Repurposing FPGA-based Products as Development Kits

Tom Verbeure
@tom_verbeure
Obsolete FPGA Products as Development Kit

Pros:

● Price!!!
● FPGA capacity
● Speciality components and features
● Satisfaction of hacking

Cons:

● Ugly hacks may be required
● Tedious reverse engineering
● Lack of generic GPIOs
● Little to no support online
Examples (1)

● **Pano Logic G1 and G2**
  ○ Obsolete FPGA-only thin clients
  ○ Huge FPGAs (Spartan 3E-1500 / Spartan 6 LX150)
  ○ All possible PC-like IOs: USB, VGA (G1) or DVI/HDMI (G2), Ethernet, DRAM, …
  ○ Easy accessible JTAG port
  ○ ~$20 on eBay
  ○ [https://github.com/tomverbeure/panologic](https://github.com/tomverbeure/panologic) and [https://github.com/tomverbeure/panologic-g2](https://github.com/tomverbeure/panologic-g2)

● **Colorlight 5A-75B**
  ○ Commercially available LED matrix controller (Not Obsolete!)
  ○ Large ECP5 FPGA - 25K Logic Elements
  ○ Fully supported by open source tools: Yosys, Nextpnr
  ○ 2x GigE, DRAM, lots of output pins
  ○ Easy accessible JTAG port
  ○ $15 on AliExpress
  ○ [https://github.com/q3k/chubby75](https://github.com/q3k/chubby75)
Examples (2)

- eeColor Color3
  - Obsolete HDMI color processor
  - 2x HDMI in, HDMI out
  - Cyclone IV EP4CE30
  - Easy accessible JTAG port
  - [https://github.com/tomverbeure/color3](https://github.com/tomverbeure/color3)
  - $20 on Amazon

- RV901T
  - Spartan 6 LX16 version of Colorlight 5A-75B
  - Requires some surgery for JTAG port
  - $18 on AliExpress
  - [https://github.com/q3k/chubby75](https://github.com/q3k/chubby75)
Examples (3)

- Comtech AHA363
  - PCIe Gzip accelerator
  - Large Intel Arria GX FPGA 90K Logic Elements
  - Easy accessible JTAG port
  - $20 on eBay
  - Reverse engineering
    - Work-in-Progress
    - Tough!
  - [https://github.com/tomverbeure/aha363](https://github.com/tomverbeure/aha363)
  - [https://tomverbeure.github.io/2020/06/14/AHA363-Reverse-Engineering.html](https://tomverbeure.github.io/2020/06/14/AHA363-Reverse-Engineering.html)
Examples (4)

- Cisco HWIC-3G-CDMA Modem
  - Obsolete Cisco WAN Card
  - Intel Cyclone II EP2C35
    - 35K Logic Elements
  - SDRAM, RS-232, Flash, ...
  - Easy access JTAG port
  - Lots of GPIOs!
  - $8 on eBay

See [FPGA Board Hack](https://hackaday.io/) on Hackaday.io for more candidates!
Reverse Engineering Process (1)

- **Gather Information**
  - Product datasheets
  - List of board components
  - Component datasheets
  - Schematic?
  - Other reverse engineering enthusiasts?

- **Get JTAG Up and Running**
  - Joint Test Action Group
    - Standard Interface for PCB Interconnecting Testing
    - Tests the joints of a PCB
  - Can daisy chain multiple chips with 4 wires
  - But also used to control chips internally
  - Essential to program FPGAs
Reverse Engineering Process (2)

- **Interconnection Discovery**
  - Ohm’ing out with multimeter
  - PCB component stripping and delayering
  - JTAG IO port capture and analysis
  - Claude’s Transmitting UART Technique

- **Blinking LED**
  - The hello world of FPGA board reverse engineering!

- **Bringing Up Peripherals**
  - Video (VGA, HDMI) is often easiest
  - Soft CPU Core
  - Ethernet
  - USB
  - ...
Reverse Engineering Process (3)

- Document Everything!
Gathering Information
JTAG Connector

AHA363

Pano Logic G1

5A-75B

Pano Logic G2

3.3V Connection

RV901T

3.3V Plane
JTAG Bringup

- OpenOCD is pretty decent at discovering the JTAG configuration...
- Info: JTAG tap: auto0.tap tap/device found: 0x41111043 (mfg: 0x021 (Lattice Semi.), part: 0x111, ver: 0x4
- Warn: AUTO auto0.tap - use "jtag newtap auto0 tap -irlen 2 -expected-id 0x41111043"
- ... but commercial tools are usually easier
Interconnection Discovery - Ohm’ing Out

- For each pin on one chip, try all pins on the other until there’s a beep…
  - As tedious as it sounds!
  - Often the only option
  - Doesn’t work for connections with resistors >50Ohm or capacitors in series
Interconnection Discovery - Delayering

- Remove all components
- Sand away layer by layer
- Merge layers on top of each other
Interconnection Discovery - JTAG IO Pad Capture

- **JTAG Boundary Chain**
  - Capture and/or control the IO pads of FPGA into a scan chain (~shift register)

- **BSDL File**
  - Boundary Scan Description Language
  - Describes all the IO pads of the FPGA in the chain

- **Multiple captures in live system expose important information**
  - Toggle rate
  - Direction of the pin

- **Capture traces with OpenOCD**

- **Analyze with script that merges trace with BSDL file**
  - [https://github.com/tomverbeure/bscan_tools](https://github.com/tomverbeure/bscan_tools)
Interconnection Discovery - JTAG IO Pad Capture

- Trace

1. 0049068029249F41249240001E000492492492781C8A1B4DB6C9000FE924024FE28049241248209378206DB1:
2. 0049168029249F41249240001E000492492492781C8A1B4D36C9000FE924024FE280492412483493FD205F69:
3. 0049068009249F41249240001E000492492492781C8A1B49B6C9000FE924024FE2804926924F2093F8205F69:
4. 0049168029249F41249240001E000492492492781C8A1B4DB6C9000FE924024FE2804926924D3493F822DF69:

- Post-Processed

589  Y9  (IOY9)  : INPUT  : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
590  Y9  (IOY9)  : OUTPUT3 : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
591  Y9  (IOY9)  : CONTROL : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
592  
593  M17  (MSEL0) : INPUT  : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
594  
595  N17  (MSEL1) : INPUT  : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
596  
597  L2  (clk25) : INPUT  : 1 0 1 1 1 1 0 0 0 0 0 0 1 0 1 0 !
598  
599  A4  (clk_to_sdram[0]) : INPUT  : 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
600  A4  (clk_to_sdram[0]) : OUTPUT3 : 1 0 0 1 1 1 0 1 1 0 1 0 0 1 0 1 0 !
601  A4  (clk_to_sdram[0]) : CONTROL : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Claude’s Transmitting UART Technique

- Create a bitstream with 1 UART TX per IO pad
- Have each UART constantly transmit a unique number
- Use oscilloscope or logic analyzer with UART decode functionality
- Probe points of interest on the PCB
- Oscilloscope will immediately show which points of interest are driven by which FPGA pin
- Might damage FPGA if an FPGA input is used as output!!!
  - JTAG IO boundary scan can first identify FPGA pins that are configured as output
- @Claude1079
Blinking LED - Hello World!

- https://vimeo.com/372548312
Work Around Board Limitations (1)

- 5A-75B: Replace unidirectional level shifters by wires
  - https://github.com/cyber-murmel
Work Around Board Limitations (2)

- Cisco Modem GPIO Expansion Board
  - Plugs into the Cisco HWIC connector
  - Converts to regular 0.1” pin header format
  - Also has support to configure the bitstream (WIP)
Cisco Modem Powered LED Cube
eeColor Color3 - HDMI RX, Overlay, HDMI TX
Pano Logic G1 - Racing the Beam Ray Tracer

Real-time ray tracing without frame buffer on small Spartan-3E 1600 FPGA.

Code at github.com/tomverbeure/rt
Contact

- My blog: https://tomverbeure.github.io
- My github: https://github.com/tomverbeure
- I love talking about this stuff! DM me on Twitter if you’re interested!
  - @tom_verbeure