:)

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

BSODomizer HD

- History
- HDMI 101
- FPGA: WTF?!
- Design
- Challenges

32"
LCD HDTV
FREE HDMI CABLE INSIDE!
HDMI
HDMI CABLE (version 1.3) INCLUDED +
PREMIUM SIZE HDTV CLEANING CLOTH
32" LIQUID CRYSTAL (LCD) HDTV / 16 X 9 WIDESCREEN ASPECT RATIO
HIGH DEFINITION 1366 X 768 NATIVE RESOLUTION
PREMIUM QUALITY GUARANTEE – ZERO DEFECTIVE BRIGHT PIXELS ALLOWED
3X HDMI (v1.3) PORTS FOR SUPERIOR ALL DIGITAL CONNECTIVITY
SIDE ACCESS HIGH DEFINITION GAME PORT
BUILT-IN DIGITAL HDTV & STANDARD TV COMBINED TUNER
PC INPUT (RGB): USE YOUR TV AS A COMPUTER MONITOR
VIZIO
HD TV

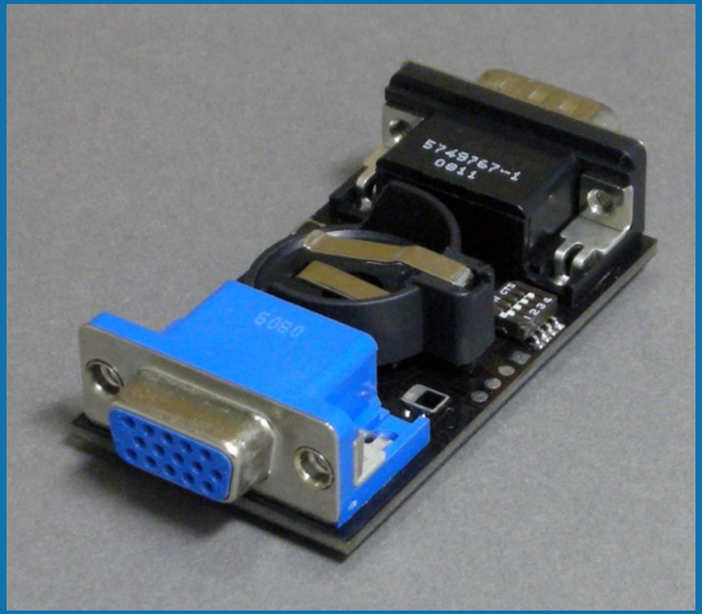
In Debt to Our Friends

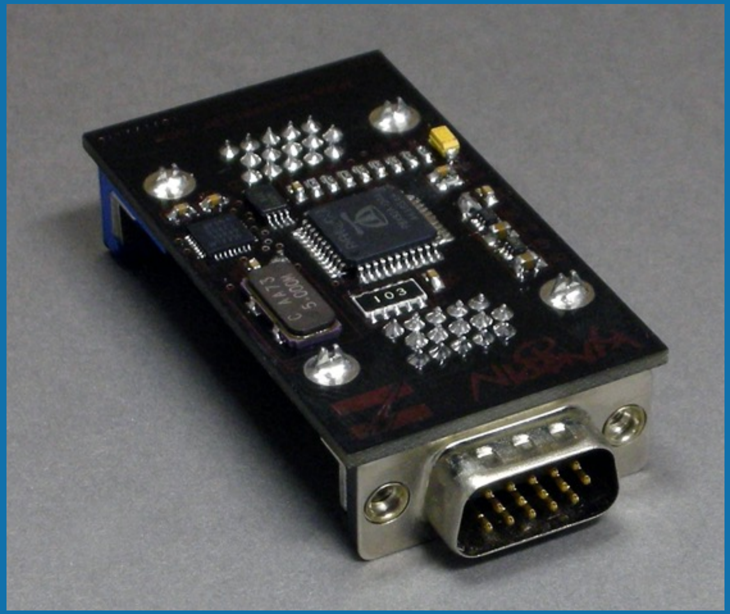
This project would not have happened without the help, support, and patience of...

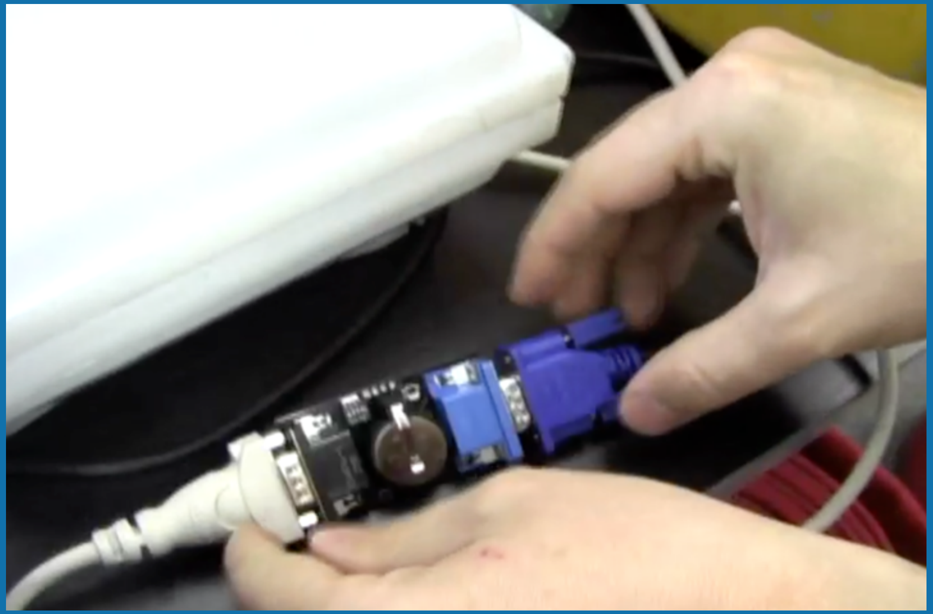
- Kris Bahnsen (l33tbunni)
- Raivis Rengelis (RaivisR)
- Parker Dillmann (LonghornEngineer)
- #tymkrs

The Original BSODomizer

- 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







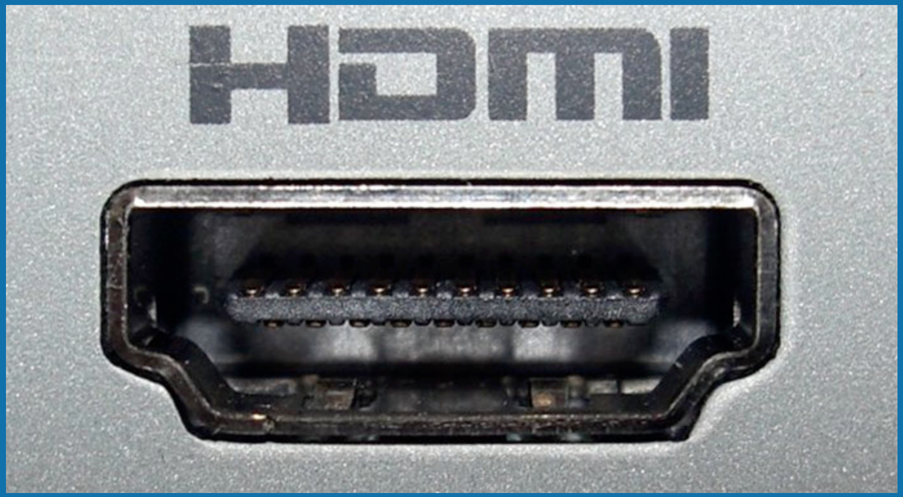
- Wanted to learn about FPGAs
- Share our work with the hacker community
- Create another ridiculous (and possibly useful) project

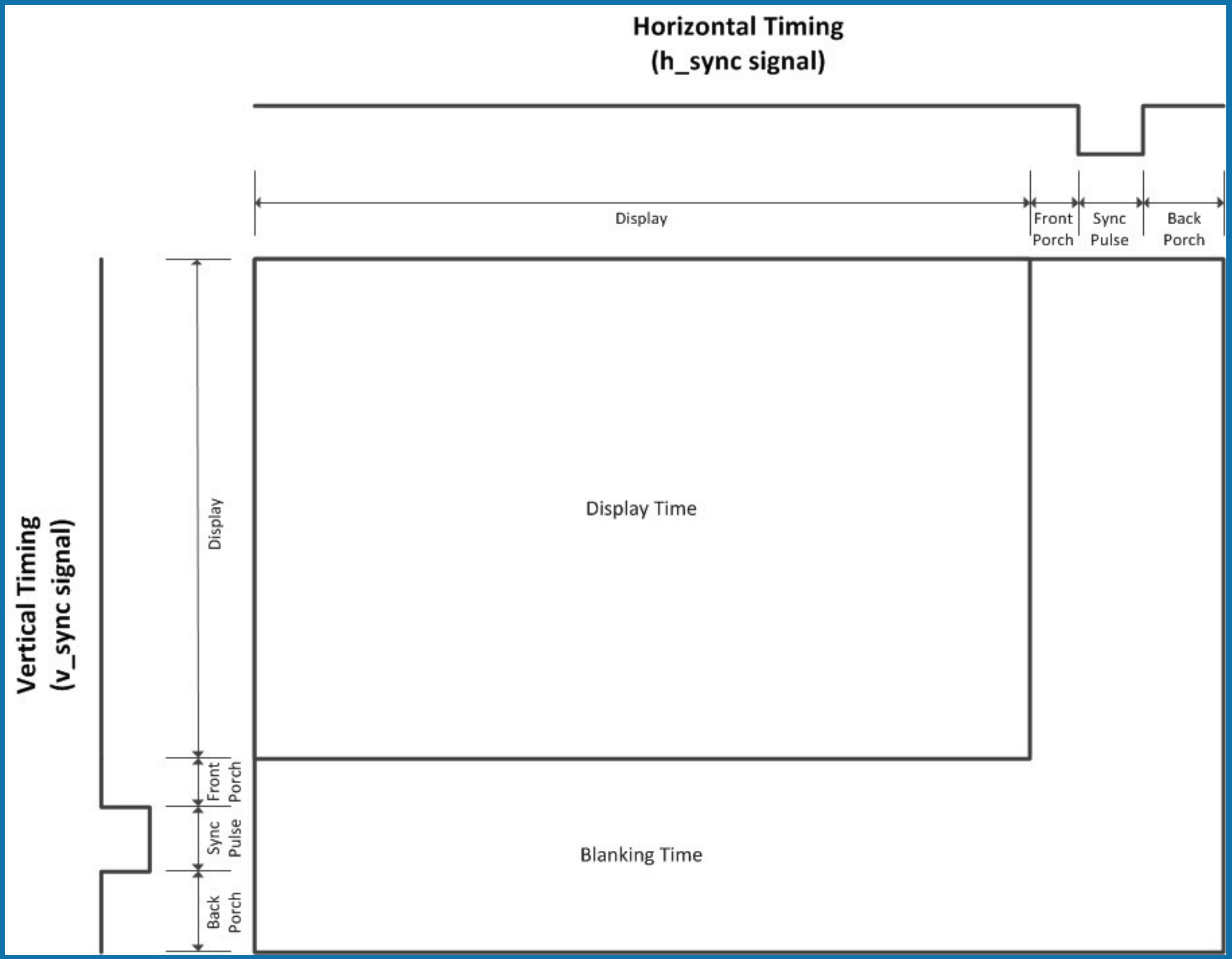
Desired Features

- 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

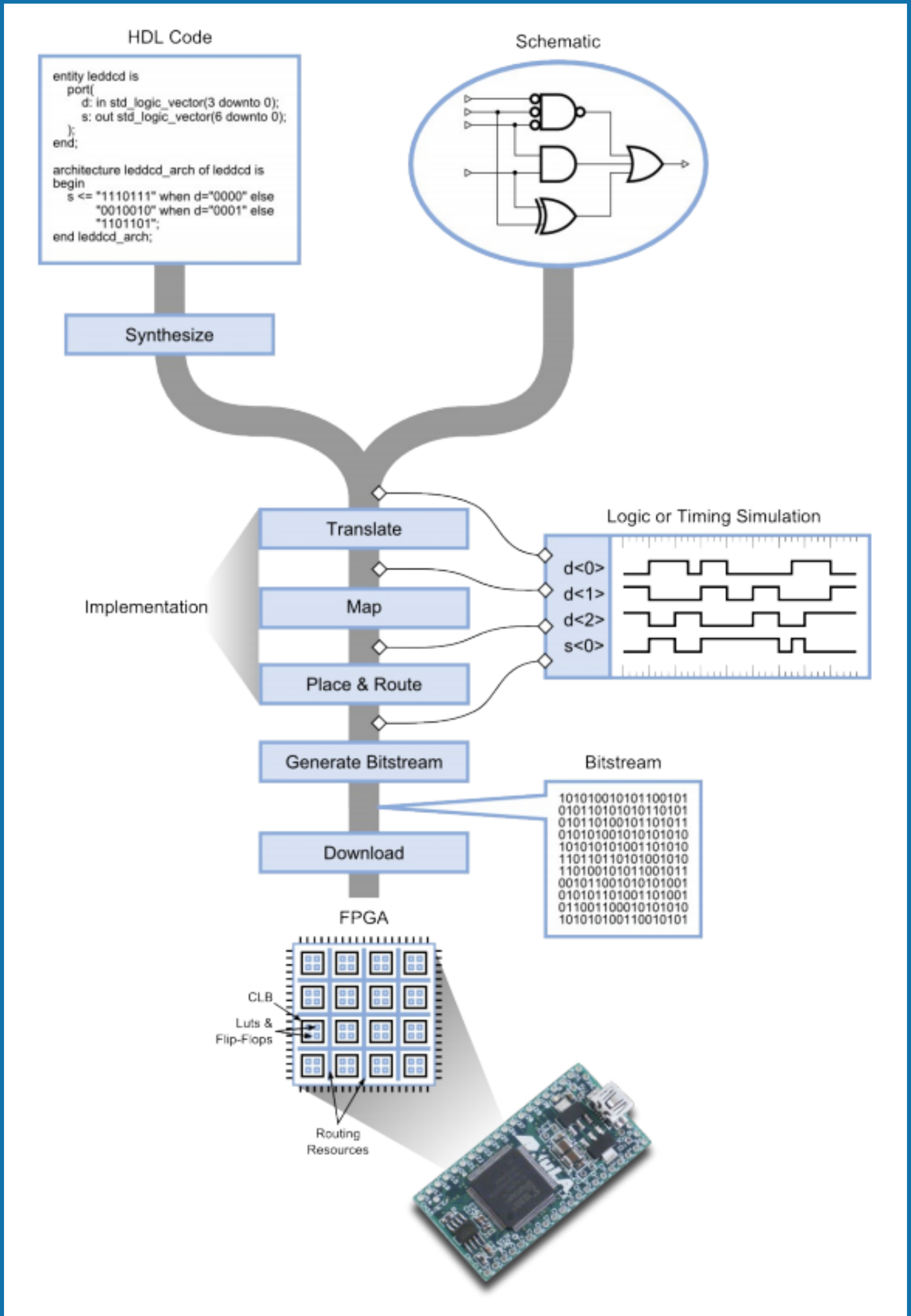
- High speed, differential signalling
  - TMDS: 3 DATA + 1 CLK
- 1080p @ 60Hz is hard and fast
  - Bit rate: ~3.6GHz
  - Pixel clock: 148.5MHz
- Try doing that with a microcontroller!
- High speed processing more efficiently handled by FPGA





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!

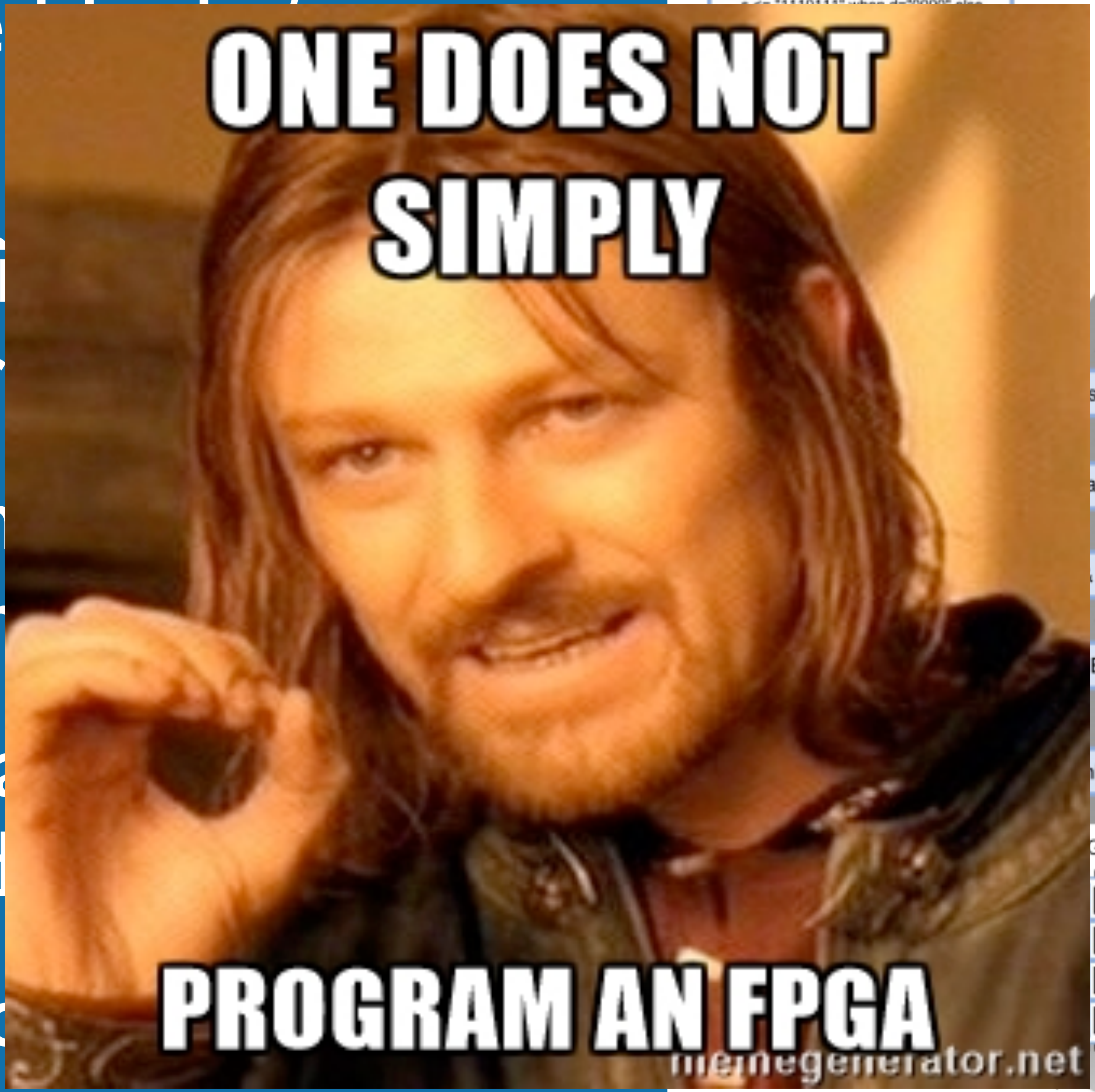


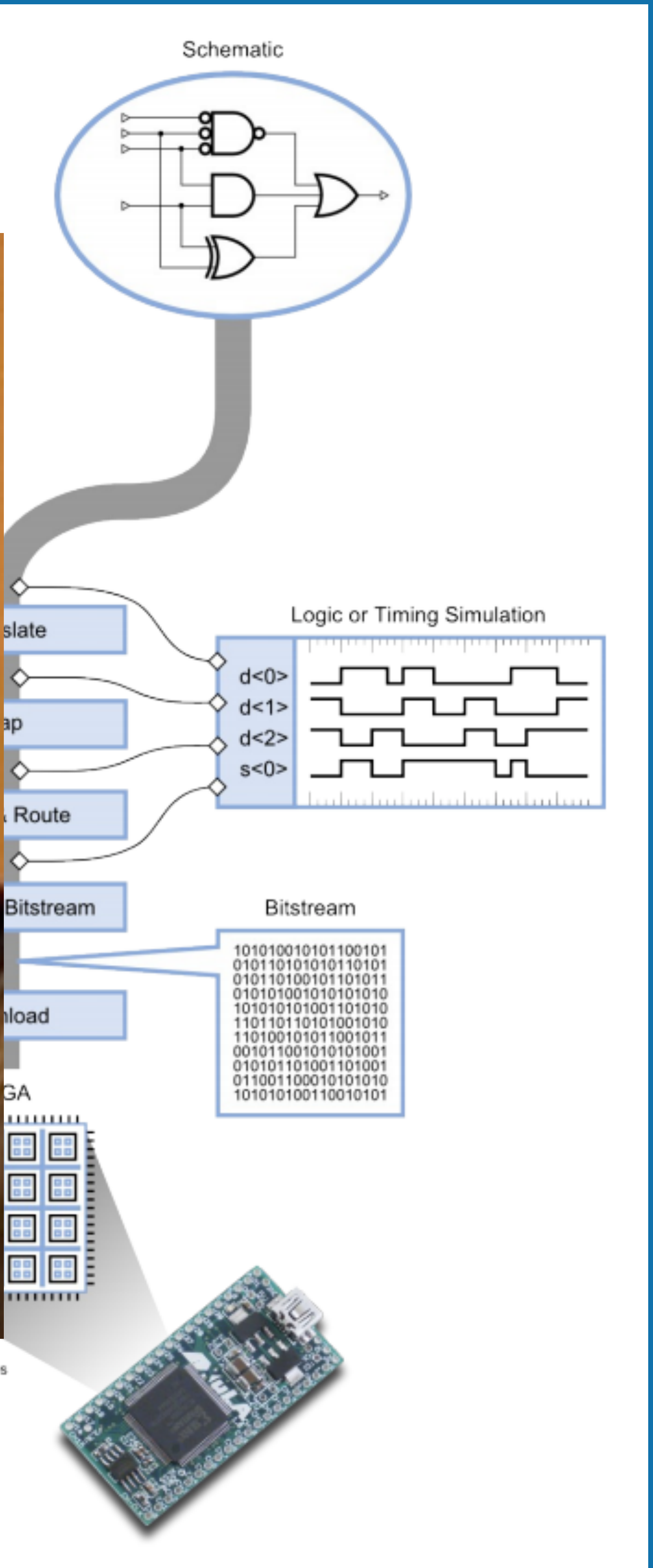
```
entity leddcd is
    port(
        d: in std_logic_vector(3 downto 0);
        s: out std_logic_vector(6 downto 0);
    );
end;

architecture leddcd_arch of leddcd is
begin
    s <= "1110111" when d="0000" else
            "0010010" when d="0001" else
            "1101101";
end leddcd_arch;
```

```
101010010101011100101
010110101010101110101
010110100101101101011
010101001010101101010
101010101010011101010
110110110101010010100
110100101010110010110
001011001010101010100
010101101001101010010
011001100010101010100
101010100110010101010
```

FPGA: WTF?!

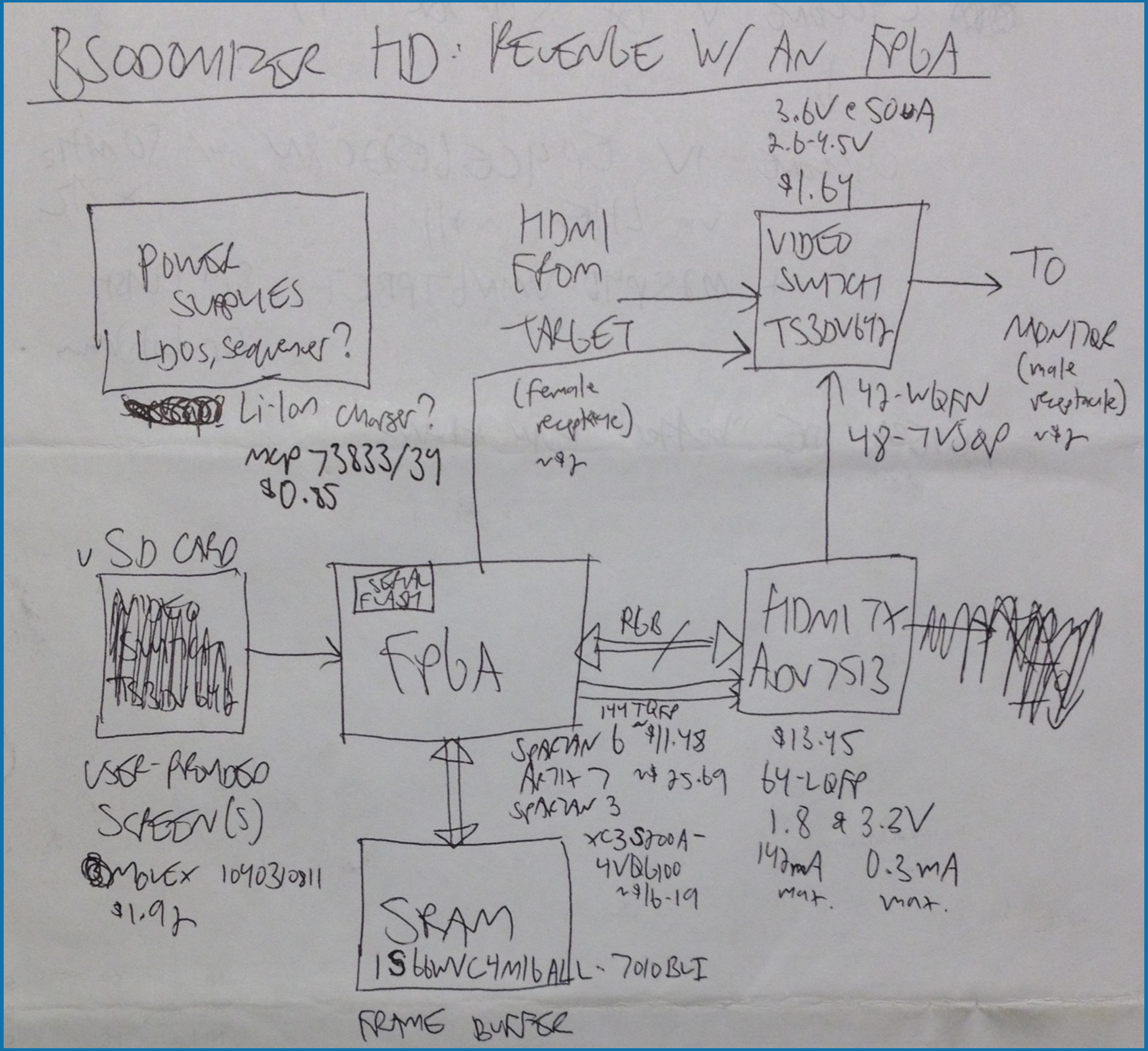
- Blank slate of digital logic
- Configurable blocks/ connections
- Behavior defi schematic or
- Design/purch to create har
- System opera synchronized
- Danger and c abounds!





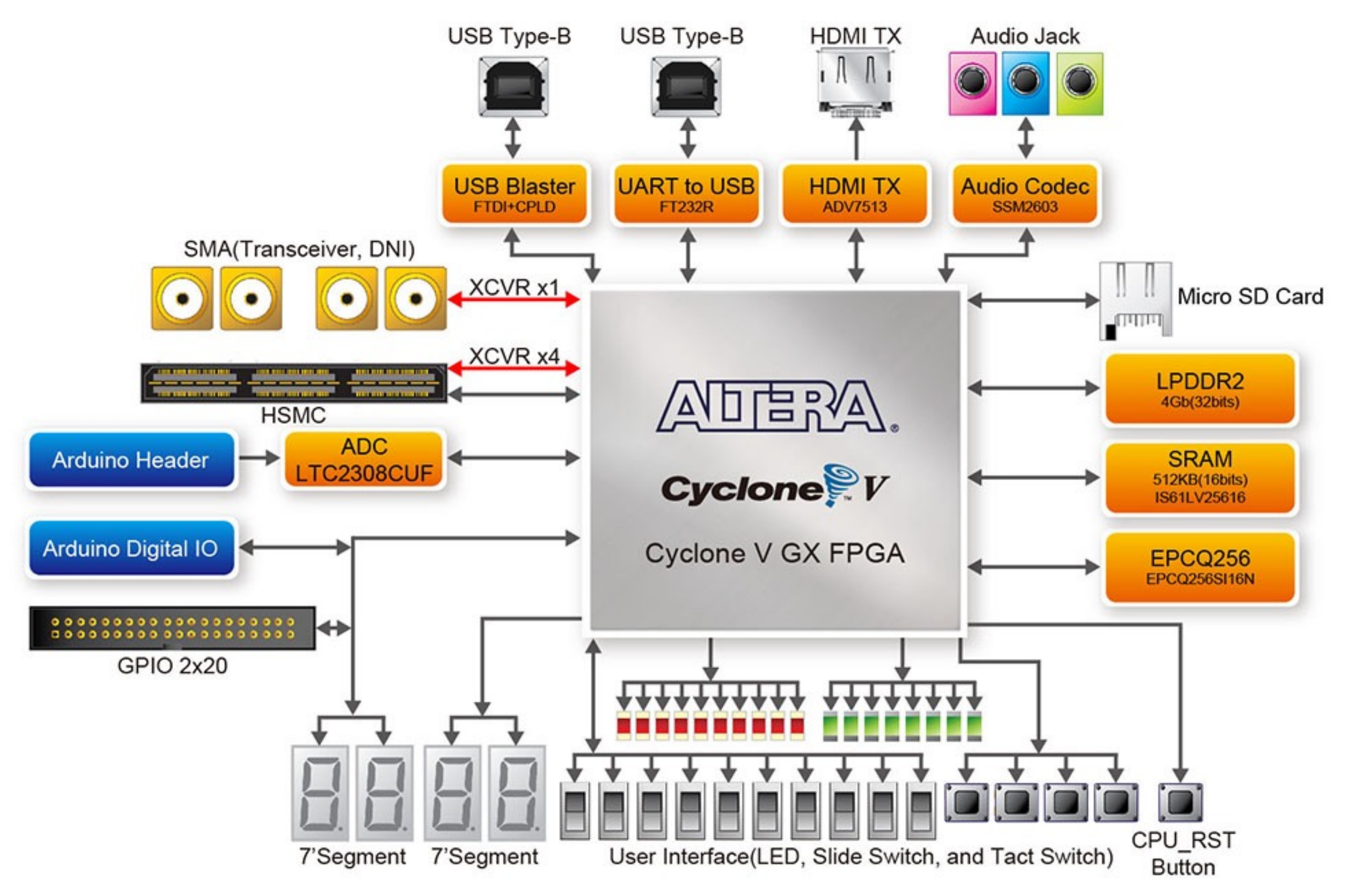
HDL Code
entity leddcd is
port(
d: in std_logic_vector(3 downto 0);
s: out std_logic_vector(6 downto 0);
);
end;
architecture leddcd_arch of leddcd is
begin
Schematic
slate
ap
Route
Bitstream
load
GA
Routing Resources
Logic or Timing Simulation
d<0>
d<1>
d<2>
s<0>
Bitstream

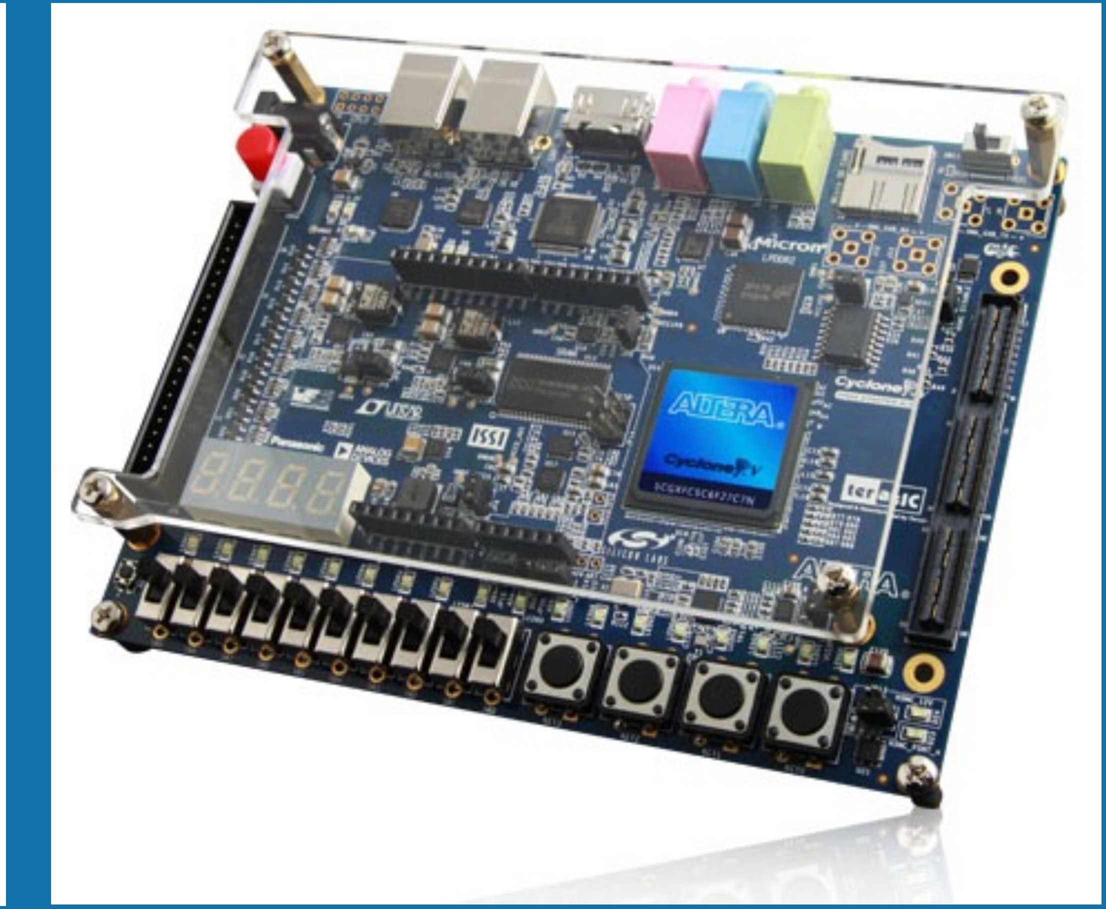
Preliminary Block Diagram



FPGA: Cyclone V GX Starter Kit

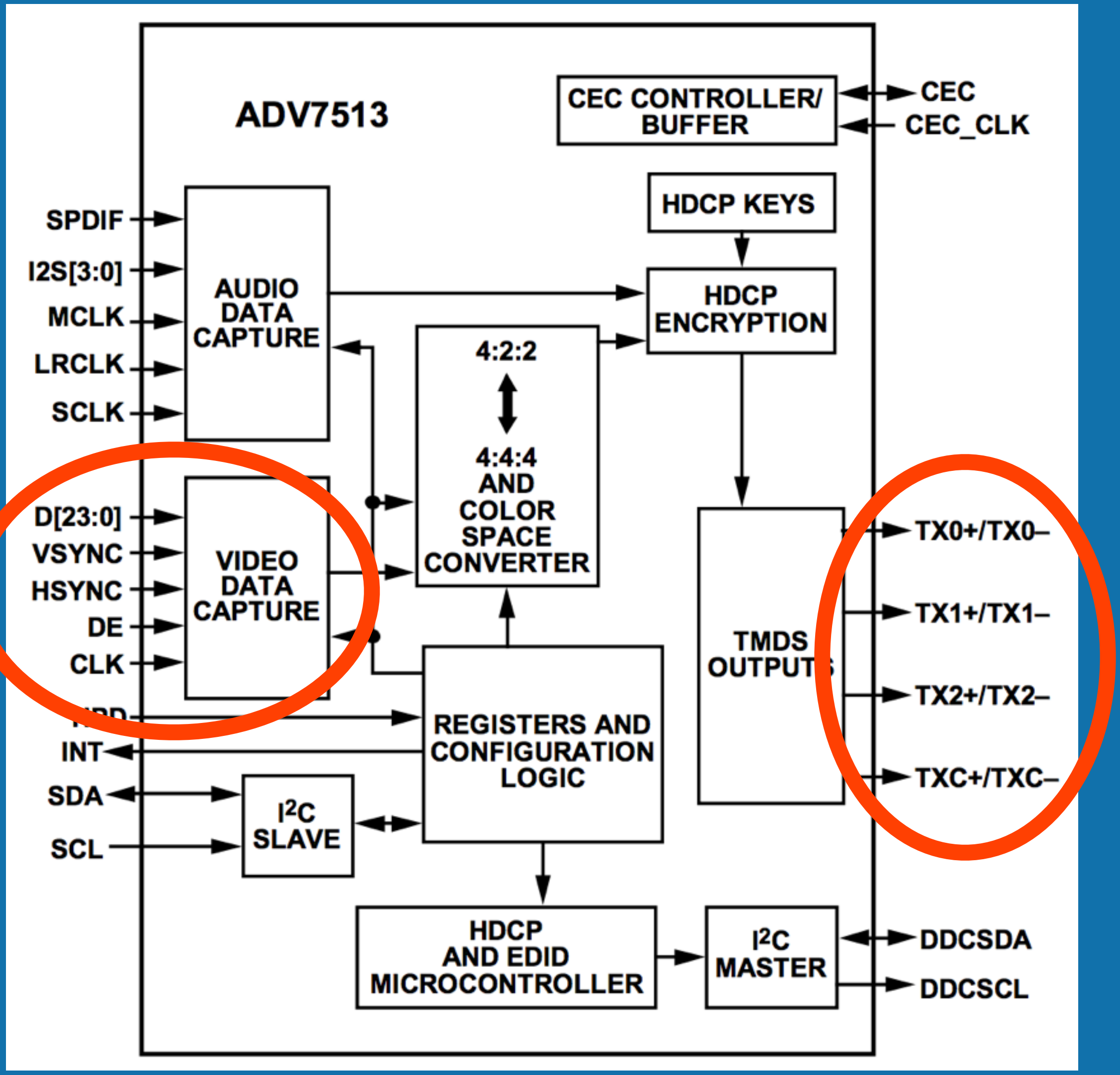
- Cyclone 5CGXFC5C6F27C7N, $179 USD
- Performance v. power v. cost
- Got up and running in minimal time (~2 days)
- Terasic does not provide schematics or PCB layout in native format :(



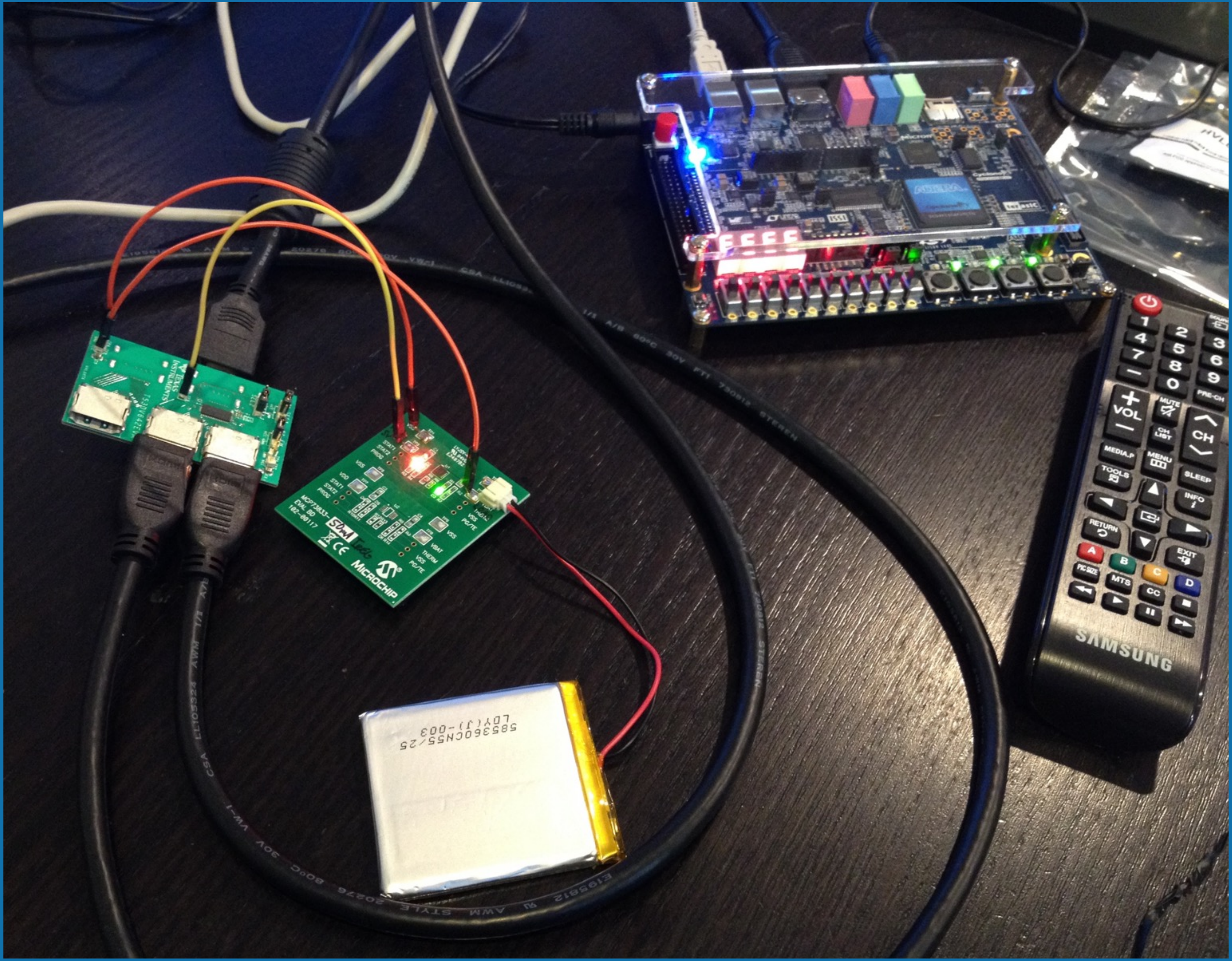


HDMI TX: ADV7513

- 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



Early Proof of Concept

- Everything about FPGA development is slow!
  - Dev. tools are giant and unwieldy
  - Long compile/test cycles (~15 minutes)
- Verilog trial by fire
- Needed to figure out how to draw on screen

img2mif

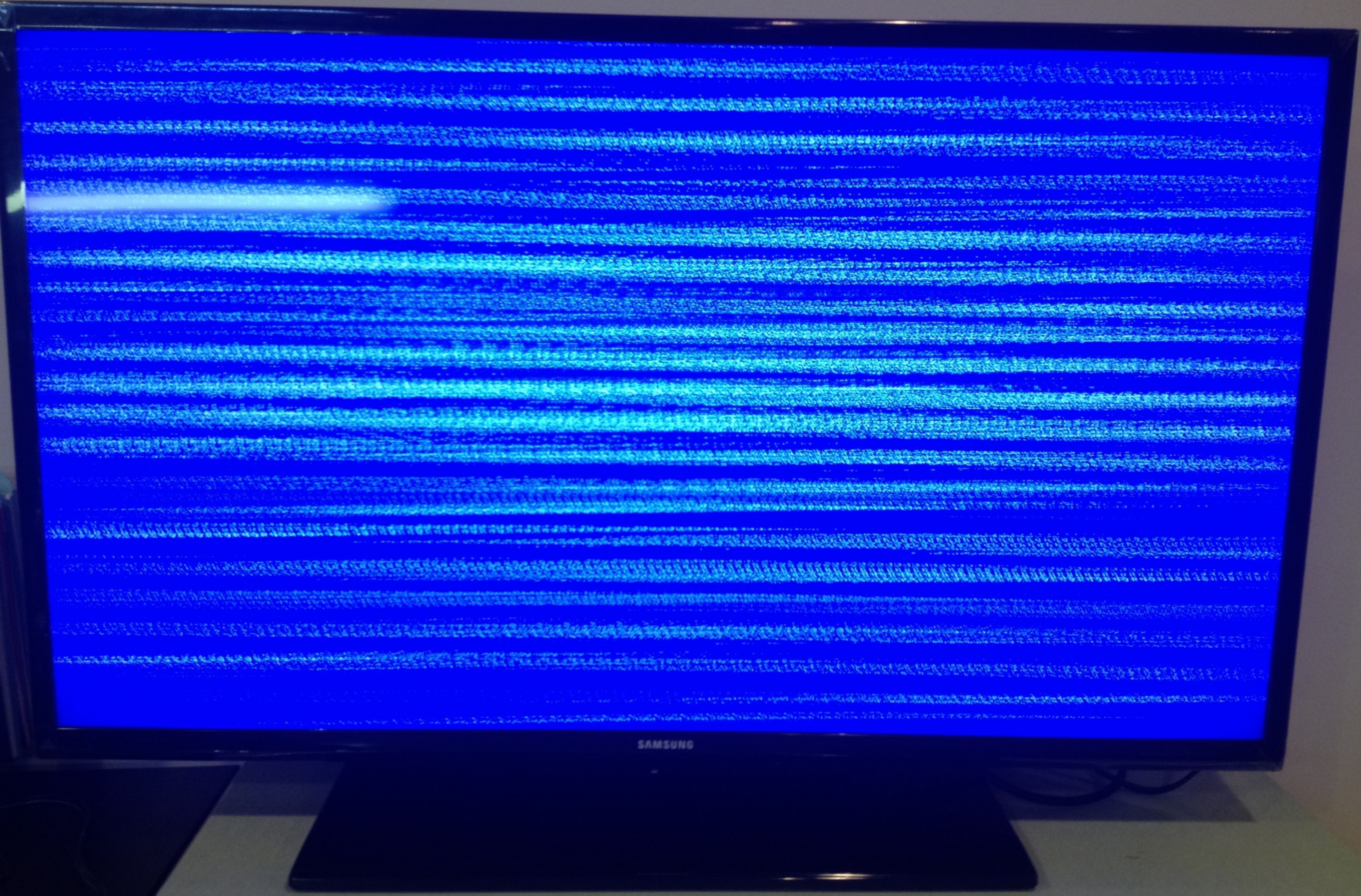
- Converts BMP to Memory Initialization File (MIF)
- Preload image into Cyclone V internal RAM
- https://github.com/joegrand/img2mif
- Forked from LonghornEngineer

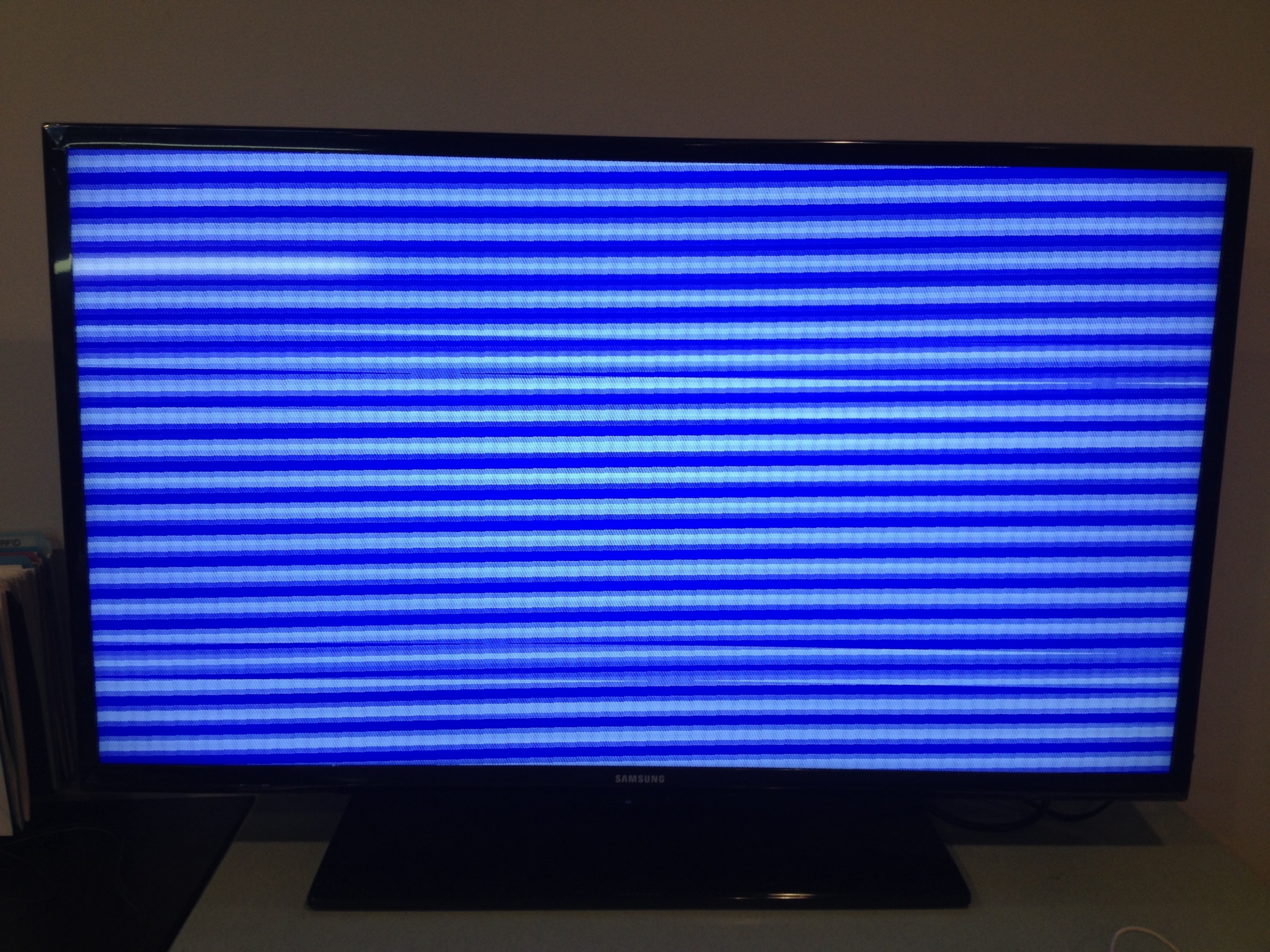
Power Supply Trickery

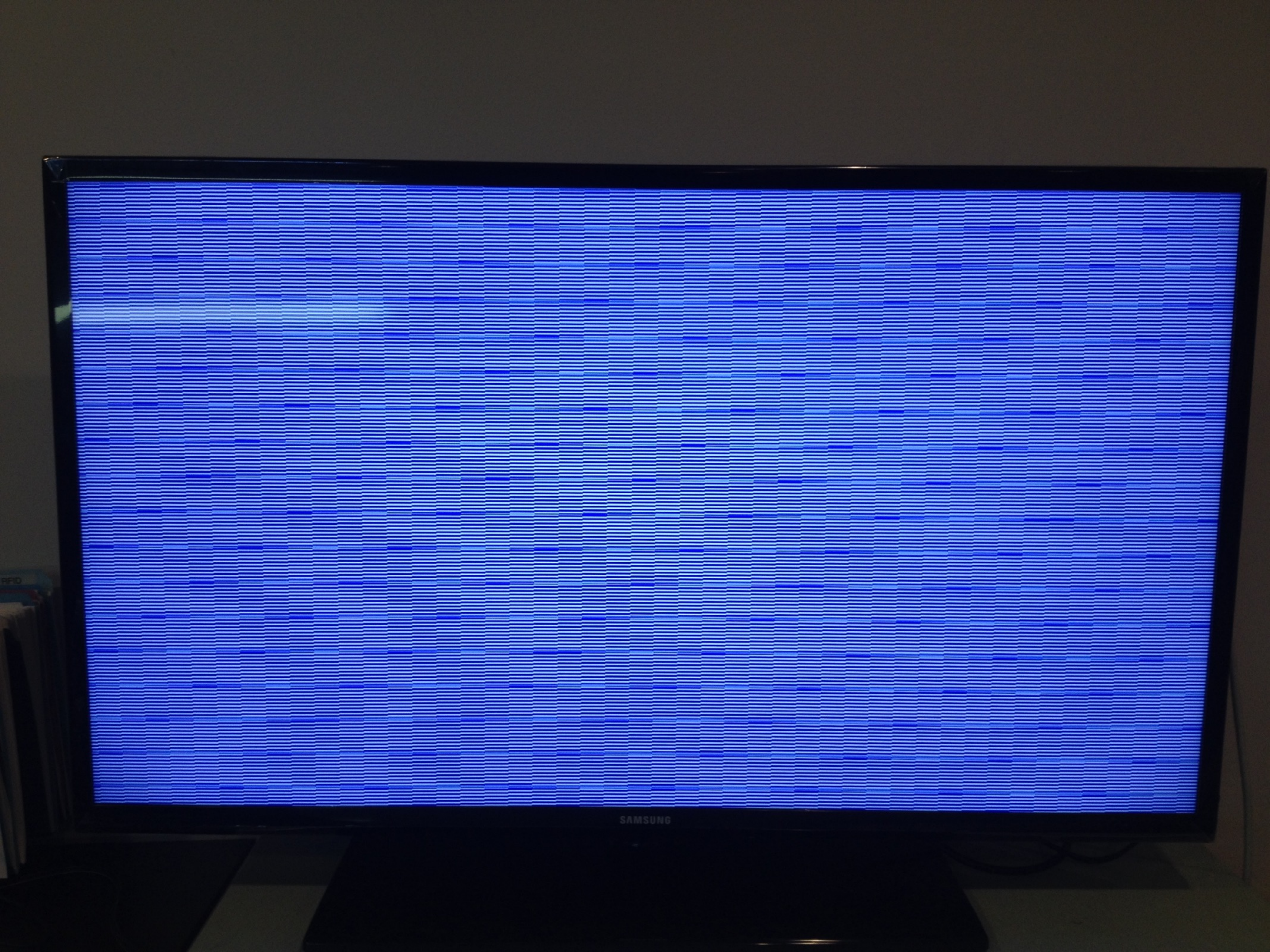
- HDMI source current must be > 55mA per spec.
- FPGAs (esp. development boards) are power hungry
- How to allow pass-through mode to work at all times?
- How to provide power to FPGA system when needed?

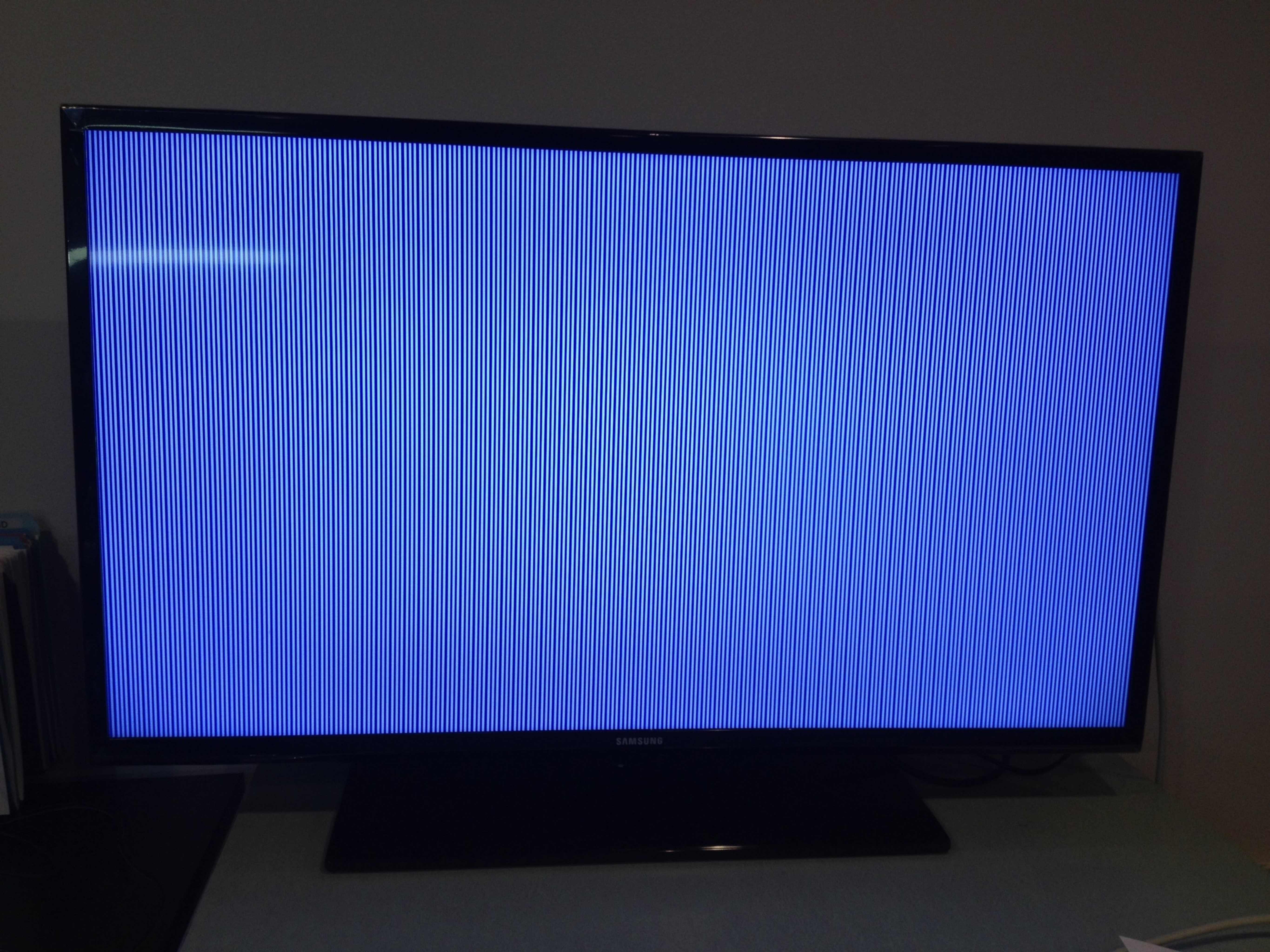
Block RAM (1080p, 1bpp)

- Much trial and error
- Very frustration
- Wow

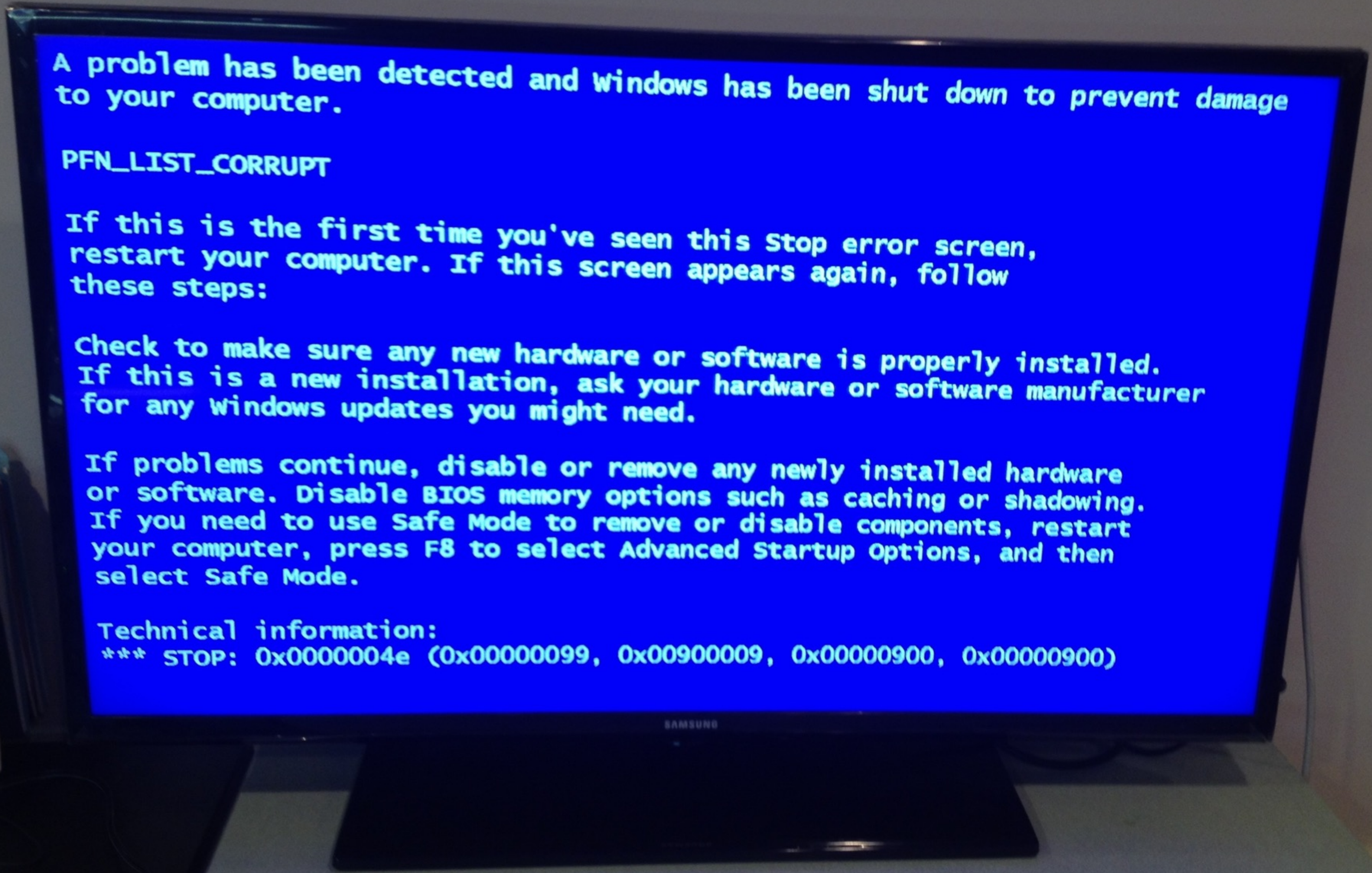

SAMSUNG


SAMSUNG


SAMSUNG


SAMSUNG

SAMSUNG
BREAKFAST



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

PFN_LIST_CORRUPT

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:
*** STOP: 0x0000004e (0x00000099, 0x00900009, 0x00000900, 0x00000900)
```

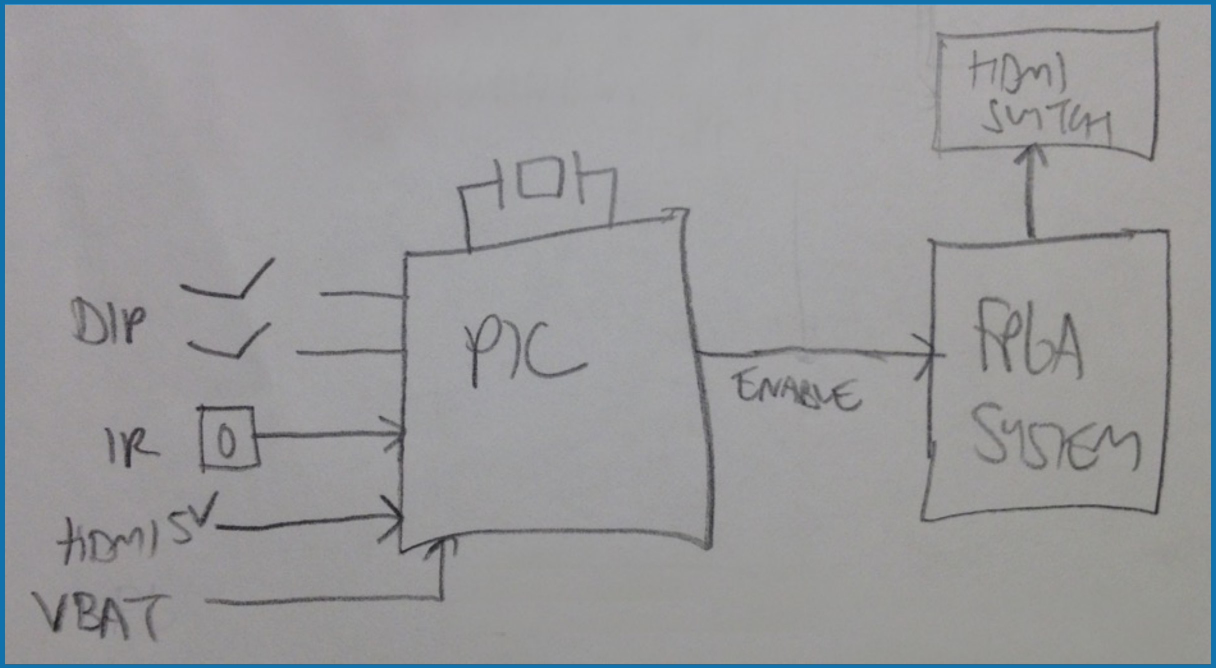
Proof of Concept Demonstration

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

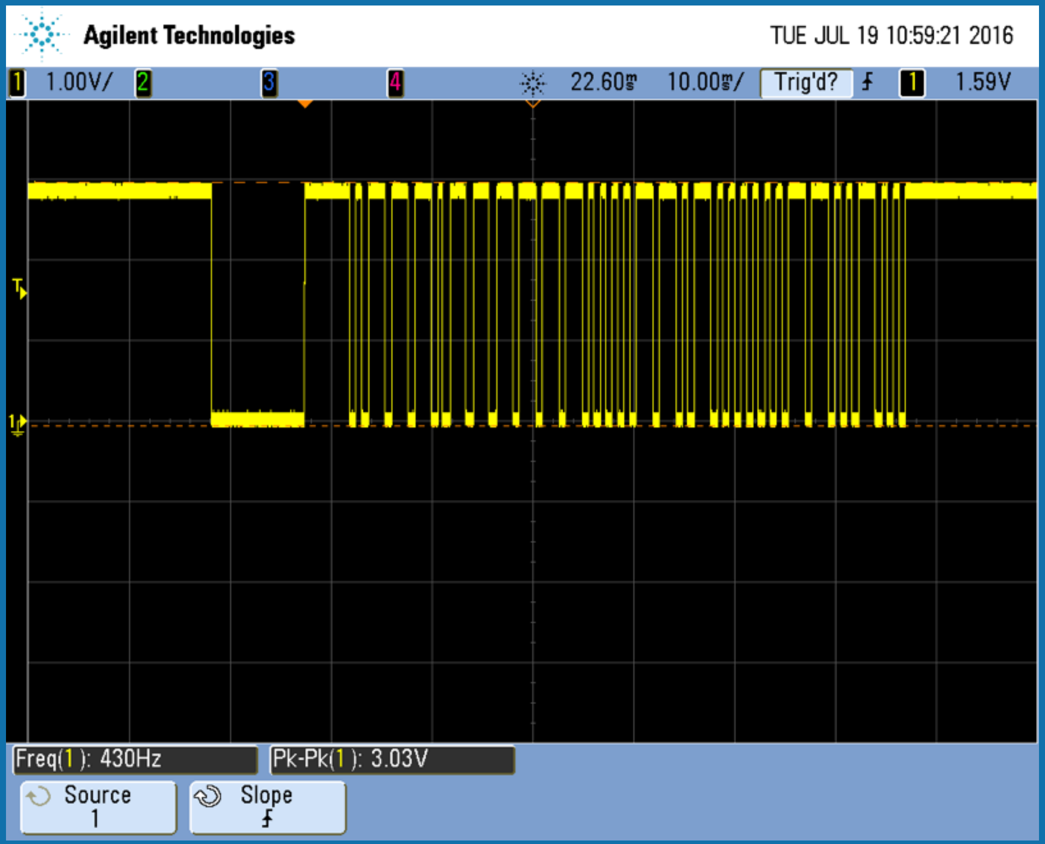
PIC Front End

- 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

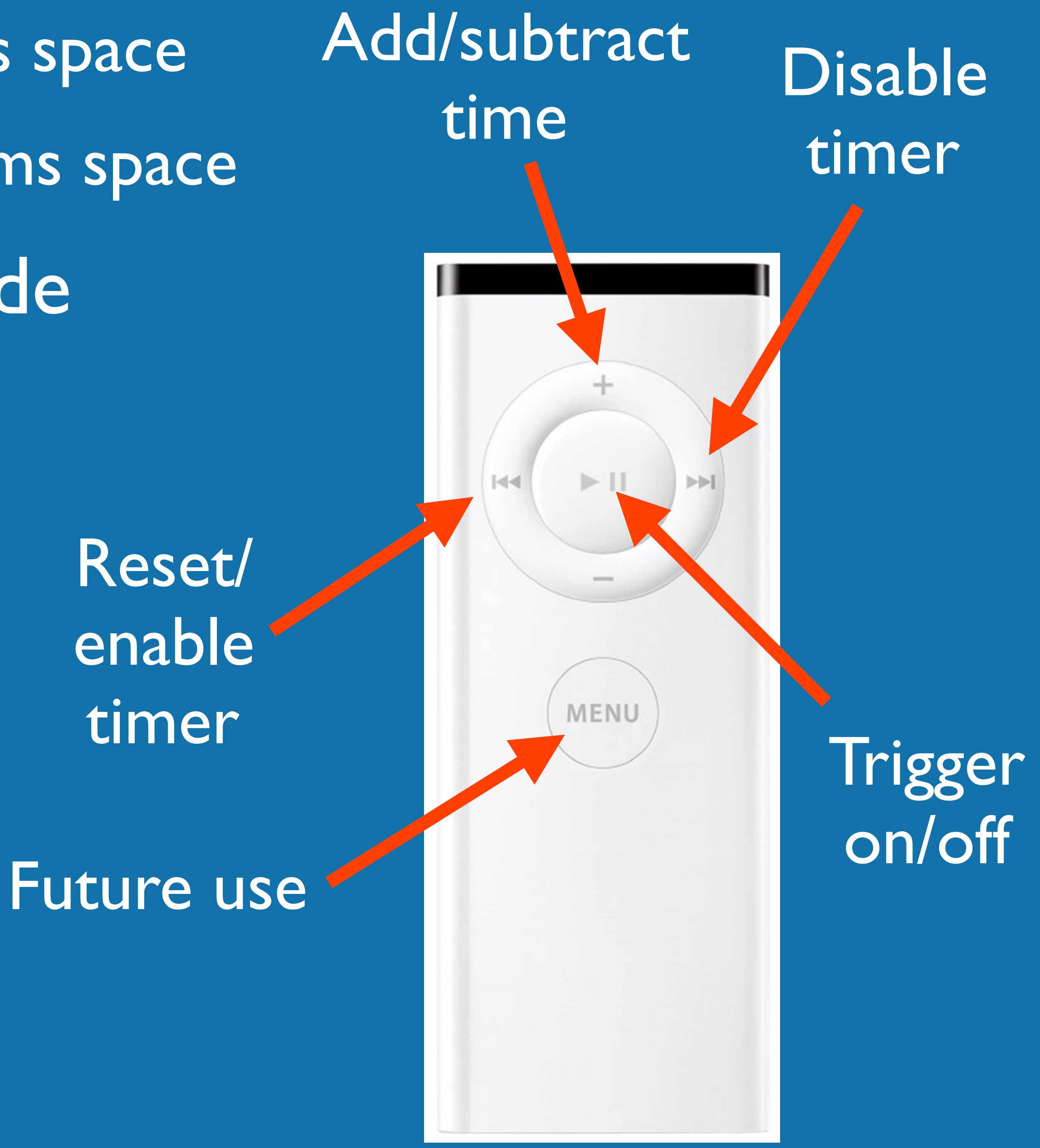
- NEC transmission protocol (same PHY, different data)
  - Start: 9ms pulse burst, 4.5ms space
  - Logic '1': 562.5µs pulse, 562.5µs space
  - Logic '0': 562.5µs pulse, 1.6875ms space
- Bare bones detection w/ wide timing margins



Agilent Technologies TUE JUL 19 10:59:21 2016

1 1.00V/ 2 3 4 22.60ms 10.00ms/ Trig'd? 1 1.59V

Freq(1): 430Hz Pk-Pk(1): 3.03V



Add/subtract time

Disable timer

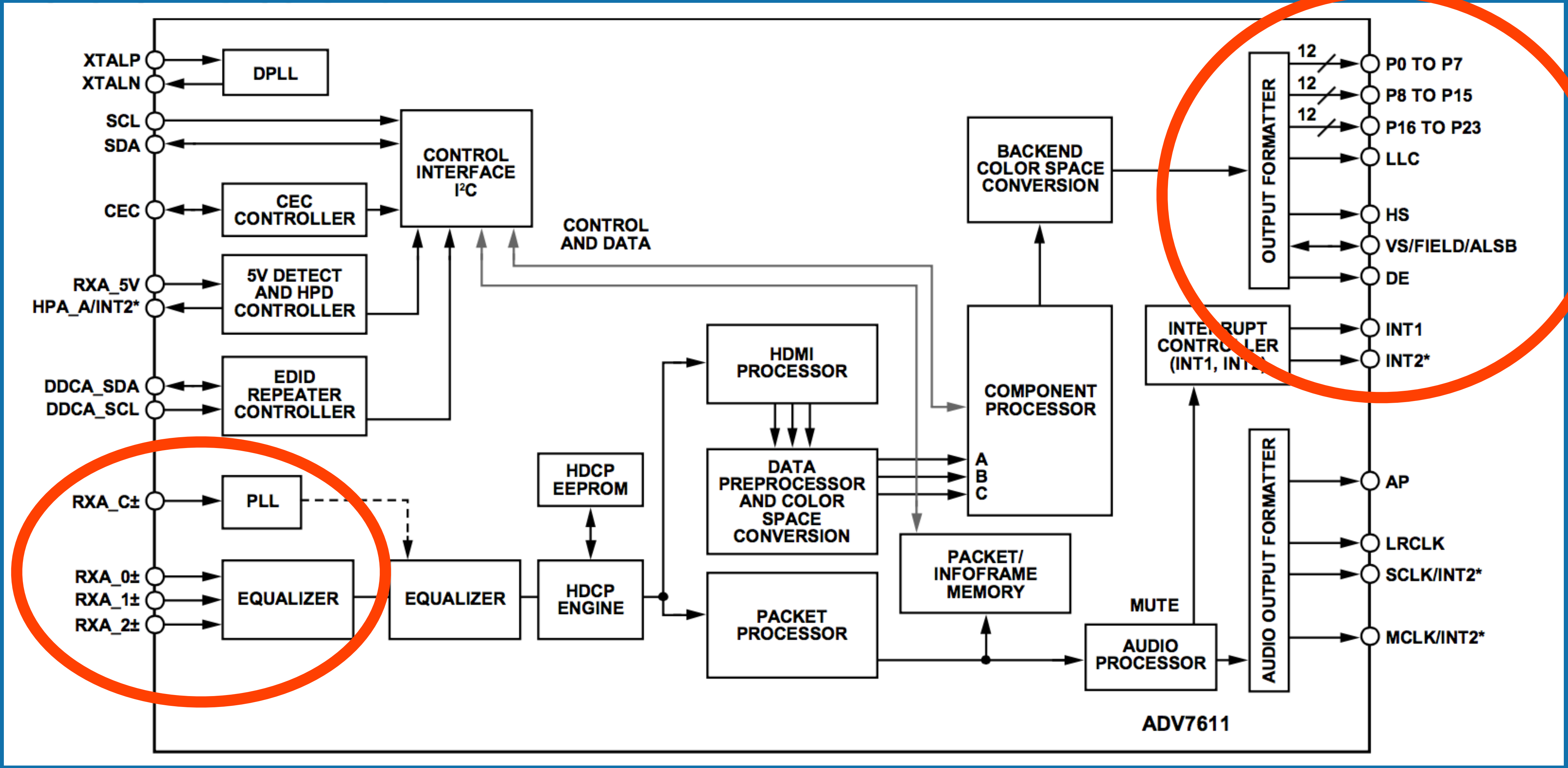
Reset/ enable timer

Trigger on/off

Future use

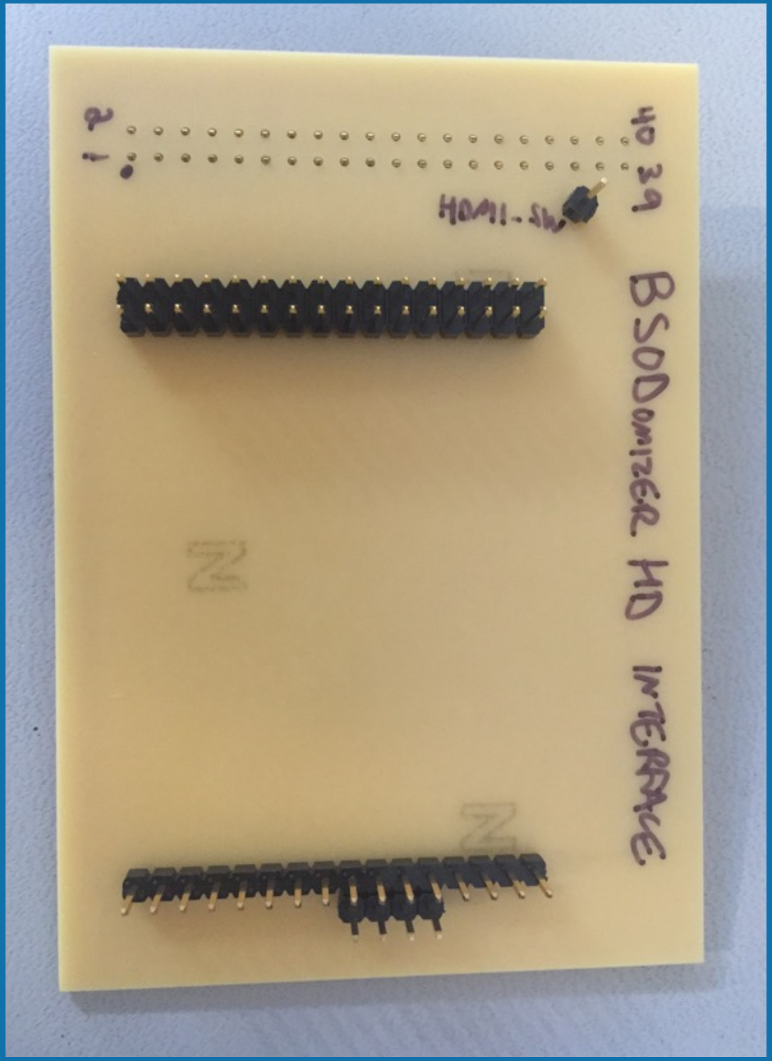
HDMI RX: ADV7611

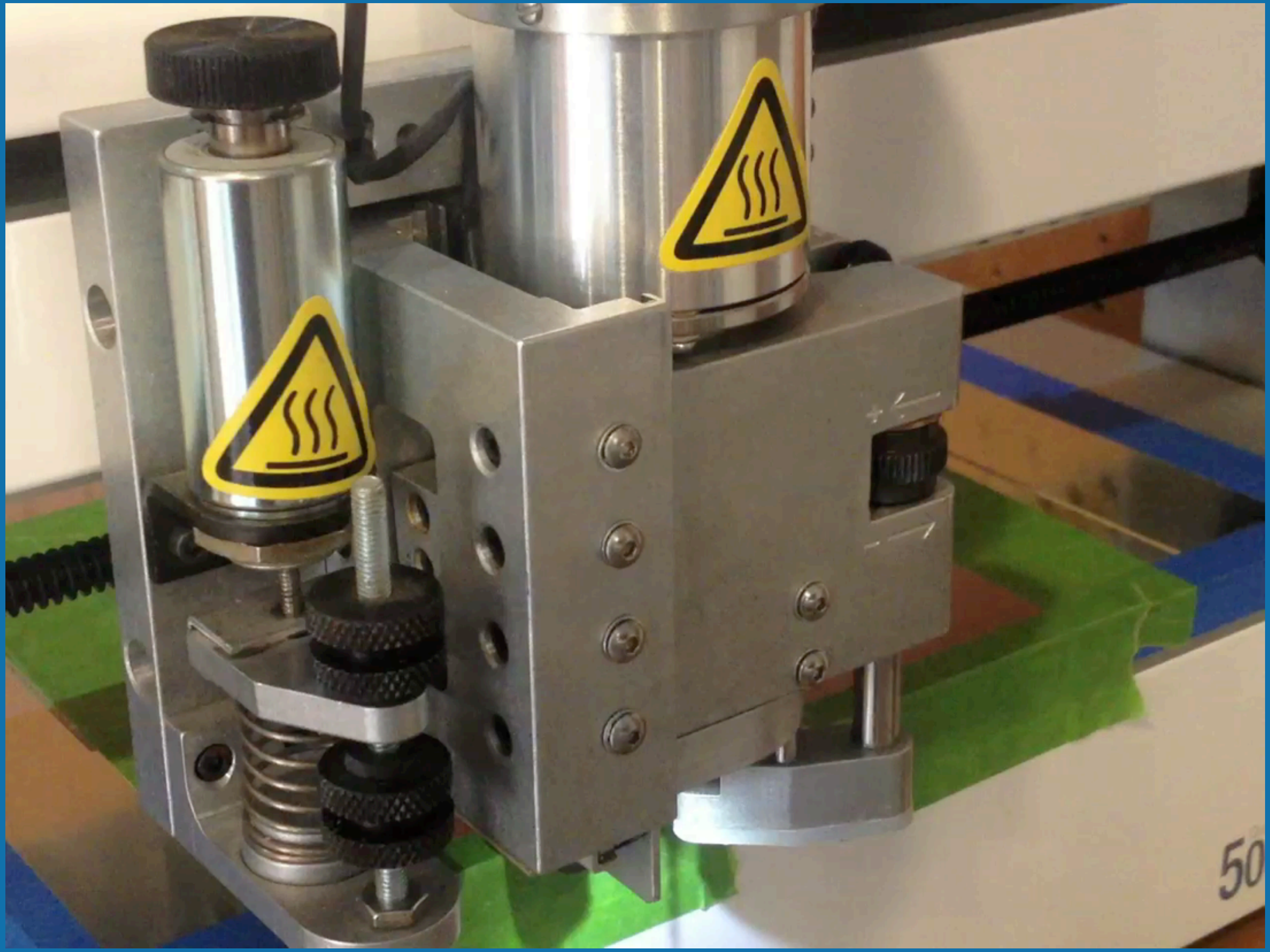
- Deserialization converter to reduce resources of FPGA
- Used HDMI Light V2 as a reference/breakout board, https://github.com/esar/hdmilight-v2



Interface Board

- C5G to HDMI RX (HDMI Light V2)
- T-Tech QuickCircuit 5000 for nearly instant gratification
- 12 mil trace/14 mil space, easily delaminated during soldering, required tiny repairs

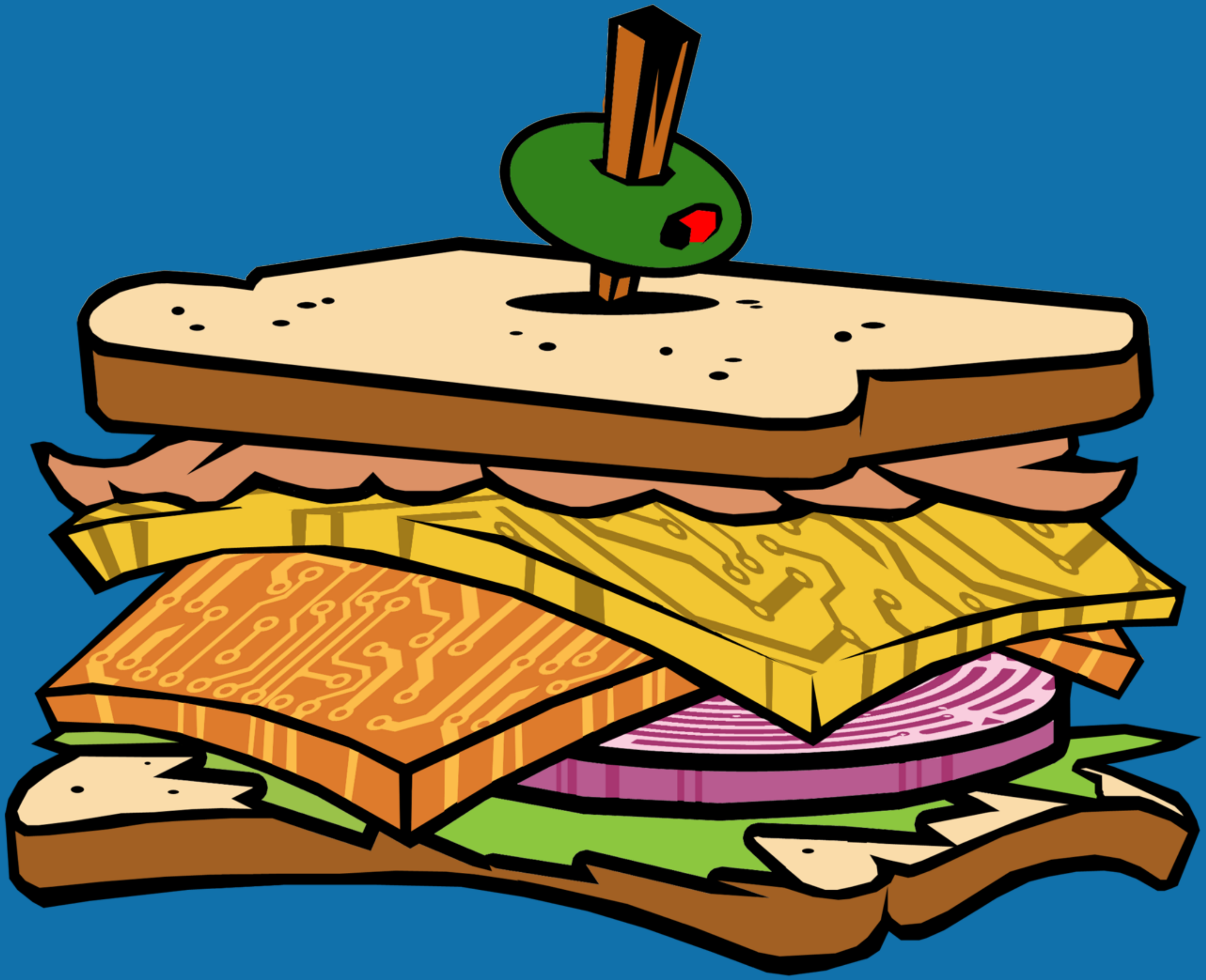




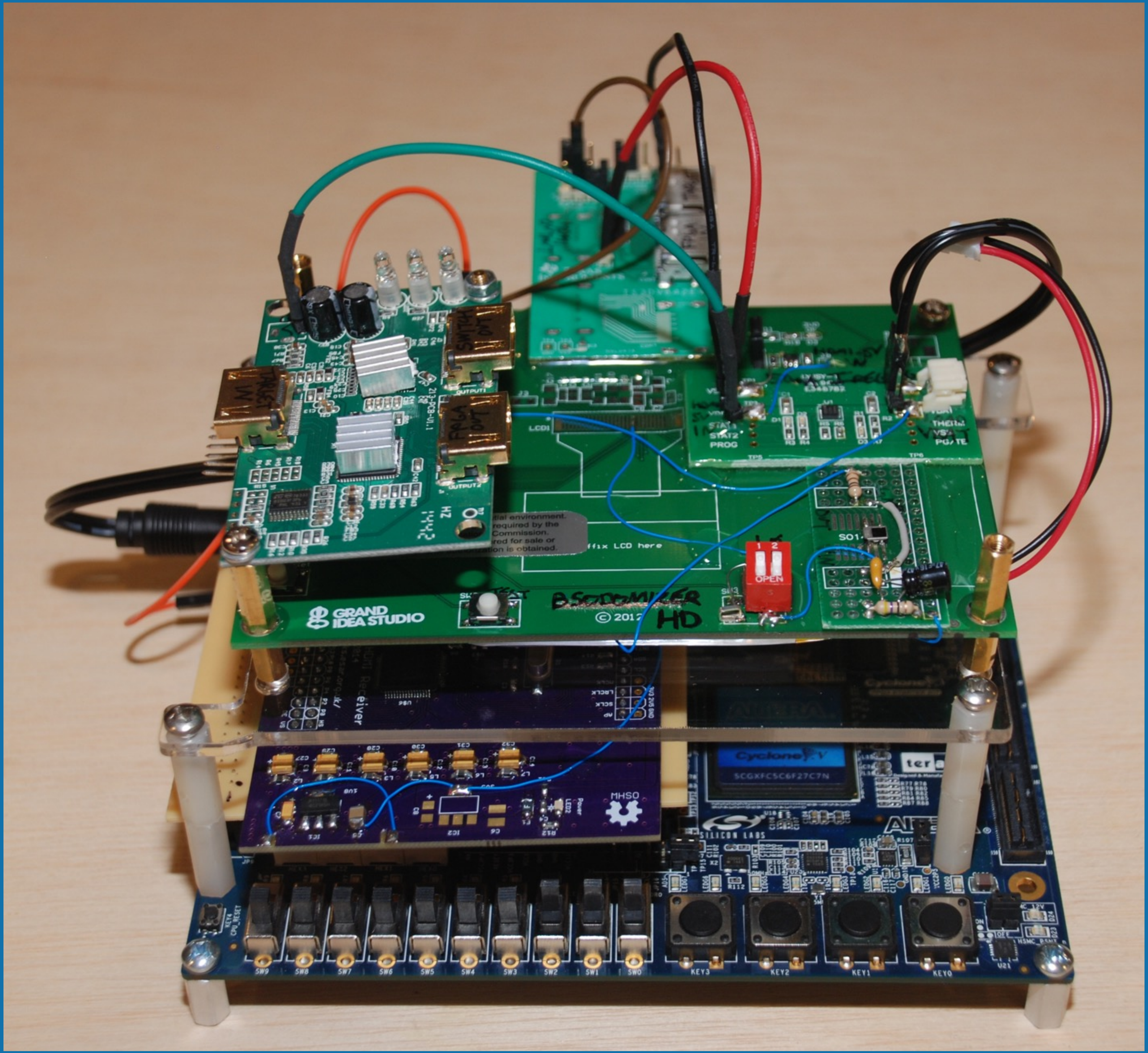
Other Subsystems

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

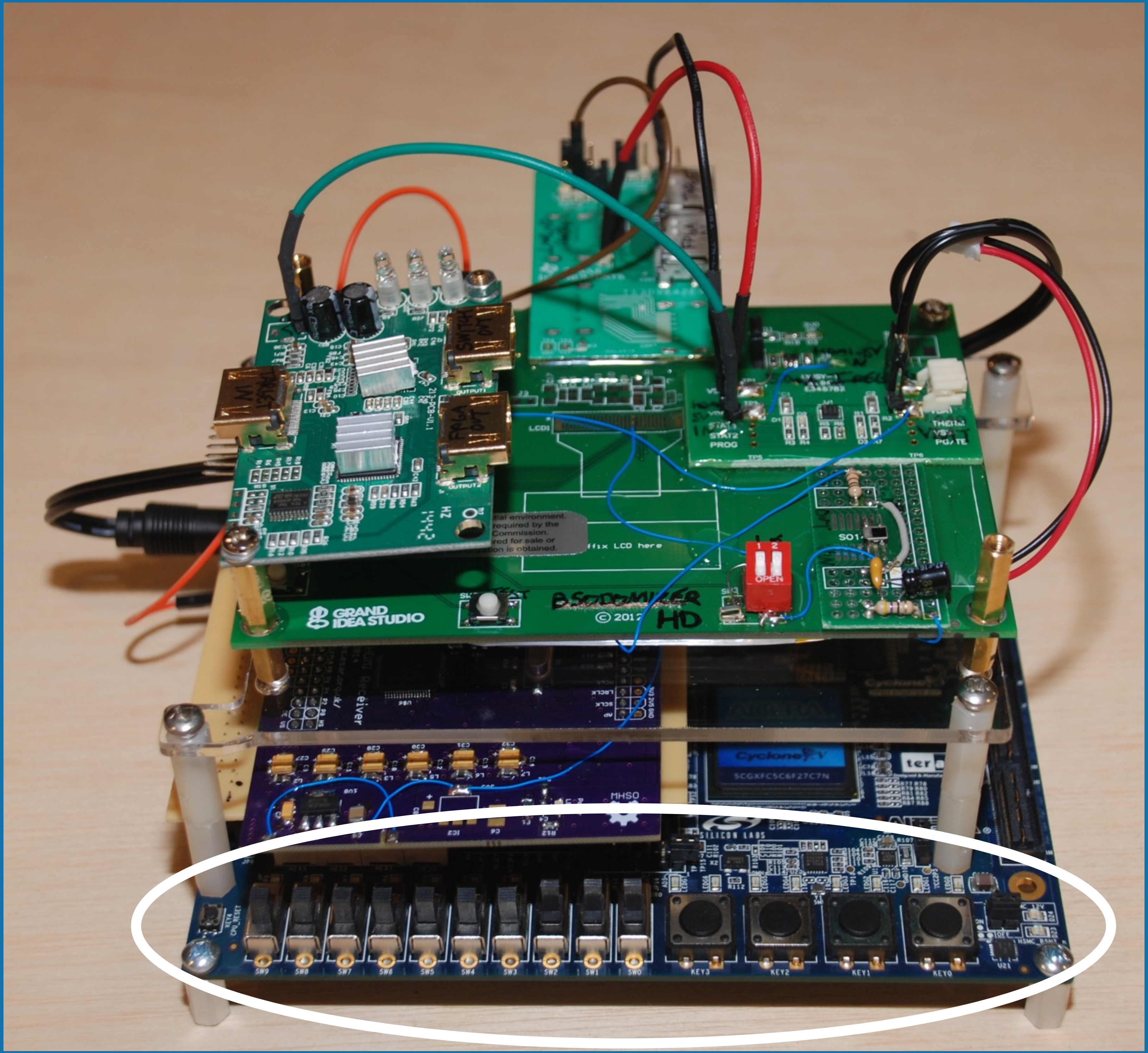
Circuit Board Sandwich



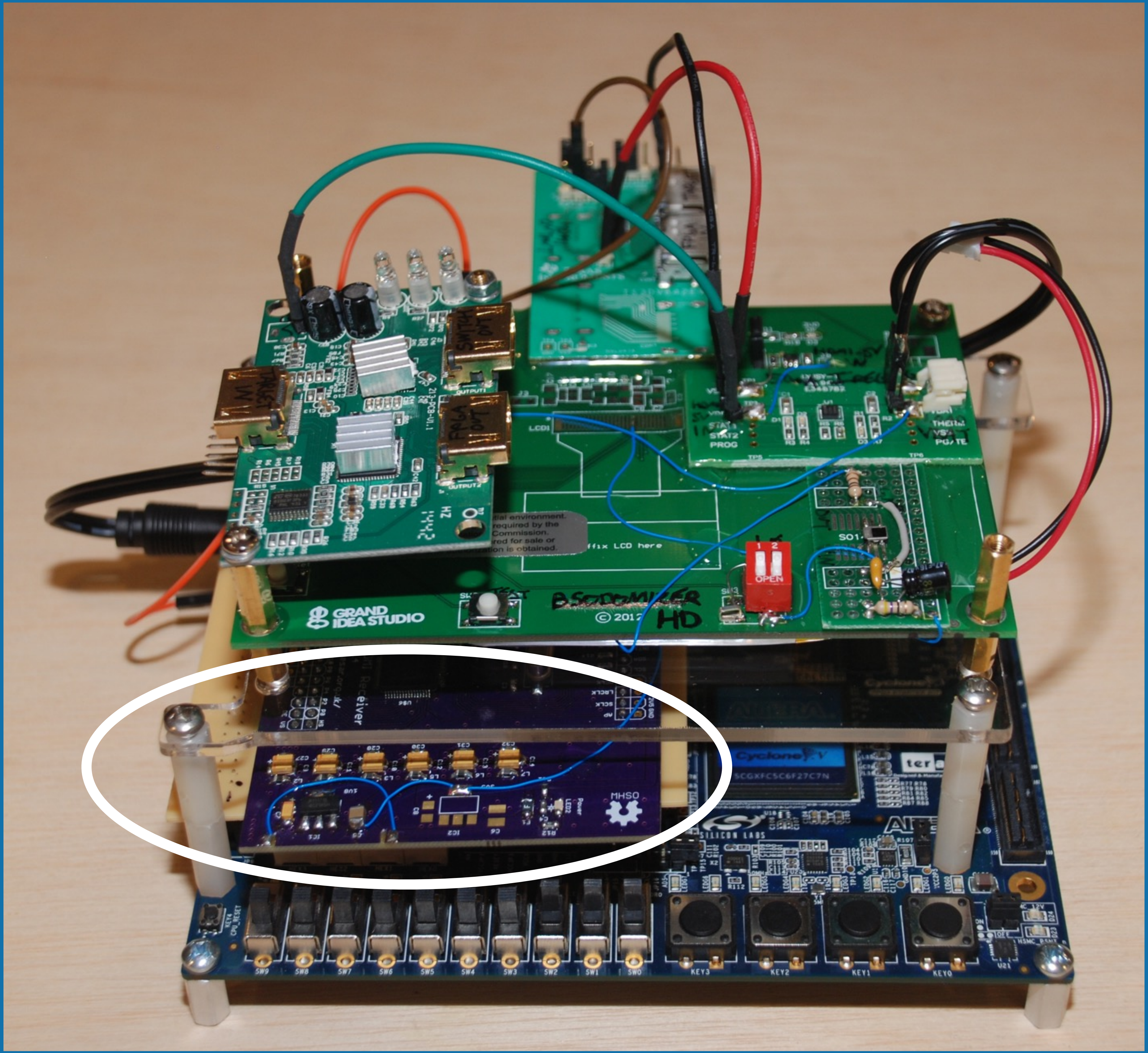
Circuit Board Sandwich



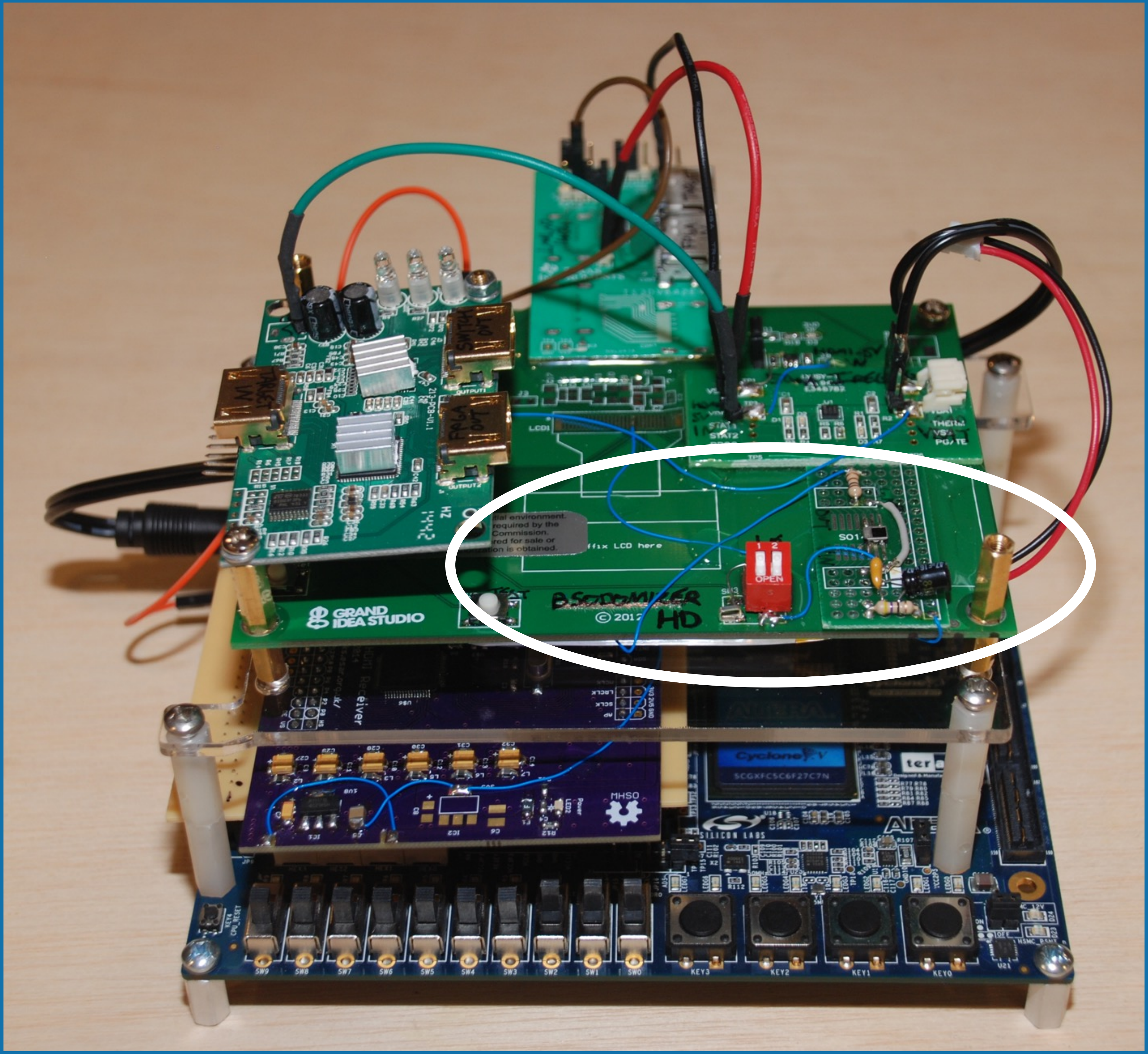
Circuit Board Sandwich



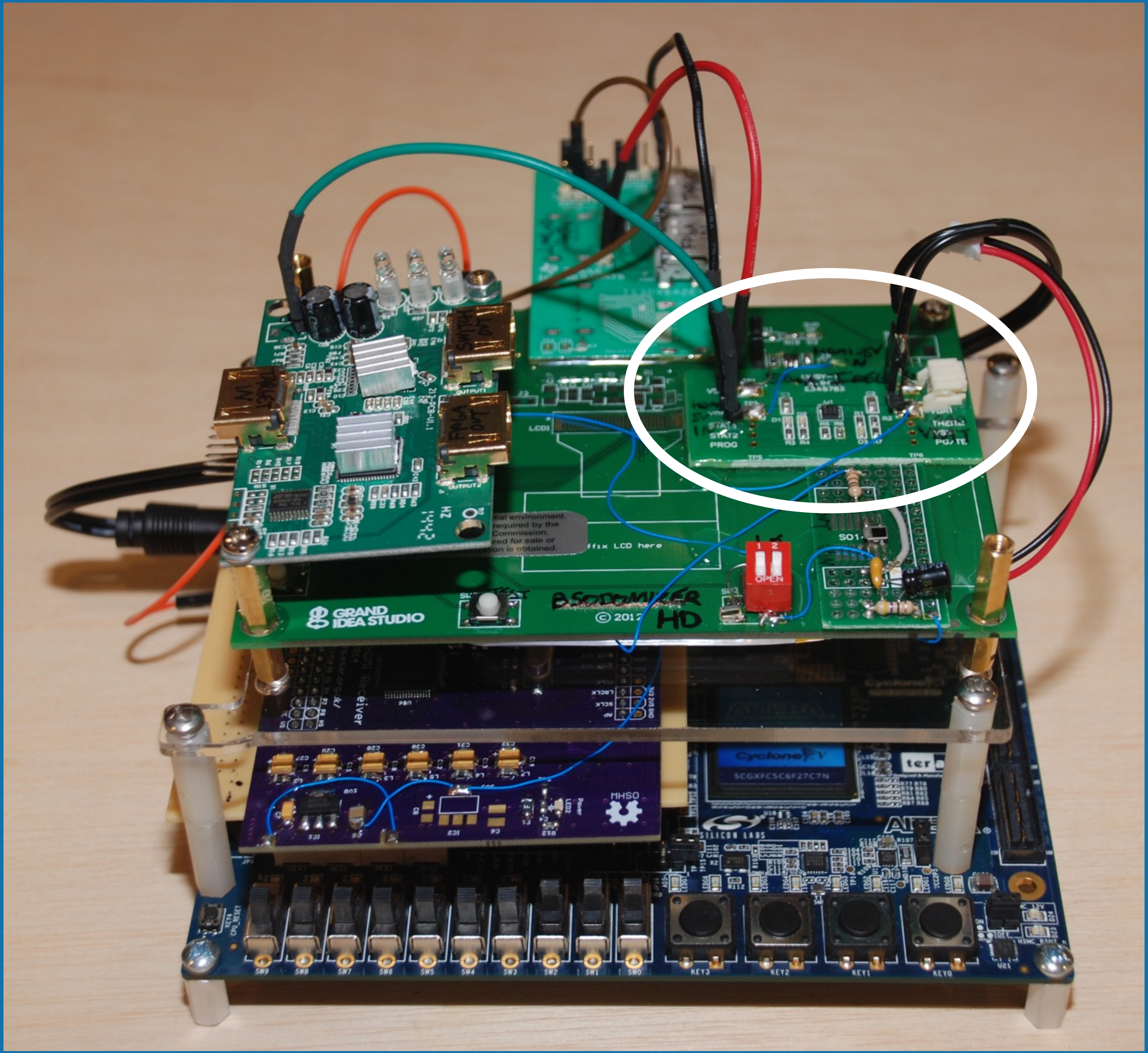
Circuit Board Sandwich



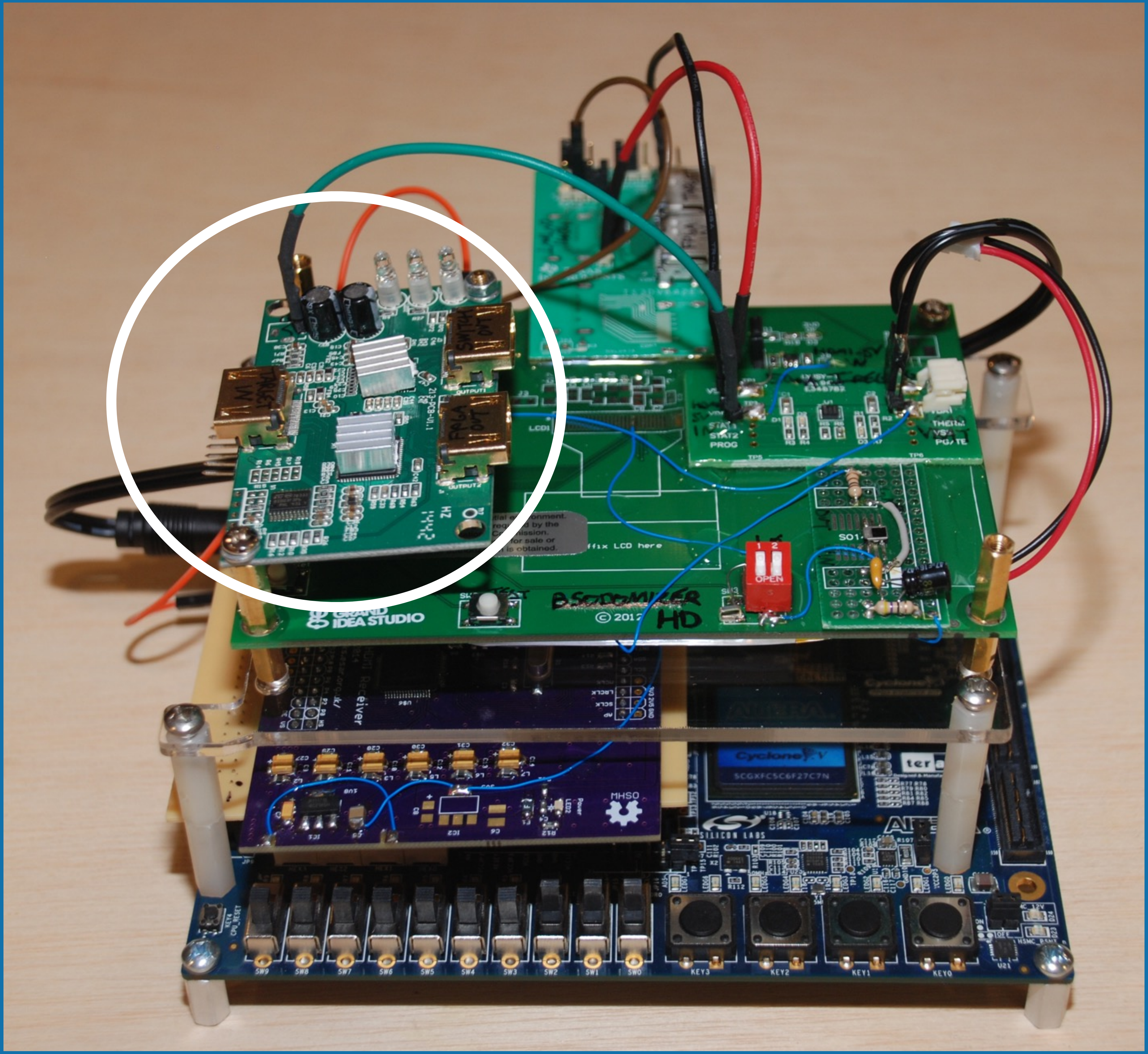
Circuit Board Sandwich



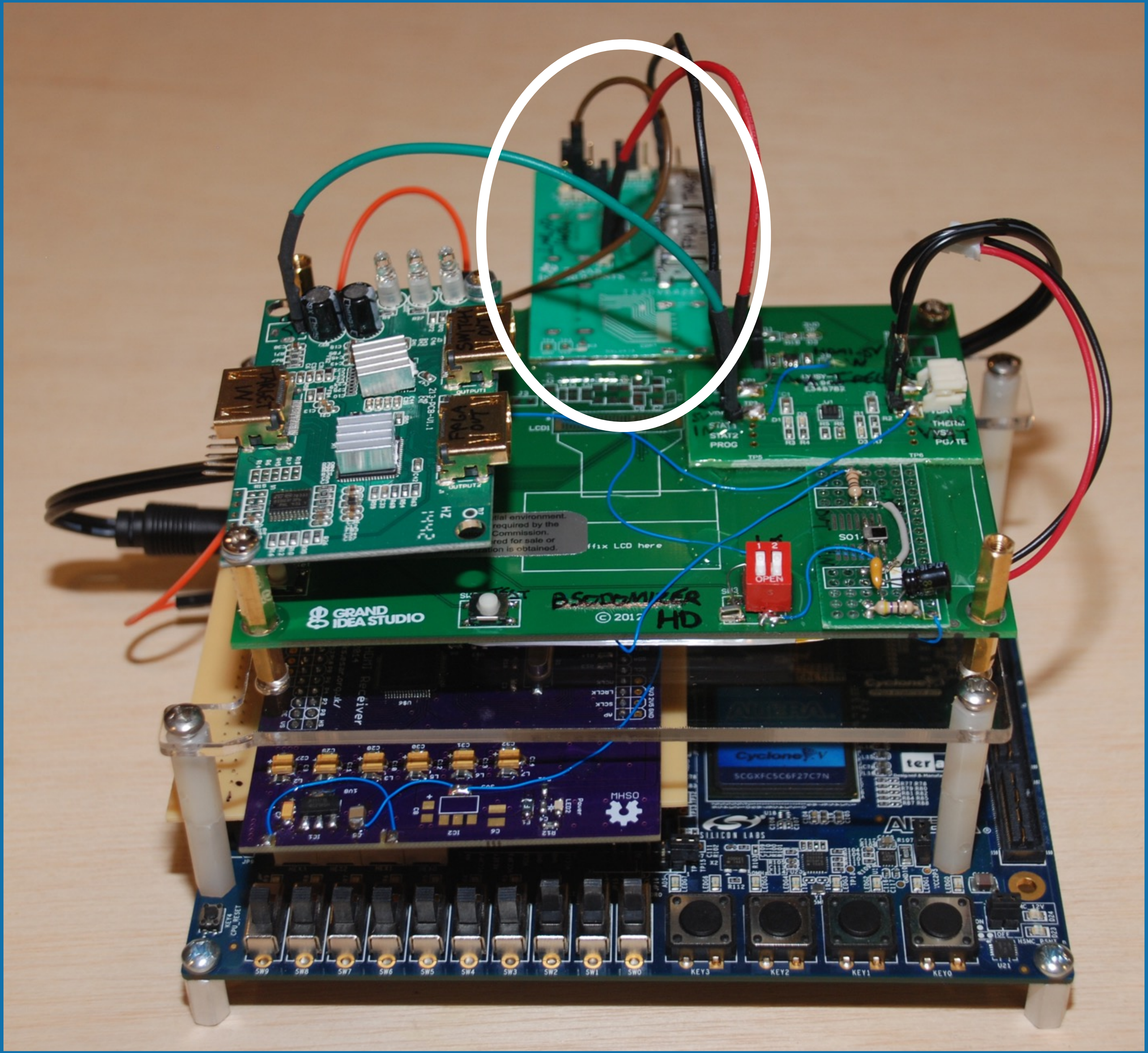
Circuit Board Sandwich



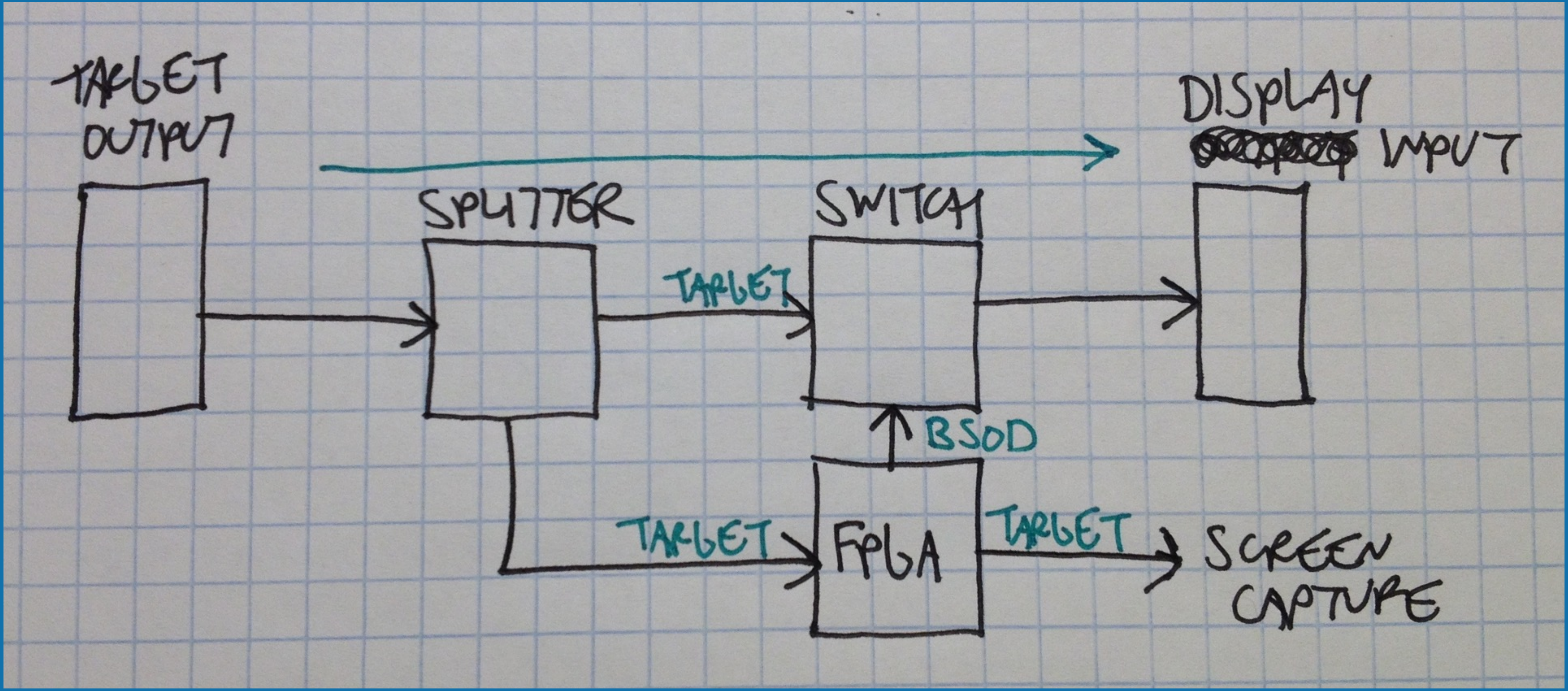
Circuit Board Sandwich



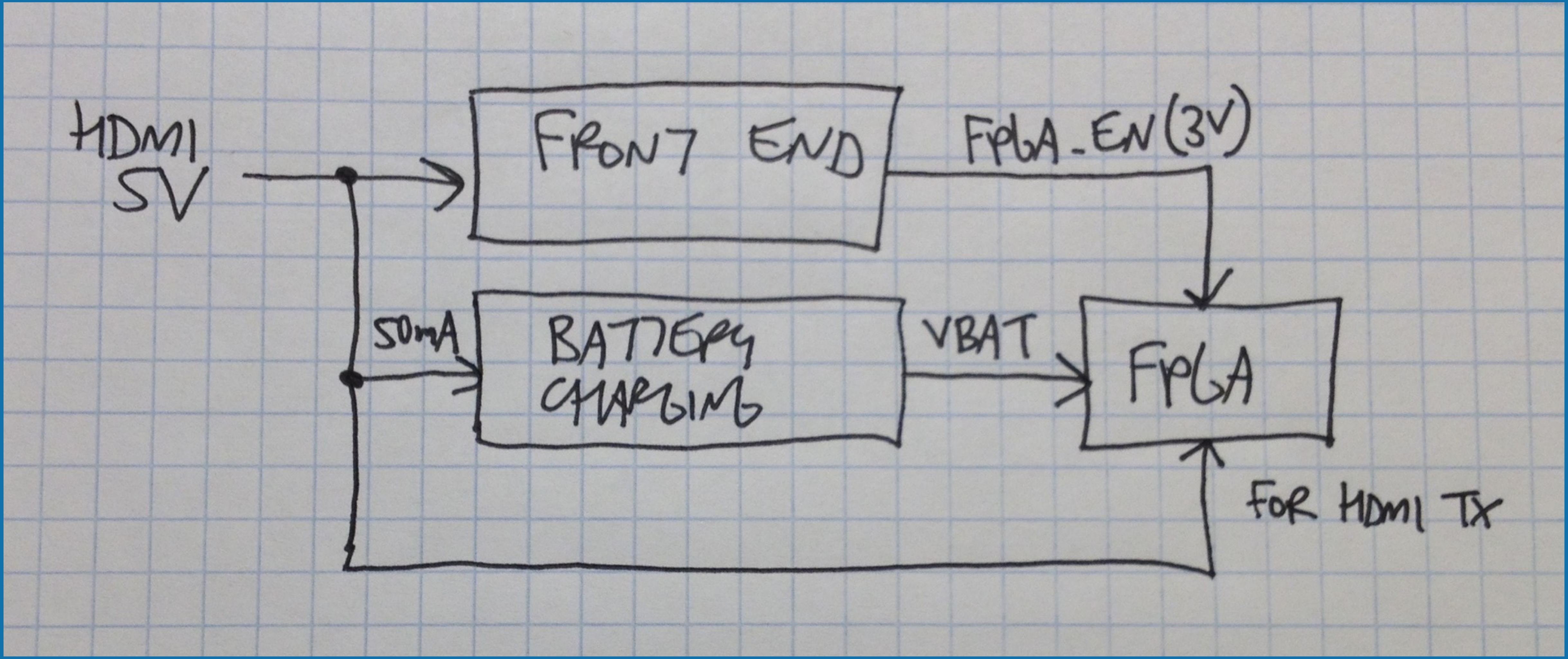
Circuit Board Sandwich



HDMI Signal Path



Power Supply Path



- Front end & battery charging always via HDMI 5V
- FPGA subsystem only powered (by battery) when triggered

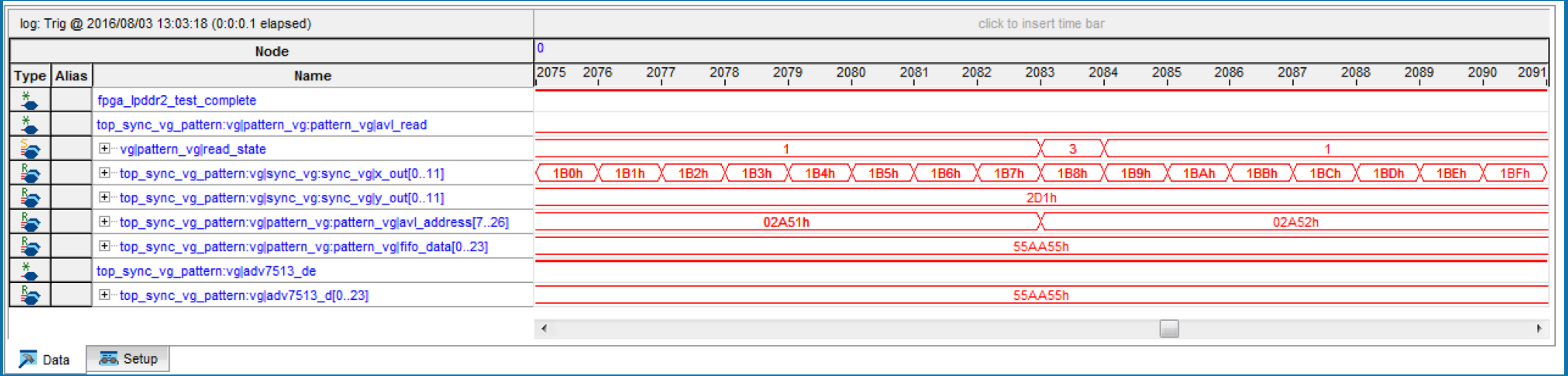
Current Measurements

- PIC Front End = HDMI 5V @ 1.76mA
- C5G Dev. Board (fully loaded) = LiPo 3.7V @ 438mA
- System functions down to 3.4V (limited by PIC to 3.6V)

- GSP585460 2000mAh, 3.7V Lithium Polymer
  - Assume 70% of capacity down to 3.6V = 1400mAh
  - ~3.2 hours of active BSODomy

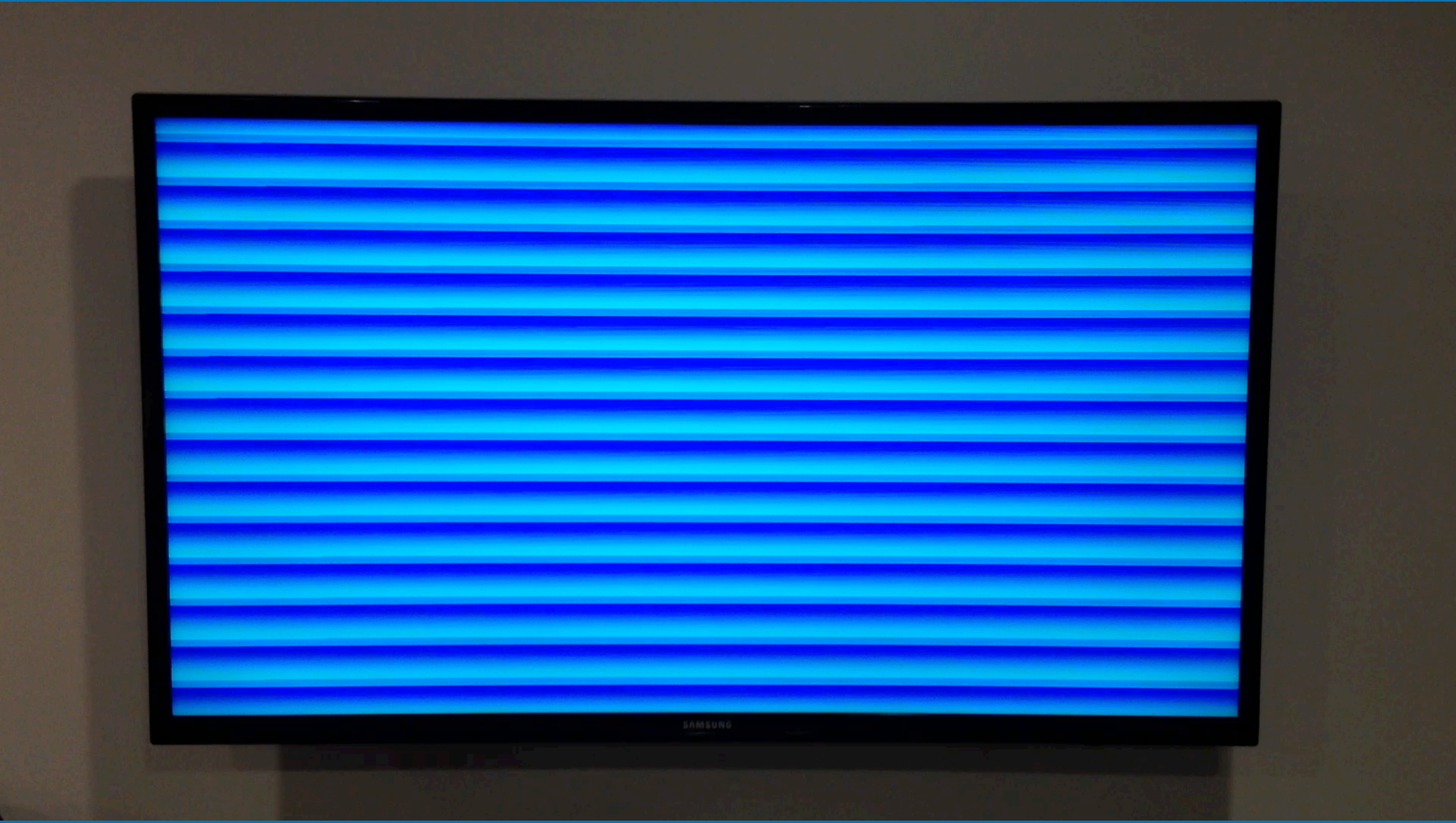
LPDDR2 SDRAM (1080p, 24bpp)

- 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...



log: Trig @ 2016/08/03 13:03:18 (0:0:0.1 elapsed)

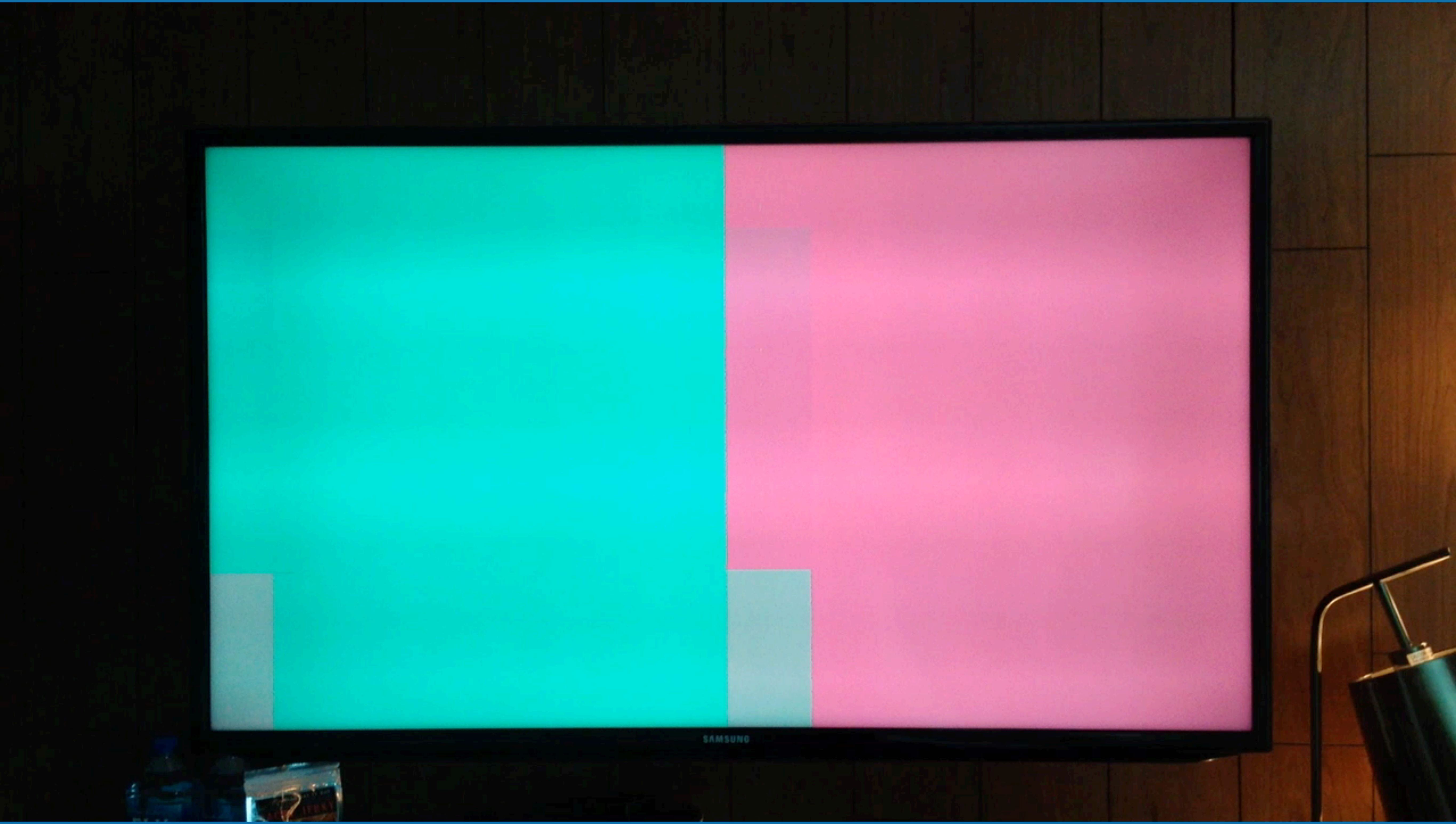
Type	Alias	Name
		fpga_lpddr2_test_complete
		top_sync_vg_pattern:vg|pattern_vg:pattern_vg|avl_read
		⊞ vg|pattern_vg|read_state
		⊞ top_sync_vg_pattern:vg|sync_vg:sync_vg|x_out[0..11]
		⊞ top_sync_vg_pattern:vg|sync_vg:sync_vg|y_out[0..11]
		⊞ top_sync_vg_pattern:vg|pattern_vg:pattern_vg|avl_address[7..26]
		⊞ top_sync_vg_pattern:vg|pattern_vg:pattern_vg|fifo_data[0..23]
		top_sync_vg_pattern:vg|adv7513_de
		⊞ top_sync_vg_pattern:vg|adv7513_d[0..23]


SAMSUNG

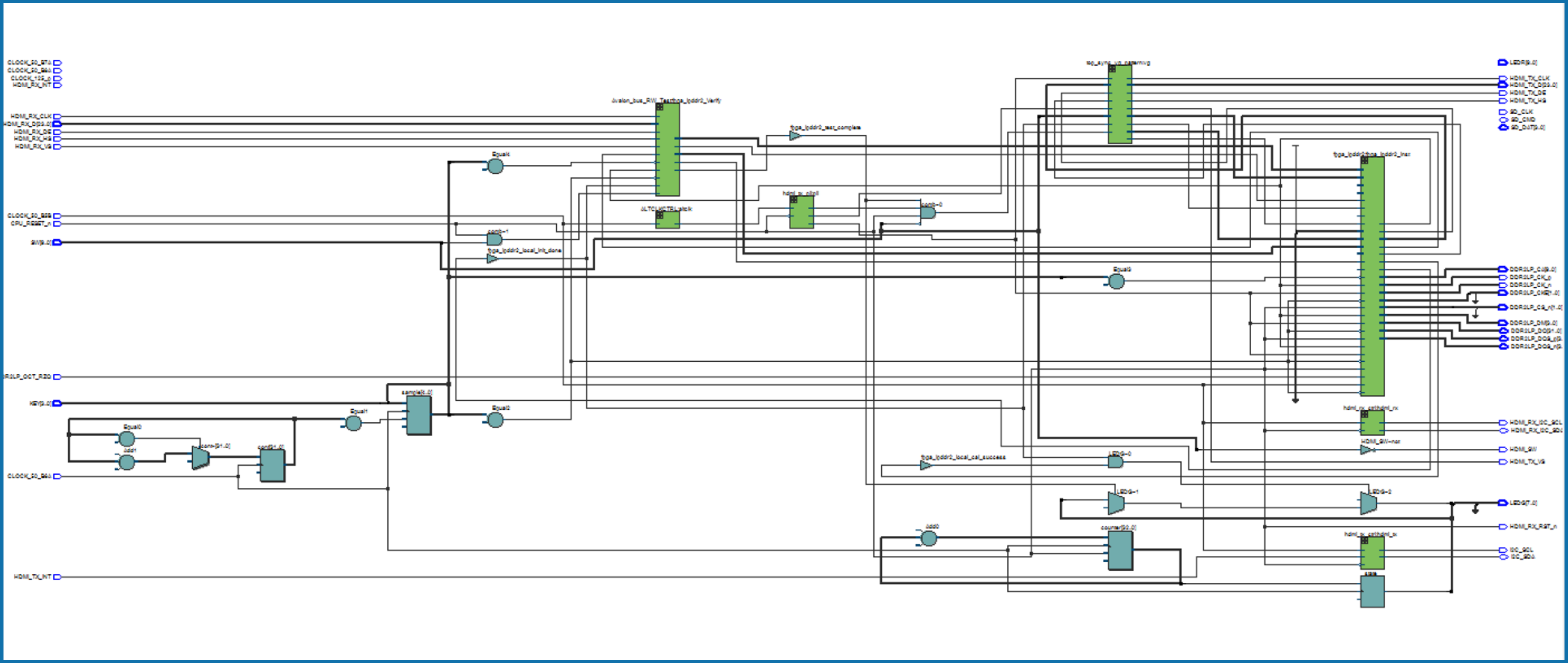
SAMSUNG

SAMSUNG

SAMSUNG


SAMSUNG

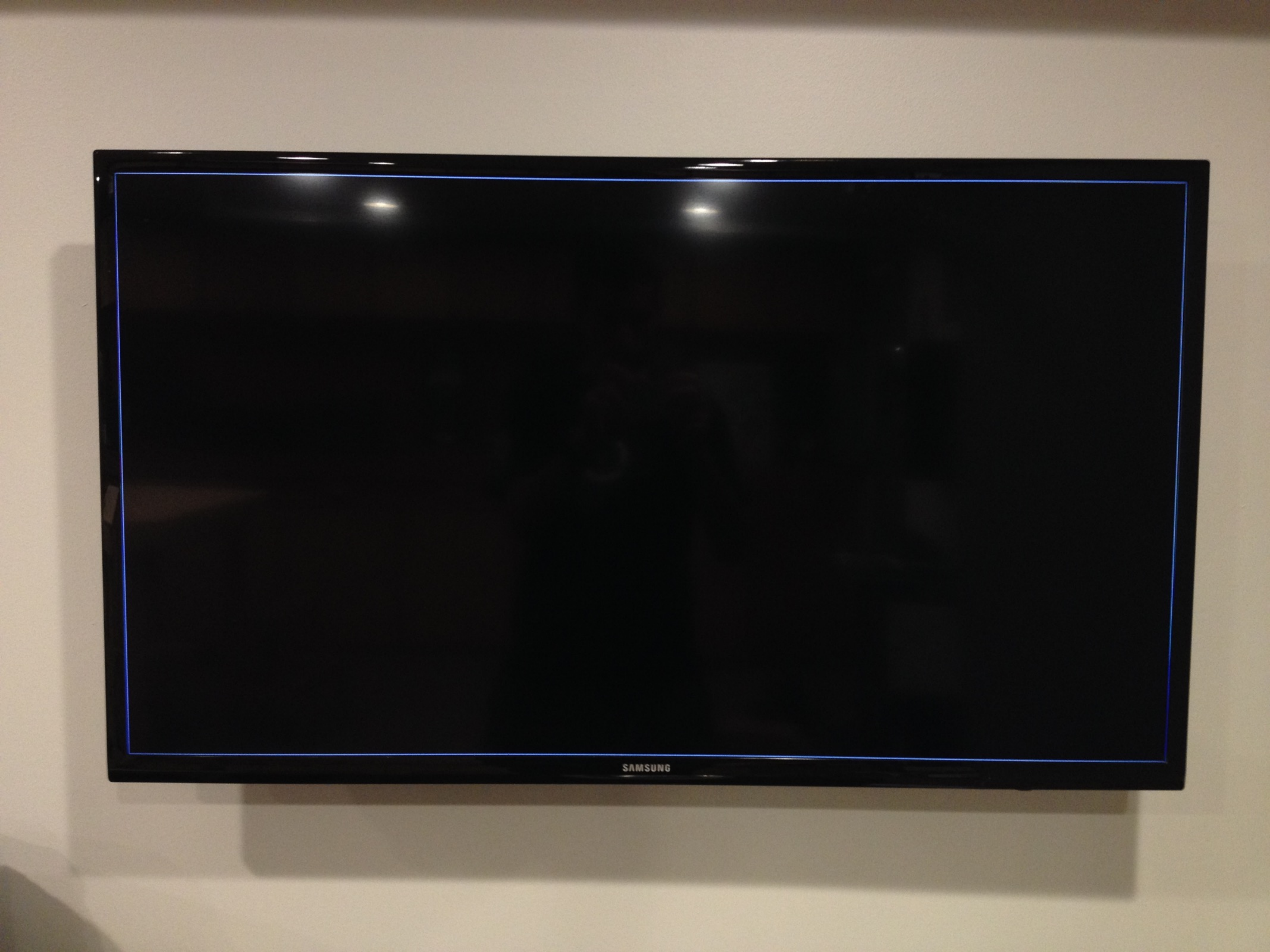
FPGA RTL View



Real World Demonstration

Gratuitous Display Modes

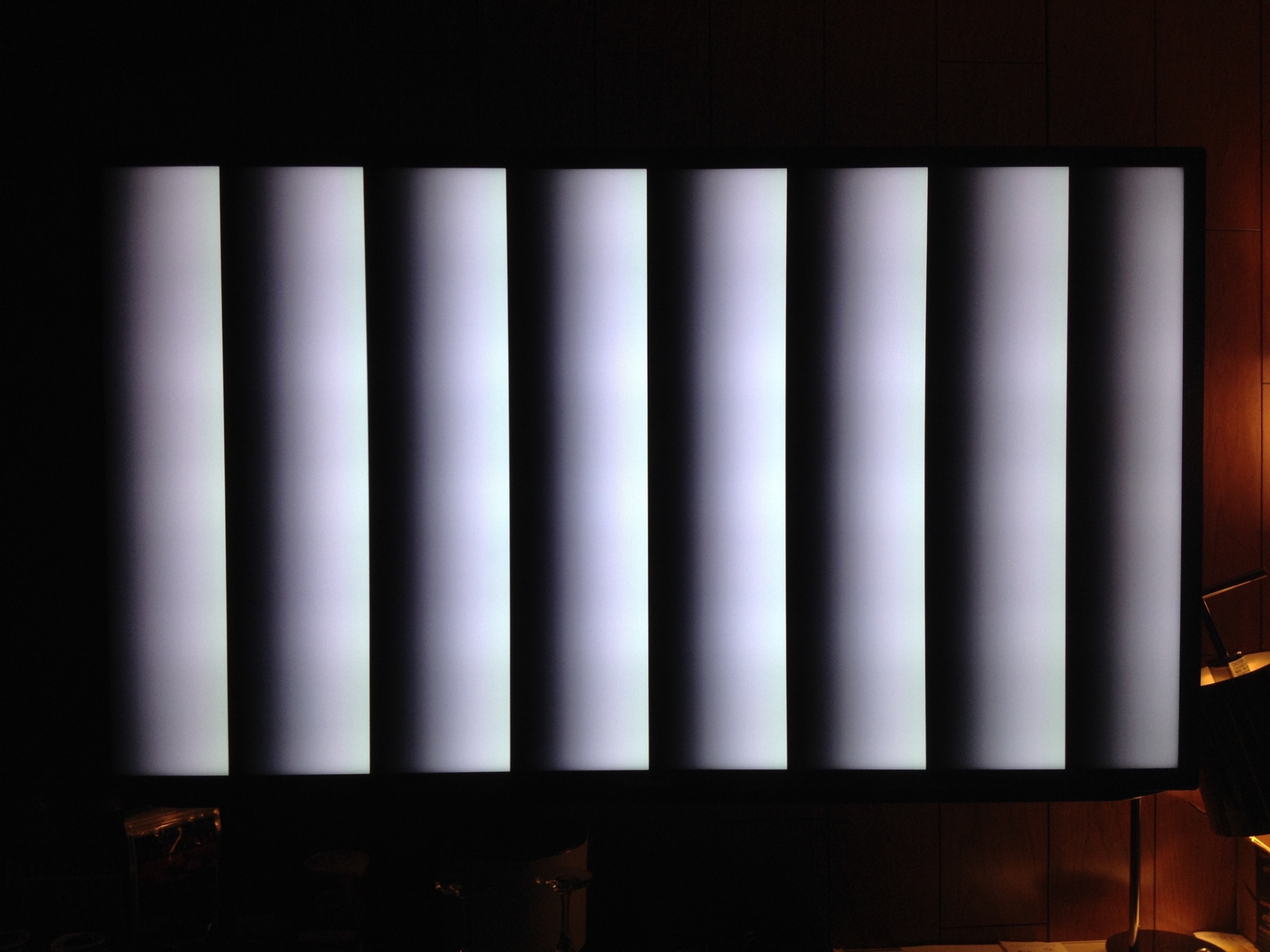
- Generated on-the-fly
- Mostly used for debugging purposes



SAMSUNG

SAMSUNG

SAMSUNG



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