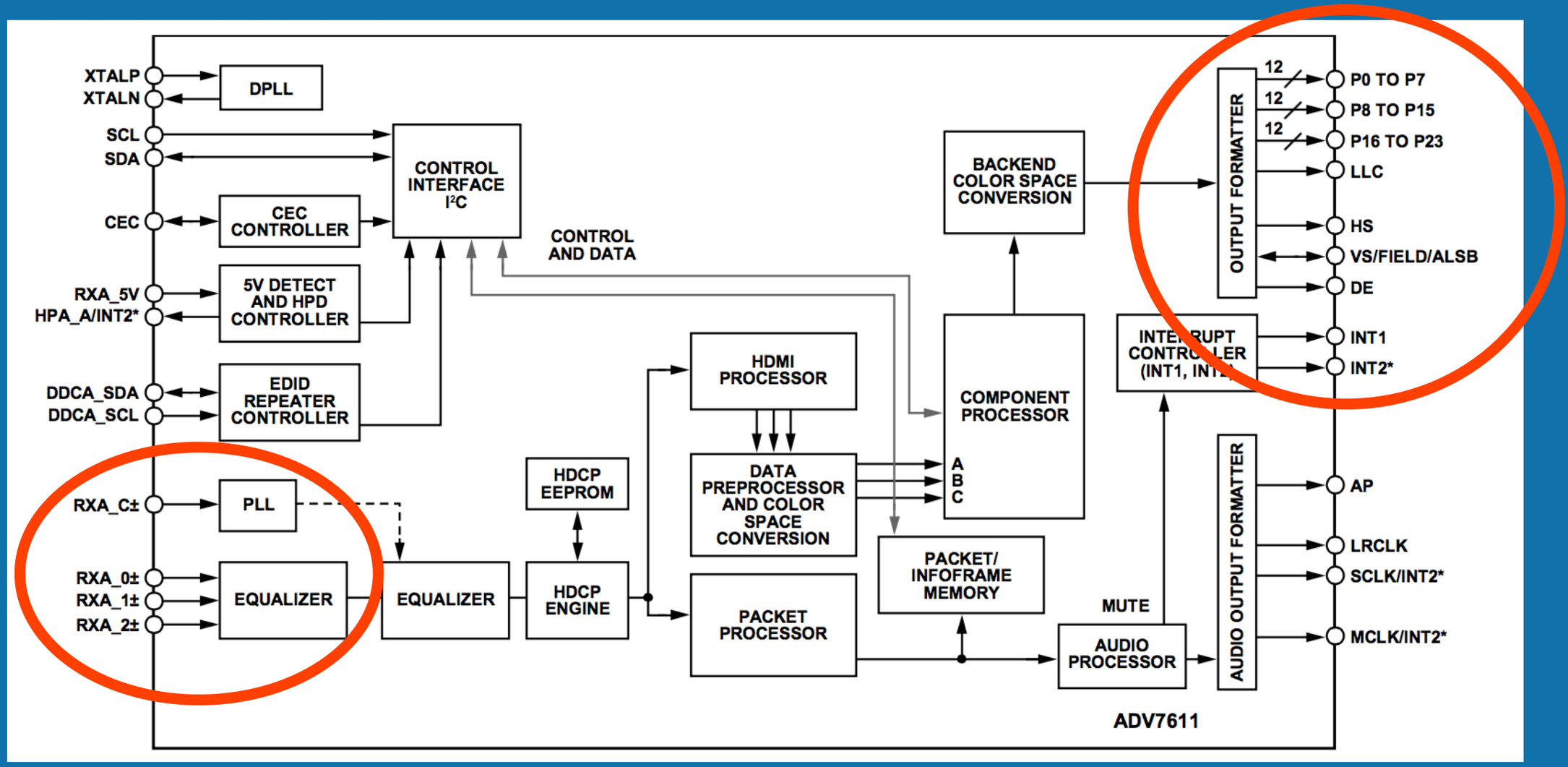
- NEC transmission protocol (same PHY, different data)
  - Start: 9ms pulse burst, 4.5ms space
  - Logic '1': 562.5µs pulse, 562.5µs space
  - Logic '0': 562.5µs pulse, 1.6875ms space
- Bare bones detection w/ wide timing margins





HDMI RX: ADV7611

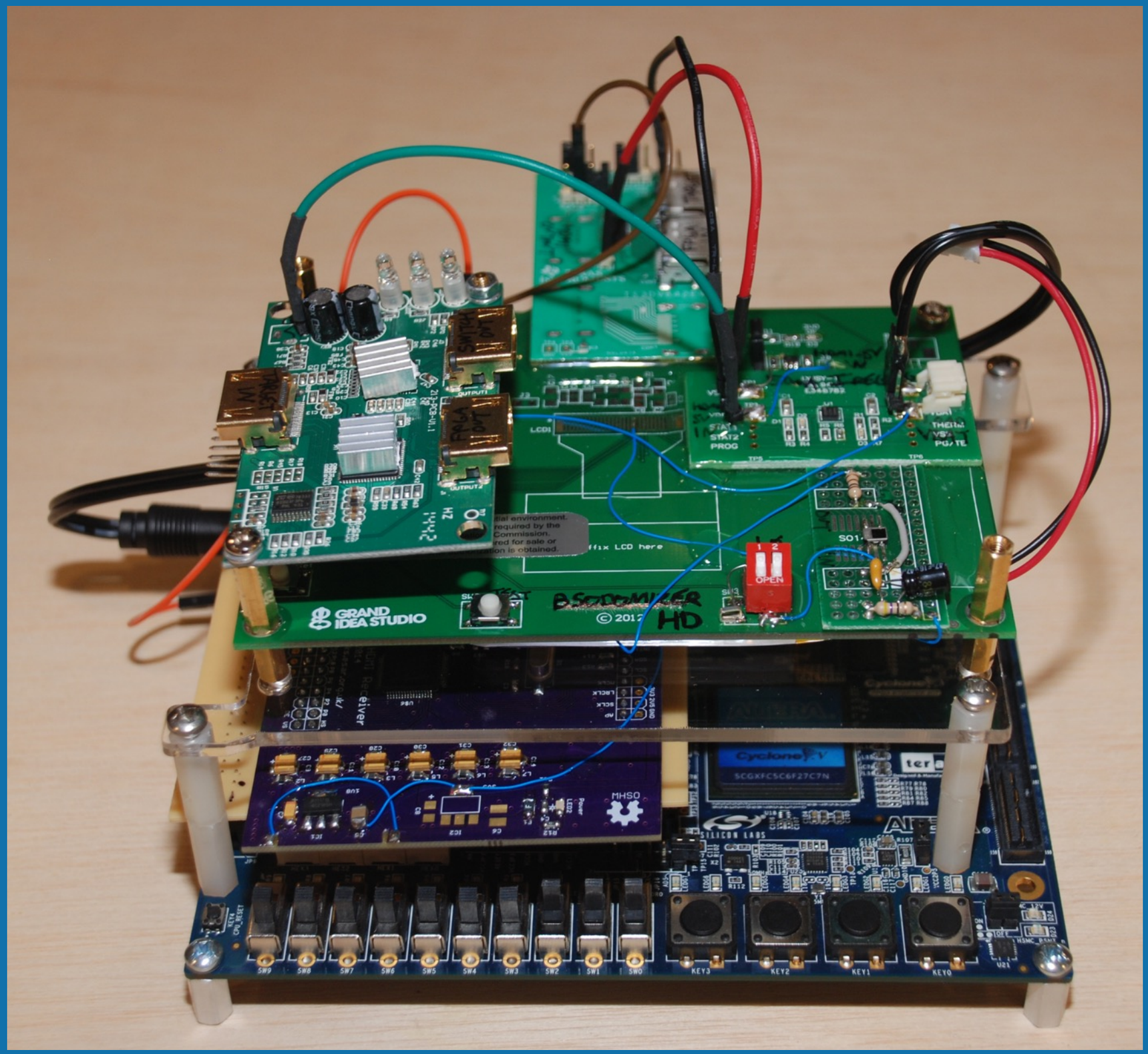
- Deserialization converter to reduce resources of FPGA
- Used HDMI Light V2 as a reference/breakout board, https://github.com/esar/hdmilight-v2



Other Subsystems

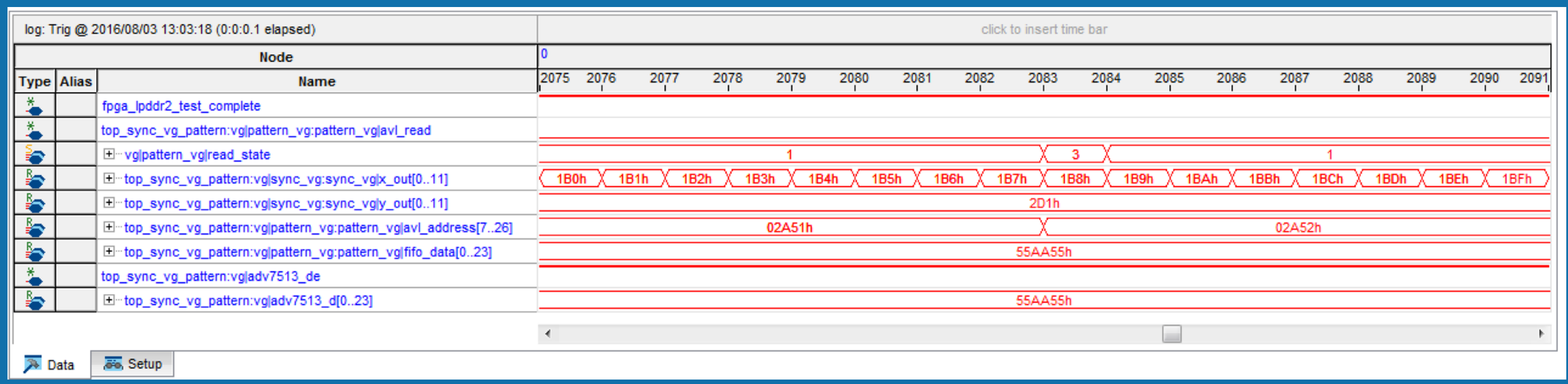
- Lithium Ion Battery Charging (Microchip MCP73833)
- HDMI Switch (Texas Instruments TS3DV642)
- HDMI Splitter (Hacked EnjoyGadgets unit)

Circuit Board Sandwich



LPDDR2 SDRAM (1080p, 24bpp)

- Read 32-bit word (8bpc RGB, MSB ignored) before it's needed on the screen
- Run memory access @ 2x PCLK (297 v. 148.5 MHz)
- Handle clock domain crossing with FIFO
- SignalTap II Logic Analyzer to peek inside the FPGA
- Trial and error, and error, and error, and error...



Real World Demonstration

Other Challenges

- Extremely aggressive timeline
- Fractional PLL conflict and physical placement
- Crossing clock domains requires finesse/ synchronization to ensure signal integrity
- HDMI RX implementation started, but device not responding
- SD card/FAT32 implementation not done
- Typos or misdefined signals/connections will not necessarily be detected by compiler!
- Debugging HDL is horrendous

Get BSODomized

- www.grandideastudio.com/portfolio/bsodomizer

  *** Development notes, schematic

  *** Original design (schematic, source code, BOM, block diagram, Gerber plots, assembly drawing)

- https://github.com/joegrand/bsodomizer-hd-pic

  *** Front End Subsystem (PIC16LF1829)

- https://github.com/joegrand/bsodomizer-hd-c5g

  *** HDL for Cyclone V GX Starter Kit

In Closing

- Committed to a project way beyond our comfort zone
- Painful & practical lessons
- Easy access to FPGA development tools & resources, but still extremely complex
- FPGAs fill a gap in the engineering world, worth giving them a try
- Sandwich to product?
  - Significant engineering remains
  - Demand may influence decision to bring to market
  - Send desires to root@bsodomizer.com

The End