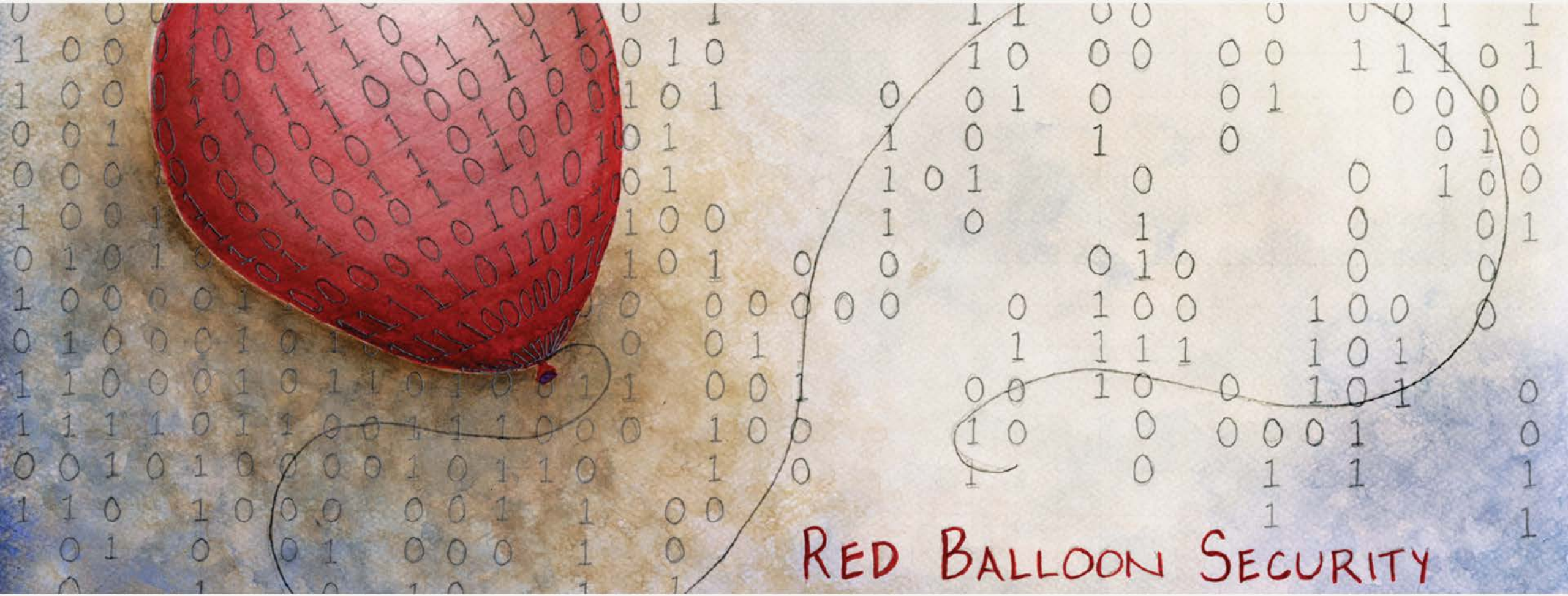


Defeating Cisco Trust Anchor: A Case-Study of Recent Advancements in Direct FPGA Bitstream Manipulation

Jatin Kataria
Ang Cui, PhD
{A|J}@redballoonsecurity.com

OBJECTIVE

- Modify Firmware On 1001-X

THRANGRYCAT.COM

Cisco Secure Boot Hardware Tampering Vulnerability

Advisory ID:	cisco-sa-20190513-secureboot	CVE-2019-1649	Download CVRF
First Published:	2019 May 13 17:30 GMT	CWE-284	Download PDF
Last Updated:	2019 May 30 19:55 GMT		Email
Version 1.8:	Interim		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvn77141		
	CSCvn77142		
	CSCvn77143		
	More...		
CVSS Score:	Base 6.7		

😾😾😾 Impact

- Cisco ASR 1000 Embedded Services Processor
- Cisco ASR 1000 Fixed Ethernet Line Card (6x10GE) (ASR1000-6TGE)
- Cisco ASR 1000 Fixed Ethernet Line Card
- Cisco ASR 1000 Series 100-Gbps Embedded Services Processor (ASR 1000-ESP100)
- Cisco ASR 1000 Series Modular Interface Processor (ASR1000-MIP100)
- Cisco ASR 1000 Series Route Processor 3 (Cisco ASR1000-RP3)
- Cisco ASR 1001-HX Router
- Cisco ASR 1001-X

Impact

- Cisco ASR 900 Series Route Switch Processor 2 - 128G
- Cisco ASR 900 Series Route Switch Processor 2 - 64G
- Cisco ASR 900 Series Route Switch Processor 3 - 200G
- Cisco ASR 900 Series Route Switch Processor and Controller 400G (A900-RSP3C-400/W)
- Cisco ASR 9000 Series 16-Port 100 Gigabit Ethernet Line Card (A99-16X100GE-X-SE)
- Cisco ASR 9000 Series 16-Port 100 Gigabit Ethernet Line Card (A9K-16X100GE-TR
- Cisco ASR 9000 Series 32-Port 100 Gigabit Ethernet Line Card (A99-32X100GE-TR
- Cisco ASR 9000 Series Route Switch Processor 5 for Packet Transport (A9K-RSP5-TR)
- Cisco ASR 9000 Series Route Switch Processor 5 for Service Edge (A9K-RSP5-SE)
- Cisco ASR 920 Series Aggregation Services Routers 10GE and 2-10GE - Passively Cooled DC model (ASR-920-10SZ-PD)
- Cisco ASR 920 Series Aggregation Services Routers 12 x 1/10GE SFP
- Cisco ASR 920 Series Aggregation Services Routers 12 x 1/10GE SFP
- Cisco ASR 920 Series Aggregation Services Routers 12GE and 2-10GE - AC model (ASR-920-12CZ-A)

Impact

- Cisco ASR 920 Series Aggregation Services Routers 12GE and 2-10GE - DC model (ASR-920-12CZ-D)
- Cisco ASR 920 Series Aggregation Services Routers 24GE Copper and 4-10GE – Modular PSU (ASR-920-24TZ-IM)
- Cisco ASR 920 Series Aggregation Services Routers 24GE Copper and 4-10GE – Modular PSU (ASR-920-24TZ-M)
- Cisco ASR 920 Series Aggregation Services Routers 24GE Fiber and 4-10GE – Modular PSU (ASR-920-24SZ-M)
- Cisco ASR 920 Series Aggregation Services Routers 2GE and 4-10GE - AC model (ASR-920-4SZ-A)
- Cisco ASR 920 Series Aggregation Services Routers 2GE and 4-10GE - DC model (ASR-920-4SZ-D)
- Cisco ASR 920 Series Aggregation Services Routers Conformal Coated - 12GE and 4-10GE
- Cisco ASR 9900 Route Processor 3 for Packet Transport (A99-RP3-TR)
- Cisco ASR 9900 Route Processor 3 for Service Edge (A99-RP3-SE)
- Cisco Catalyst 6800 16-port 10GE with Integrated DFC4-XL (C6800-16P10G-XL)
- Cisco Catalyst 6800 32-port 10GE with Dual Integrated Dual DFC4-XL (C6800-32P10G-XL)

Impact

- Cisco Catalyst 6800 8-port 10GE with Integrated DFC4-XL (C6800-8P10G-XL)
- Cisco Catalyst 6800 8-port 40GE with Dual Integrated Dual DFC4-EXL (C6800-8P40G-XL)
- Cisco Catalyst 6800 Series Supervisor Engine 6T XL
- Cisco Catalyst 6816-X-Chassis (Standard Tables) (C6816-X-LE)
- Cisco Catalyst 6824-X-Chassis and 2 x 40G (Standard Tables) (C6824-X-LE-40G)
- Cisco Catalyst 6832-X-Chassis (Standard Tables) (C6832-X-LE)
- Cisco Catalyst 6840-X-Chassis and 2 x 40G (Standard Tables) (C6840-X-LE-40G)
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9500 Series High-Performance Switch with 24x 1/10/25G Gigabit Ethernet + 4x 40/100G Uplink (C9500-24Y4C)
- Cisco Catalyst 9500 Series High-Performance Switch with 32x 100 Gigabit Ethernet (C9500-32C)
- Cisco Catalyst 9500 Series High-Performance Switch with 32x 40 Gigabit Ethernet (C9500-32QC)
- Cisco Catalyst 9500 Series High-Performance Switch with 48x 1/10/25G Gigabit Ethernet + 4x 40/100G Uplink (C9500-48Y4C)

Impact

- Cisco Catalyst 9500 Series Switch with 12x 40G Gigabit Ethernet (C9500-12Q)
- Cisco Catalyst 9500 Series Switch with 16x 1/10G Gigabit Ethernet (C9500-16X)
- Cisco Catalyst 9500 Series Switch with 24x 40G Gigabit Ethernet (C9500-24Q)
- Cisco Catalyst 9500 Series Switch with 40x 1/10G Gigabit Ethernet (C9500-40X)
- Cisco Catalyst 9600 Supervisor Engine-1
- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco IC3000 Industrial Compute Gateway
- Cisco MDS 9000 Family 24/10 SAN Extension Module (DS-X9334-K9)
- Cisco NCS 200 Series 10/40/100G MR Muxponder (NCS2K-MR-MXP-K9)
- Cisco NCS 5500 Series 24 Ports of 100GE and 12 Ports of 40GE High-Scale Line Card (NC55-24H12F-SE)
- Cisco NCS 5500 Series 36 ports of 100GE High-Scale Line Card (NC55-36X100G-A-SE)
- Cisco NCS 5504 Fabric Card (NC55-5504-FC)
- Cisco NCS 5516 Fabric Card (NC55-5516-FC)

Impact

- Cisco NCS 55A2 Fixed 24X10G + 16X25G MPA Chassis (NCS-55A2-MOD-S)
- Cisco NCS 55A2 Fixed 24X10G + 16X25G MPA Chassis
- Cisco NCS 55A2 Fixed 24X10G + 16X25G MPA Chassis
- Cisco NCS 55A2 Fixed 24X10G + 16X25G MPA Scale Chassis (NCS-55A2-MOD-SE-S)
- Cisco NCS 55A2 Fixed 24X10G + 16X25G MPA Scale Chassis
- Cisco NCS5501 - 40x10G and 4x100G Scale Chassis (NCS-5501-SE)
- Cisco NCS5501 Fixed 48x10G and 6x100G Chassis (NCS-5501)
- Cisco NCS5502 - 48x100G Scale Chassis (NCS-5502-SE)
- Cisco NCS5502 Fixed 48x100G Chassis (NCS-5502)
- Cisco NCS55A1 Fixed 24x100G Chassis (NCS-55A1-24H)
- Cisco NCS55A1 Fixed 36x100G Base Chassis (NCS-55A1-36H-S)
- Cisco NCS55A1 Fixed 36x100G Scale Chassis (NCS-55A1-36H-SE)
- Cisco Network Convergence System 1002
- Cisco Network Convergence System 5001
- Cisco Network Convergence System 5002
- Cisco NCS 5500 12X10
- Cisco Network Convergence System 5500 Series: 1.2-Tbps IPoDWDM Modular Line Card (NC55-6X200-DWDM-S)

Impact

- Cisco Network Convergence System 5500 Series: 36X100G MACsec Modular Line Cards (NC55-36X100G-S)
- Cisco Nexus 31108PC-V
- Cisco Nexus 31108TC-V
- Cisco Nexus 3132C-Z Switches (N3K-C3132C-Z)
- Cisco Nexus 3264C-E Switches (N3K-C3264C-E)
- Cisco Nexus 7000 M3-Series 48-Port 1/10G Ethernet Module (N7K-M348XP-25L)
- Cisco Nexus 7700 M3-Series 12-Port 100G Ethernet Module (N77-M312CQ-26L)
- Cisco Nexus 7700 M3-Series 24-Port 40G Ethernet Module (N7K-M324FQ-25L)
- Cisco Nexus 7700 M3-Series 48-Port 1/10G Ethernet Module (N77-M348XP-23L)
- Cisco Nexus 7700 Supervisor 3 (N77-SUP3E)
- Cisco Nexus 9332C ACI Spine Switch with 32p 40/100G QSFP28
- Cisco Nexus 9364C ACI Spine Switch with 64p 40/100G QSFP28
- Cisco Nexus 9500 4-Core/4-Thread Supervisor (N9K-SUP-A)
- Cisco Nexus 9500 6-Core/12-Thread Supervisor (N9K-SUP-B)

Impact

- Nexus 9200 with 48p 1/10G/25G SFP+ and 6p 40G QSFP or 4p 100G QSFP28 (N9K-C92160YC-X)
- Nexus 9200 with 48p 10/25 Gbps and 18p 100G QSFP28 (N9K-C92300YC)
- Nexus 9200 with 48p 100M/1GT
- Nexus 9200 with 56p 40G QSFP+ and 8p 100G QSFP28 (N9K-C9230AQC)
- Nexus 9200 with 72p 40G QSFP+ (N9K-C9272Q)
- Nexus 9300 with 48p 1/10G/25G SFP and 6p 40G/100G QSFP28
- Nexus 9300 with 48p 100M/1G BASE-T
- Nexus 9300 with 48p 10G BASE-T and 6p 40G/100G QSFP28
- Nexus 9K Fixed with 32p 100G QSFP28 (N9K-C9232C)
- Nexus 9K Fixed with 48p 1/10G/25G SFP and 12p 40G/100G QSFP28 (N9K-C93240YC-FX2)
- Nexus 9K Fixed with 48p 1/10G/25G SFP and 6p 40G/100G QSFP28 (N9K-C93180YC-EX)
- Nexus 9K Fixed with 48p 10G BASE-T and 6p 40G/100G QSFP28 (N9K-C93108TC-EX)
- Nexus 9K Fixed with up to 32p 40/50G QSFP+ or up to 18p 100G QSFP28 (N9K-C93180LC-EX)

Impact

- Cisco 1-Port Gigabit Ethernet WAN Network Interface Module (NIM-1GE-CU-SFP)
- Cisco 1120 Connected Grid Router
- Cisco 1240 Connected Grid Router
- Cisco 2-Port Gigabit Ethernet WAN Network Interface Module (NIM-2GE-CU-SFP)
- Cisco 3000 Series Industrial Security Appliances
- Cisco 4000 Series Integrated Services Router Packet 1024-Channel High-Density Voice DSP Module (SM-X-PVDM-1000)
- Cisco 4000 Series Integrated Services Router Packet 2048-Channel High-Density Voice DSP Module (SM-X-PVDM-2000)
- Cisco 4000 Series Integrated Services Router Packet 3080-Channel High-Density Voice DSP Module (SM-X-PVDM-3000)
- Cisco 4000 Series Integrated Services Router Packet 768-Channel High-Density Voice DSP Module (SM-X-PVDM-500)
- Cisco 4221 Integrated Services Router
- Cisco 4321 Integrated Services Router

Impact

- Cisco ASA 5506-X with FirePOWER Services
- Cisco ASA 5506H-X with FirePOWER Services
- Cisco ASA 5506W-X with FirePOWER Services
- Cisco ASA 5508-X with FirePOWER Services
- Cisco ASA 5516-X with FirePOWER Services
- Cisco Firepower 2100 Series
- Cisco Firepower 4000 Series
- Cisco Firepower 9000 Series
- 10Gbps Optical Encryption Line Card for the Cisco NCS 2000 Series and Cisco ONS 15454 MSTP (15454-M-WSE-K9)
- CBR-8 Converged Broadband Router
- Cisco 5000 Series Enterprise Network Compute System
- Cisco 809 Industrial Integrated Services Routers
- Cisco 829 Industrial Integrated Services Routers
- Supervisor A+ for Nexus 9500 (N9K-SUP-A+)

Impact

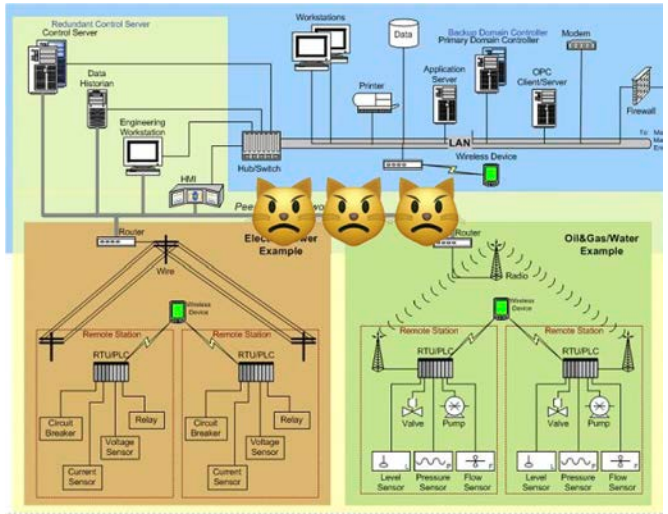
- Cisco Packet-over-T3/E3 Service Module (SM-X-1T3/E3)
- Cisco cBR-8 Integrated CCAP 40G Remote PHY Line Card (CBR-CCAP-LC-40G-R)
- Cisco cBR-8 Integrated CCAP Line Card includes 2 DS D3.1 Modules as well as 1 US D3.1 Module (CBR-LC-8D31-16U31)
- MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9)
- Nexus 9200 with 36p 40G 100G QSFP28 (N9K-C9236C)
- Supervisor B+ for Nexus 9500 (N9K-SUP-B+)
- Cisco 4331 Integrated Services Router
- Cisco 4351 Integrated Services Router
- Cisco 4431 Integrated Services Router
- Cisco 4451-X Integrated Services Router
- Cisco 4461 Integrated Services Router
- Analog Voice Network Interface Modules for Cisco 4000 Series ISRs (NIM-2FXO, NIM-4FXO, NIM-2FXS, NIM-4FXS, NIM-2FXS/4FXO, NIM-2FXSP, NIM-4FXSP, NIM-2FXS/4FXOP, NIM-4E/M, NIM-2BRI-NT/TE, NIM-4BRI-NT/TE)
- Cisco 4000 Series Integrated Services Router T1/E1 Voice and WAN Network Interface Modules (NIM-1MFT-T1/E1, NIM-2MFT-T1/E1, NIM-4MFT-T1/E1, NIM-8MFT-T1/E1, NIM-1CE1T1-PRI, NIM-2CE1T1-PRI, NIM-8CE1T1-PRI)

😾😾😾 Impact

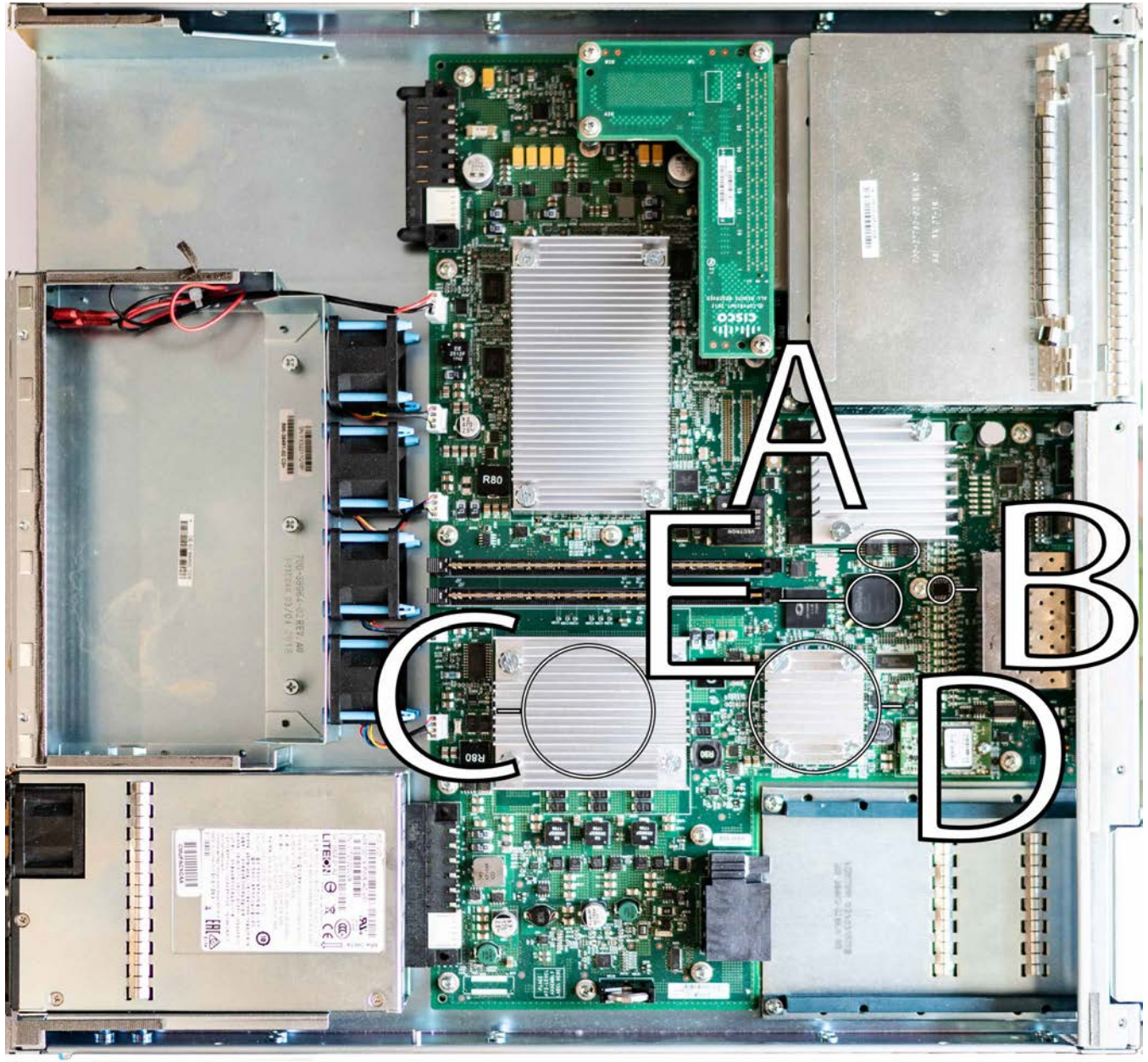
- Cisco ASA 5506-X
- Cisco ASA 5506H-X
- Cisco ASA 5506W-X
- Cisco ASA 5508-X
- Cisco ASA 5516-X
- Cisco Firepower 2100 Series
- Cisco Firepower 4000 Series
- Cisco Firepower 9000 Series

😾😾😾 Impact


MOVIECLIPS.com


Redundant Control Server
Control Server
Workstations
Data
Backup Domain Controller
Primary Domain Controller
Modem
Data Historian
Printer
Application Server
OPC Client/Server
Firewall
Engineering Workstation
LAN
Hub/Switch
Wireless Device
HMI
Router
Wire
Radio
Oil&Gas/Water Example
Remote Station
RTU/PLC
Circuit Breaker
Relay
Voltage Sensor
Current Sensor
Valve
Pump
Level Sensor
Pressure Sensor
Flow Sensor

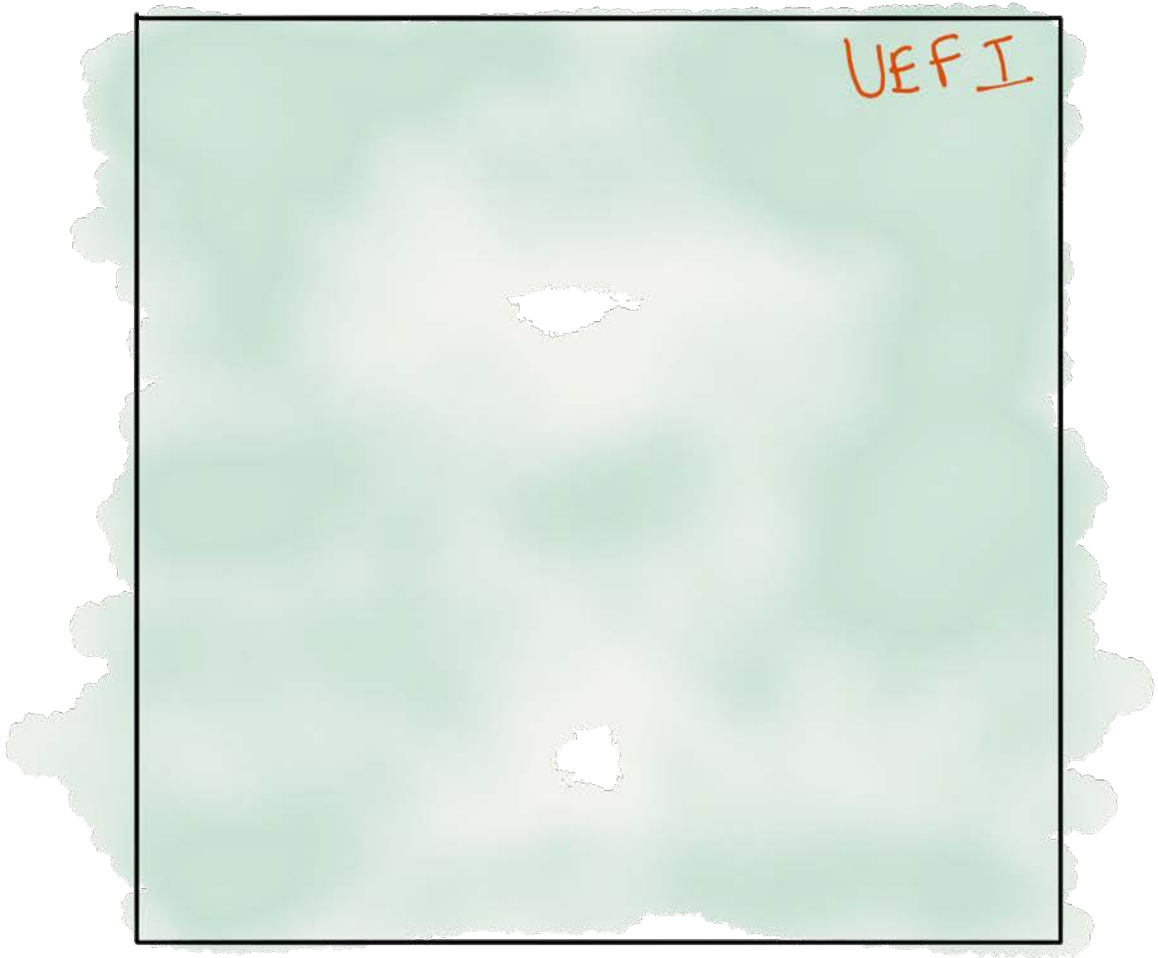
Hw Analysis



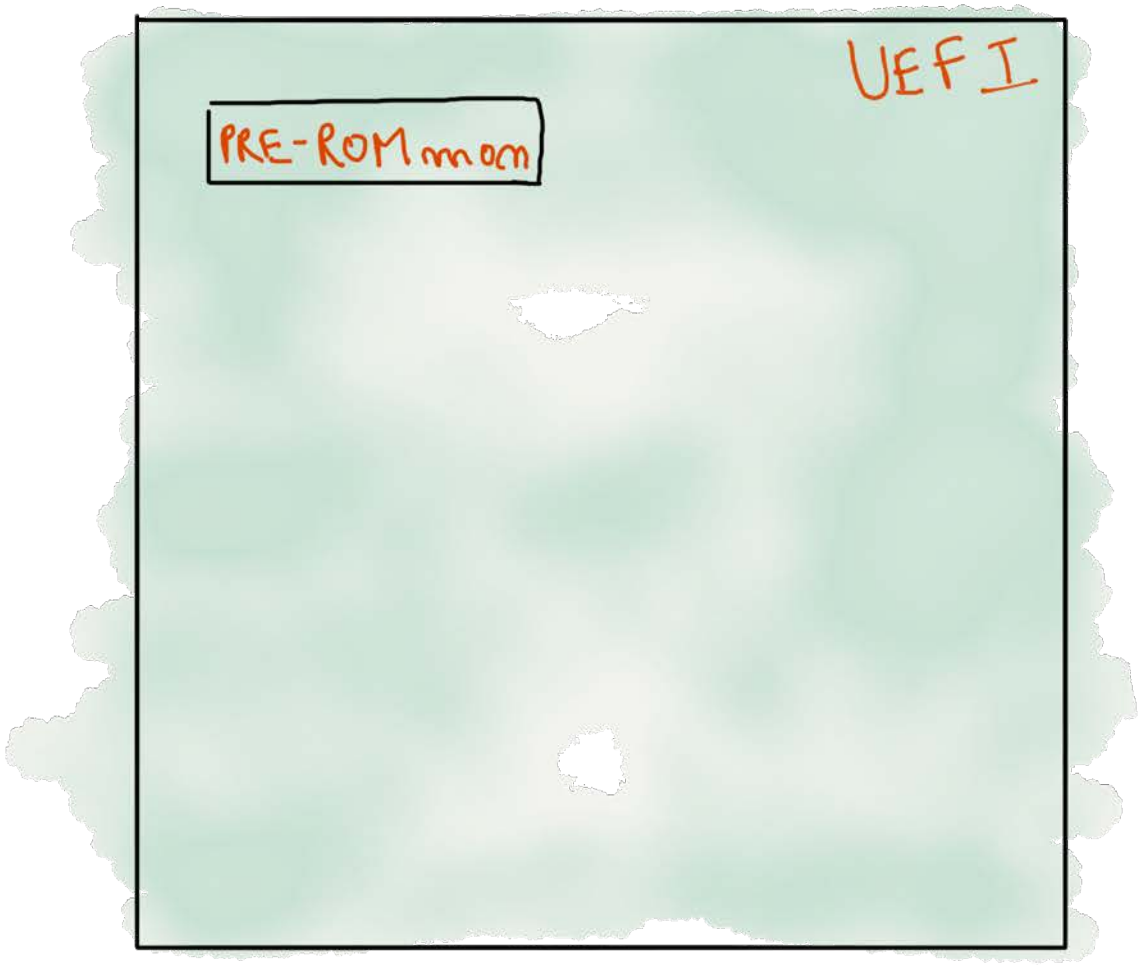
A) Bootloader Flash **B)** FPGA Bitstream SPI Flash **C)** Intel Xeon (Route Processor)

D) Intel Comunications Processor **E)** FPGA (Trust Anchor, other services)

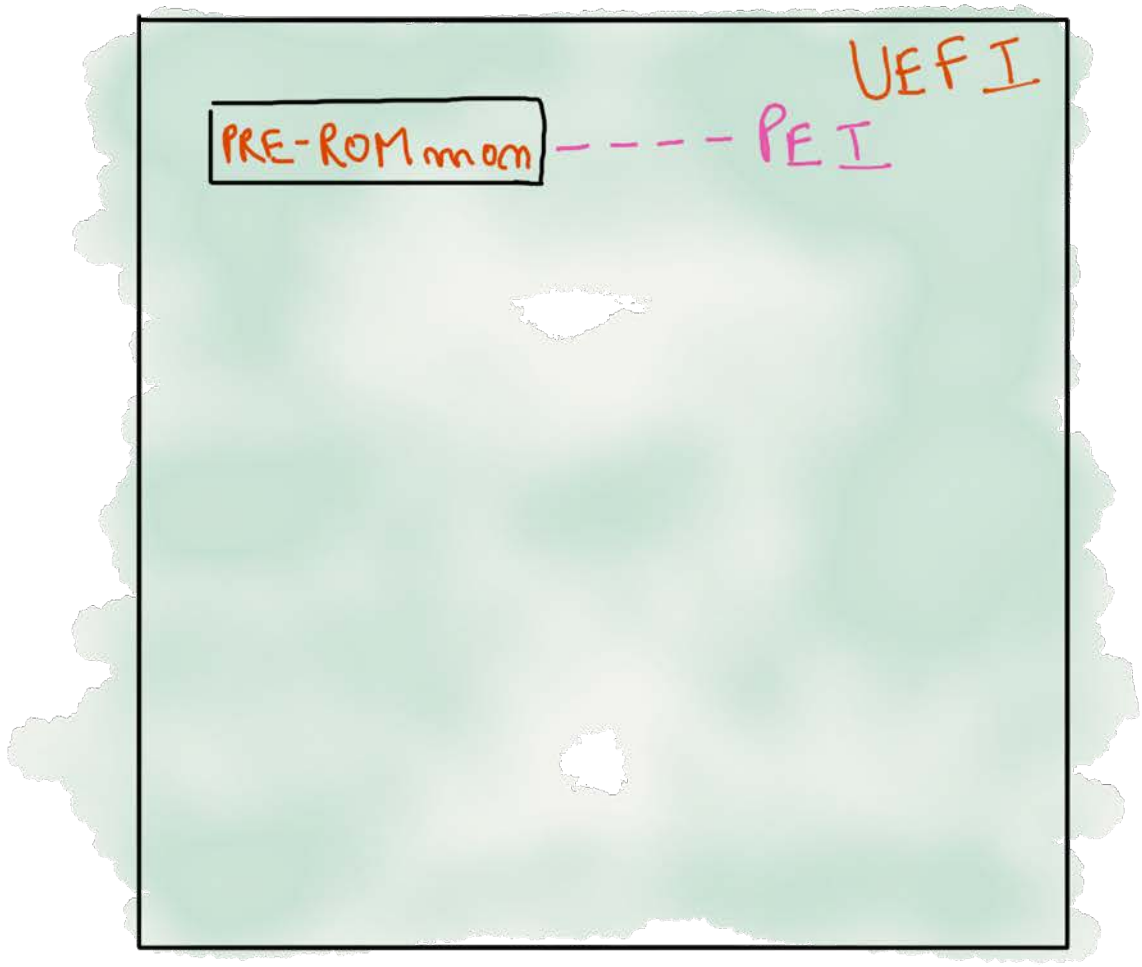
ASR 1001-X
SOFTWARE ANALYSIS



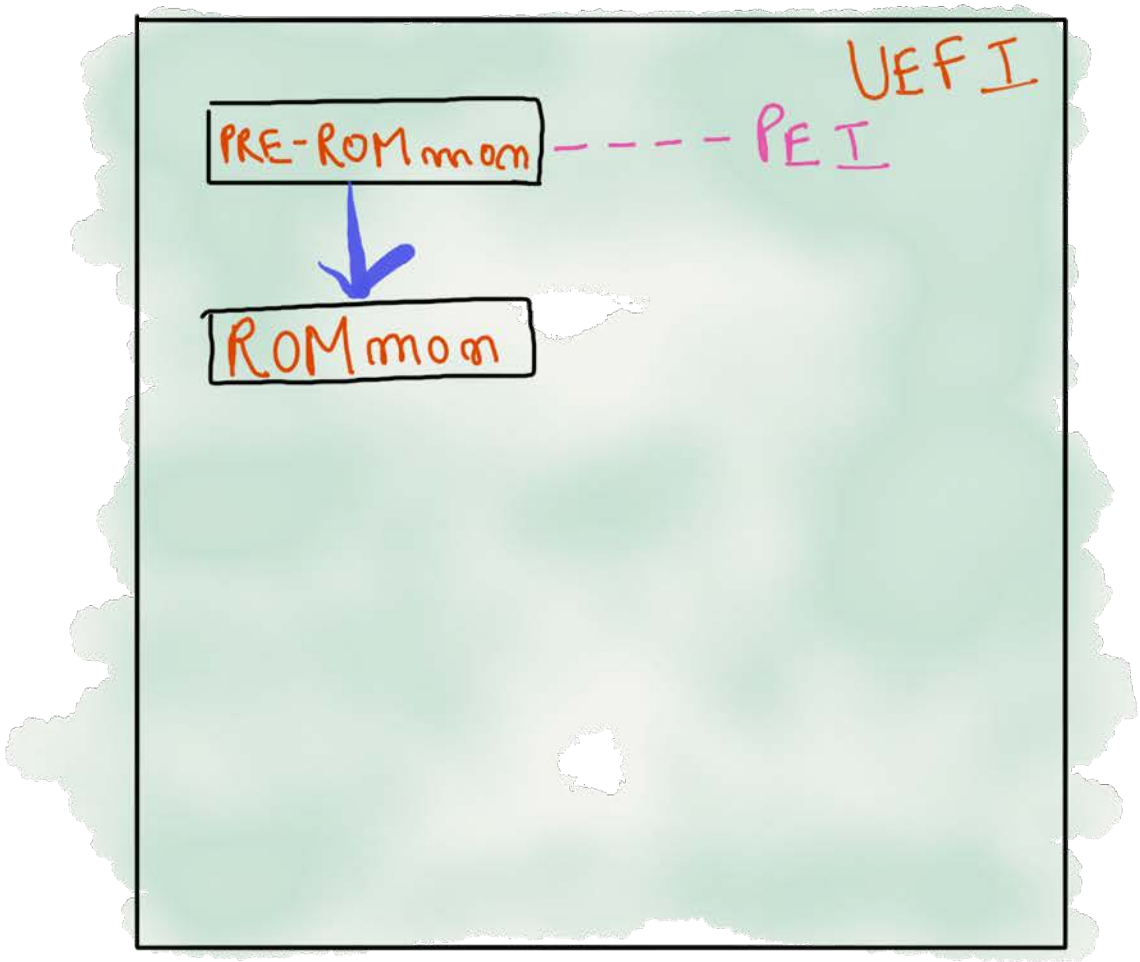
ASR 1001-X SOFTWARE ANALYSIS



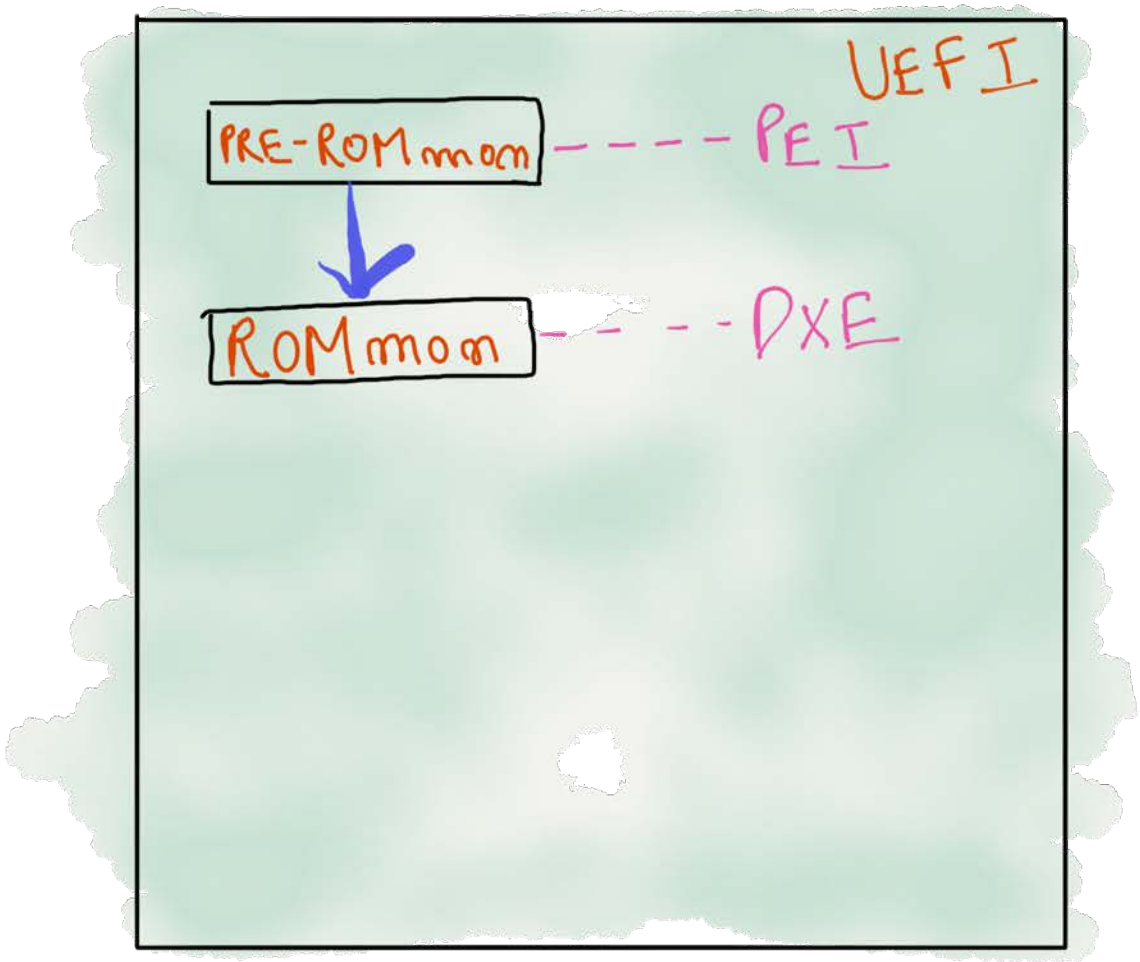
ASR 1001-X
SOFTWARE ANALYSIS



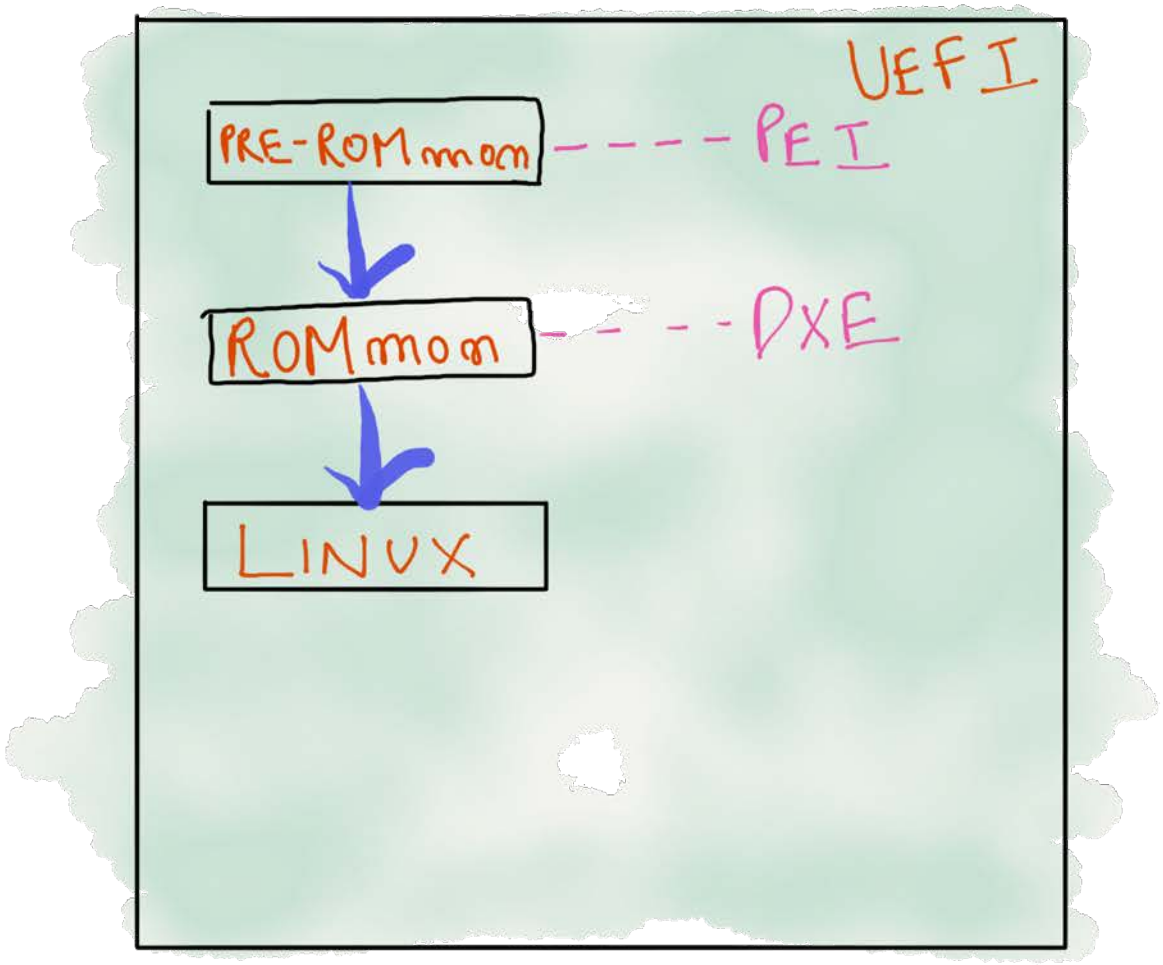
ASR 1001-X
SOFTWARE ANALYSIS



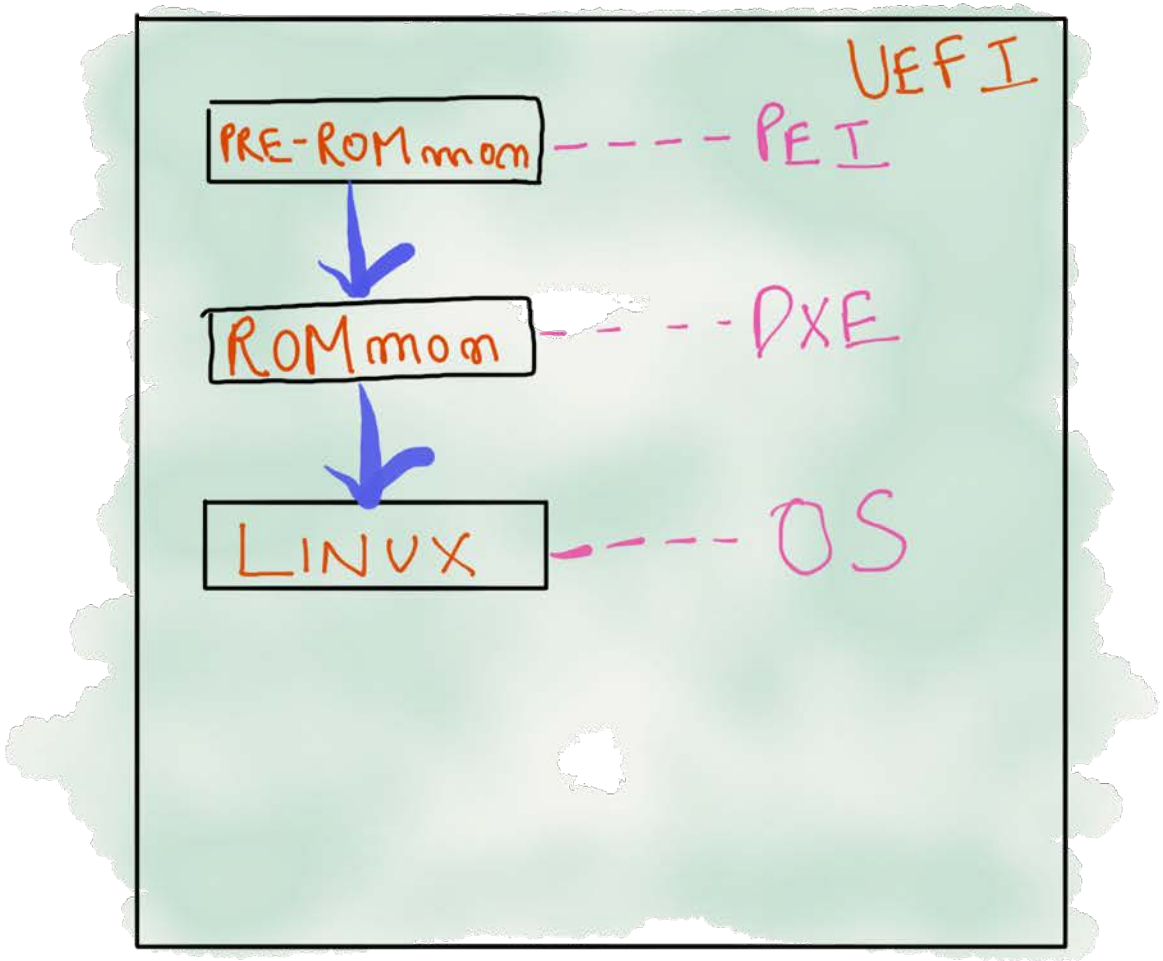
ASR 1001-X
SOFTWARE ANALYSIS



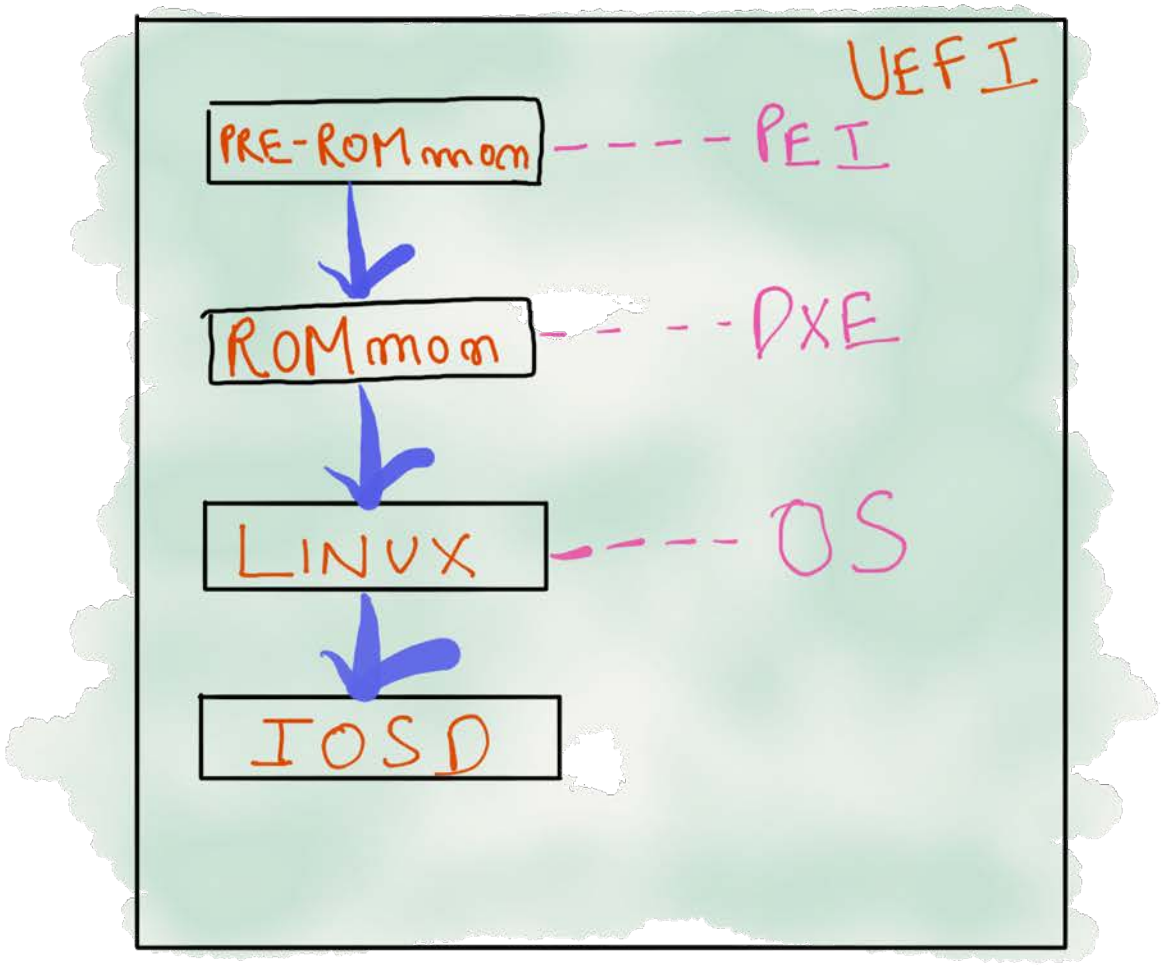
ASR 1001-X
SOFTWARE ANALYSIS



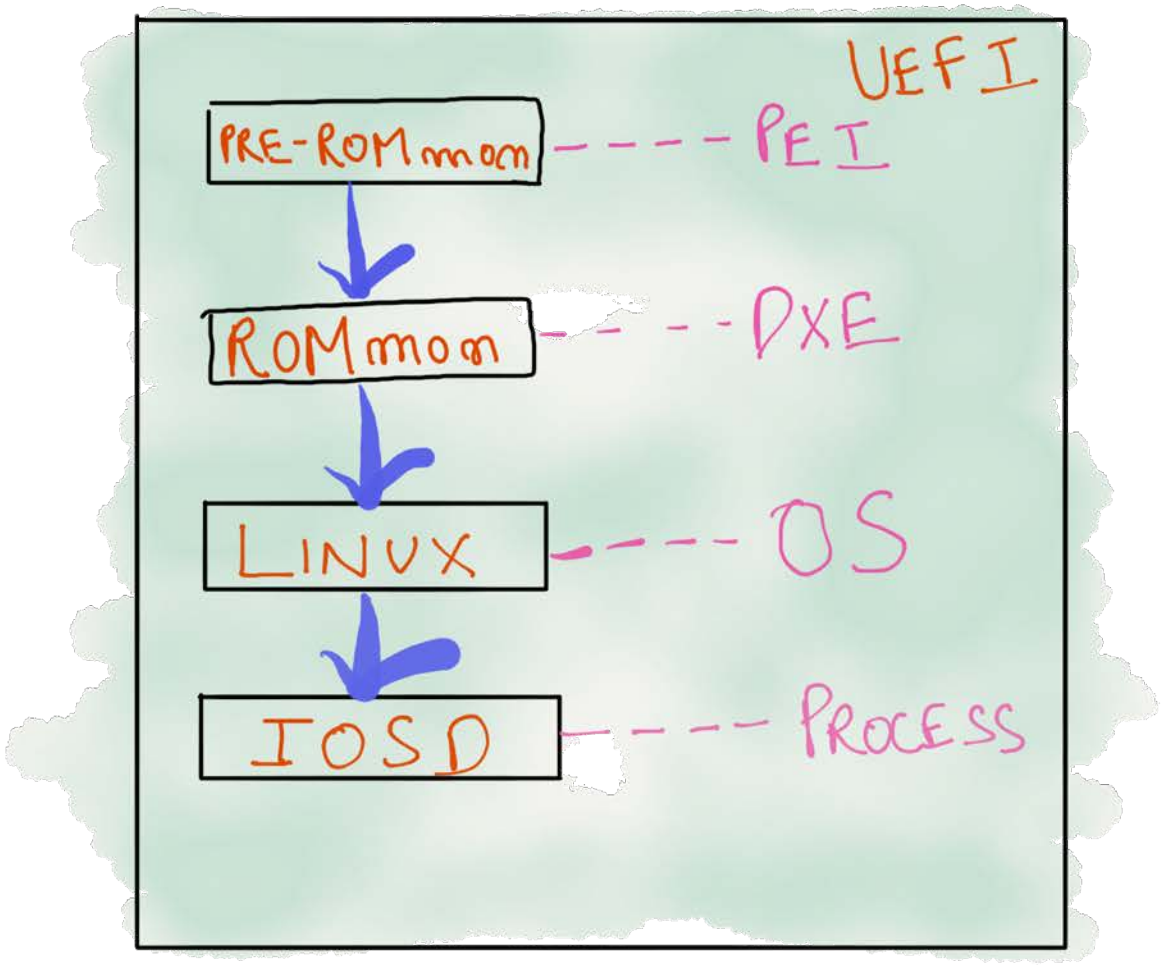
ASR 1001-X
SOFTWARE ANALYSIS



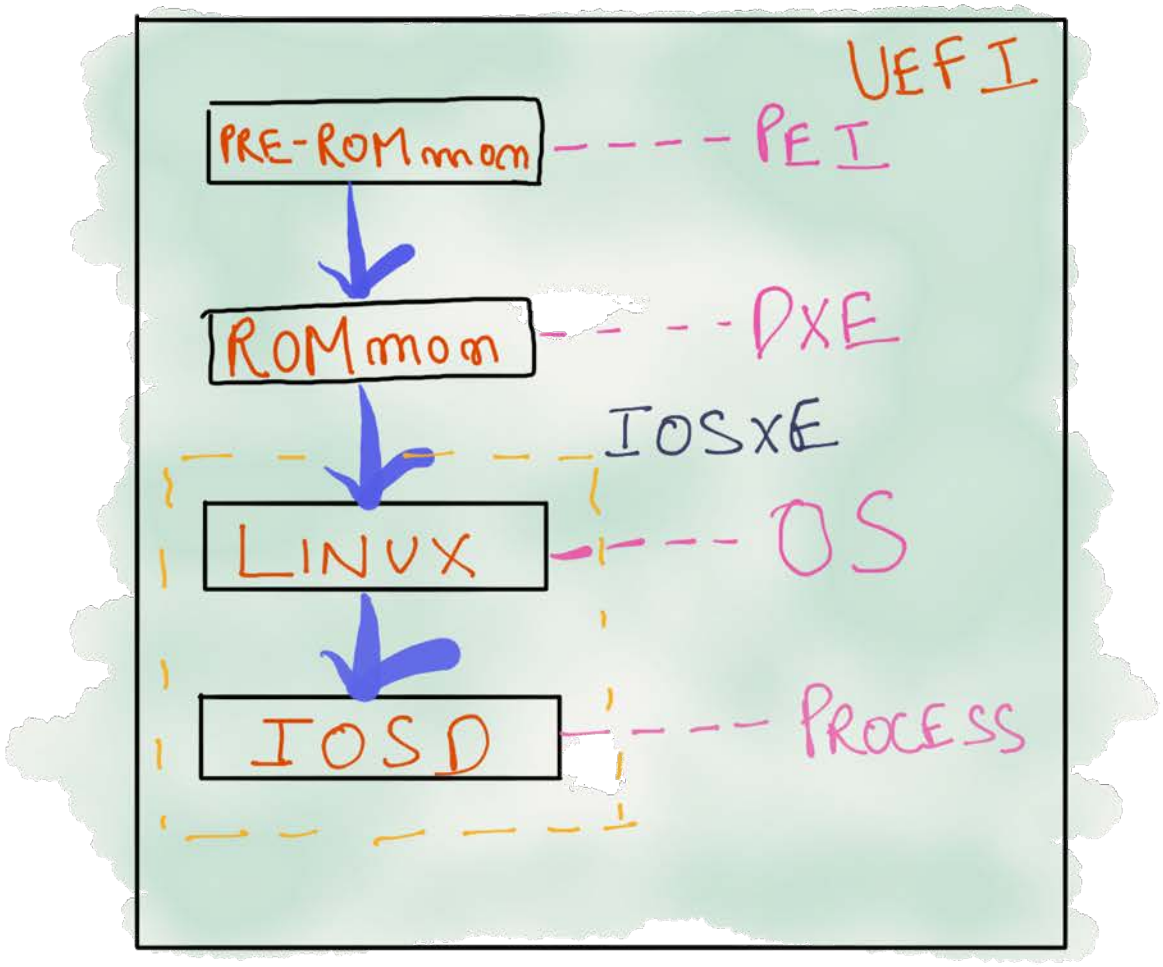
ASR 1001-X
SOFTWARE ANALYSIS



ASR 1001-X
SOFTWARE ANALYSIS



ASR 1001-X
SOFTWARE ANALYSIS



ASR 1001-X
SOFTWARE ANALYSIS

- NO Hash

ASR 1001-X
SOFTWARE ANALYSIS

- NO Hash
- NO Certs

ASR 1001-X
SOFTWARE ANALYSIS

- NO Hash
- NO Certs
- Easy Mod for UEFI

Easy MOD

- Disable PreROMMon check & Boot mod fw

Easy MOD

- Disable PreROMMon check & Boot mod fw
- Everything works! But wait...
  Meow!!

Easy MOD

- Disable PreROMMon check & Boot mod fw
- Everything works! But wait...
  Meow!
- RESET!!

💯 Seconds of Solitude

- Route Processor Resets in 💯 seconds

```
Current image running: Boot ROM0
Last reset cause: PowerOn

ASR1001-X platform with 8388608 Kbytes of main memory

Rommon upgrade requested
Maximum upgrade attempts exceeded, continuing with old Rommon...
rommon 1 >
```

Hypotheses for 💯

- X86 Mitigations

Hypotheses for 💯

- X86 Mitigations
  - VMM is disabled

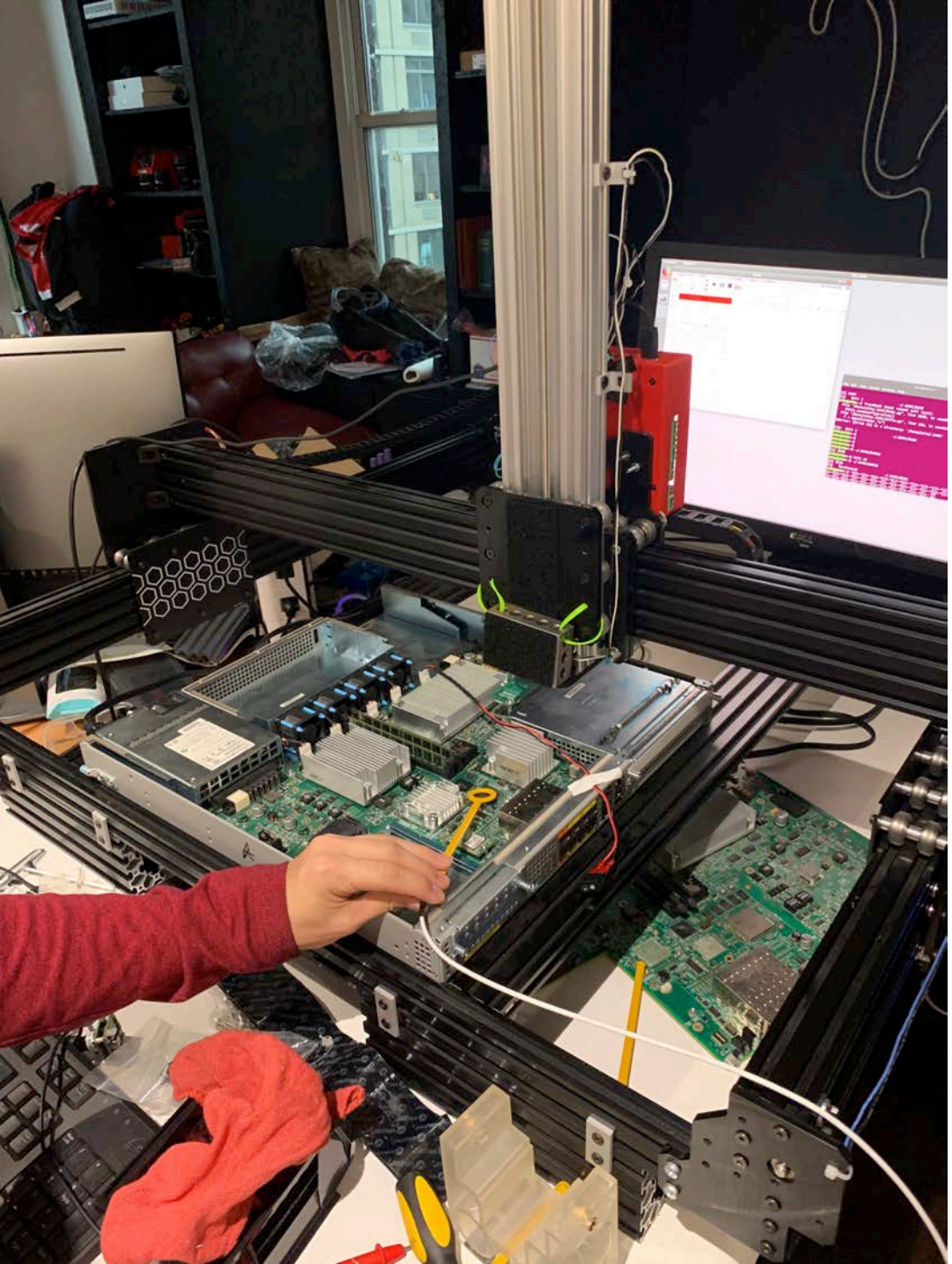
Hypotheses for 💯

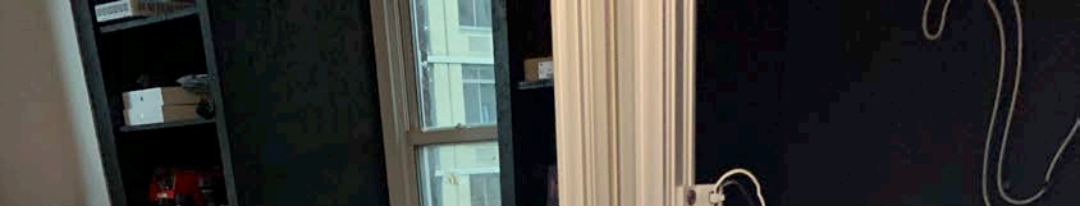
- X86 Mitigations
  - VMM is disabled
  - Disable Watchdog timers

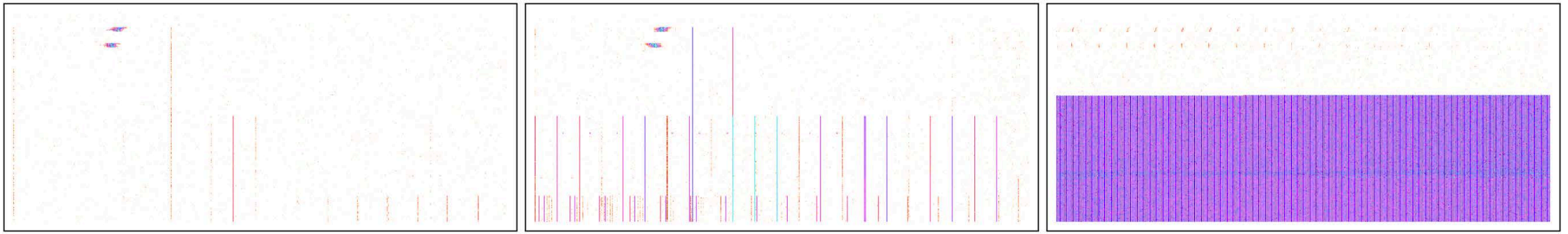
Hypotheses for 💯

- X86 Mitigations
  - VMM is disabled
  - Disable Watchdog timers
  - Disable SMM
    - SMI_EN

ELECTROMAGNETIC EMANATION!





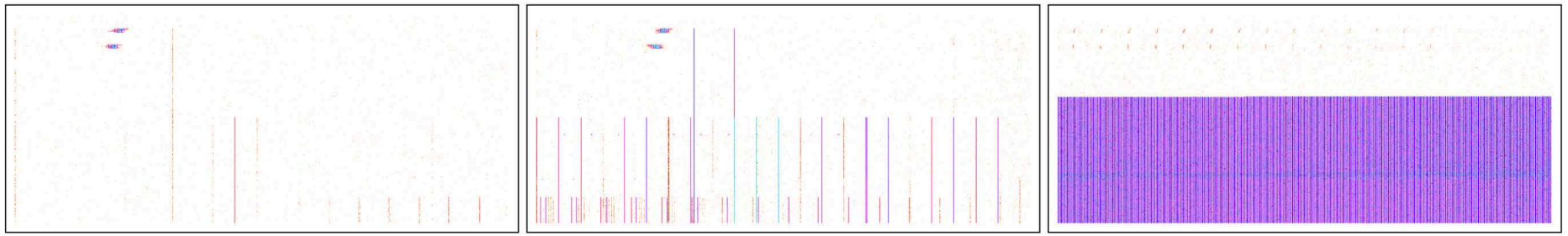


(a) FPGA Bitstream SPI Flash (b) FPGA (c) CPU Power Circuitry

Figure 4: Electromagnetic Spectrum During Boot at 145 MHz (5 MHz Span)

Hypotheses for 💯

- ~~X86~~
- Unknown bits on SPI bus
  - Hardware analysis showed microloader on spi bus

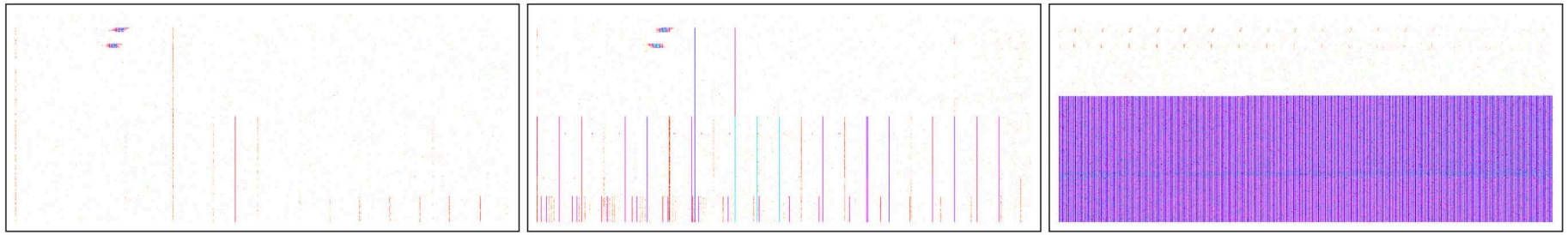


(a) FPGA Bitstream SPI Flash (b) FPGA (c) CPU Power Circuitry

Figure 4: Electromagnetic Spectrum During Boot at 145 MHz (5 MHz Span)

Hypotheses for 💯

- X86
- Unkown bits on SPI bus
  - Hardware analysis showed microloader on spi bus
  - Also contained Interrupt handlers for the real/protected mode.

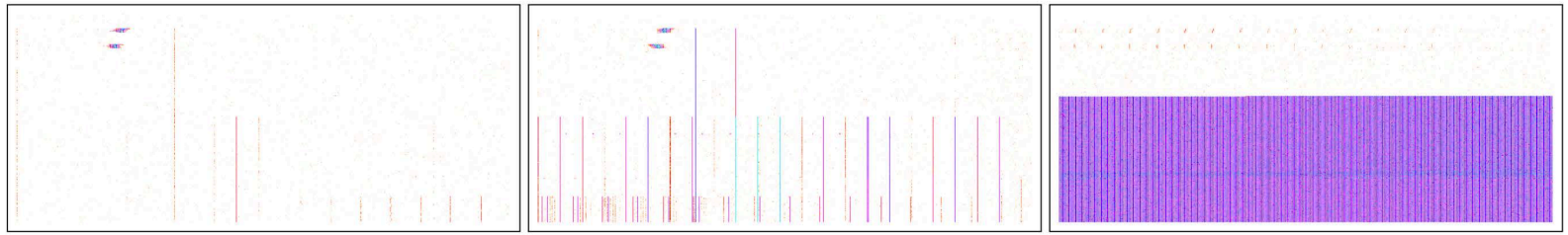


(a) FPGA Bitstream SPI Flash (b) FPGA (c) CPU Power Circuitry

Figure 4: Electromagnetic Spectrum During Boot at 145 MHz (5 MHz Span)

Hypotheses for 💯

- X86
- Unknown bits on SPI bus
  - Hardware analysis showed microloader on spi bus
  - Also contained Interrupt handlers for the real/protected mode.
  - BIOS/ROM/vBIOS (0xc000-0xffff)

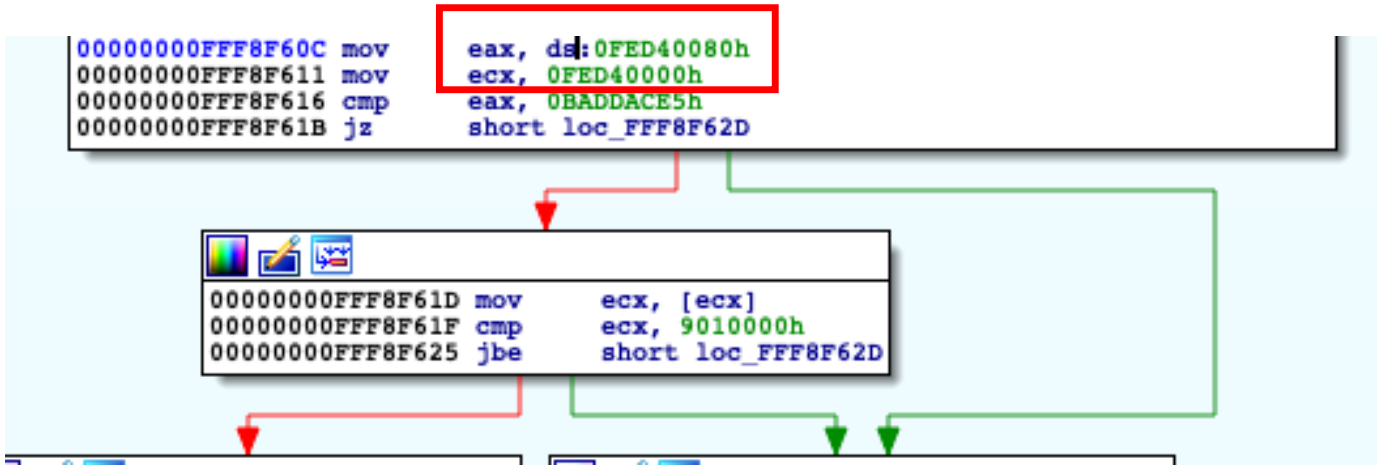


(a) FPGA Bitstream SPI Flash (b) FPGA (c) CPU Power Circuitry

Figure 4: Electromagnetic Spectrum During Boot at 145 MHz (5 MHz Span)

Hypotheses for 💯

- x86
- Unknown bits on SPI bus
- PRE-ROMmon



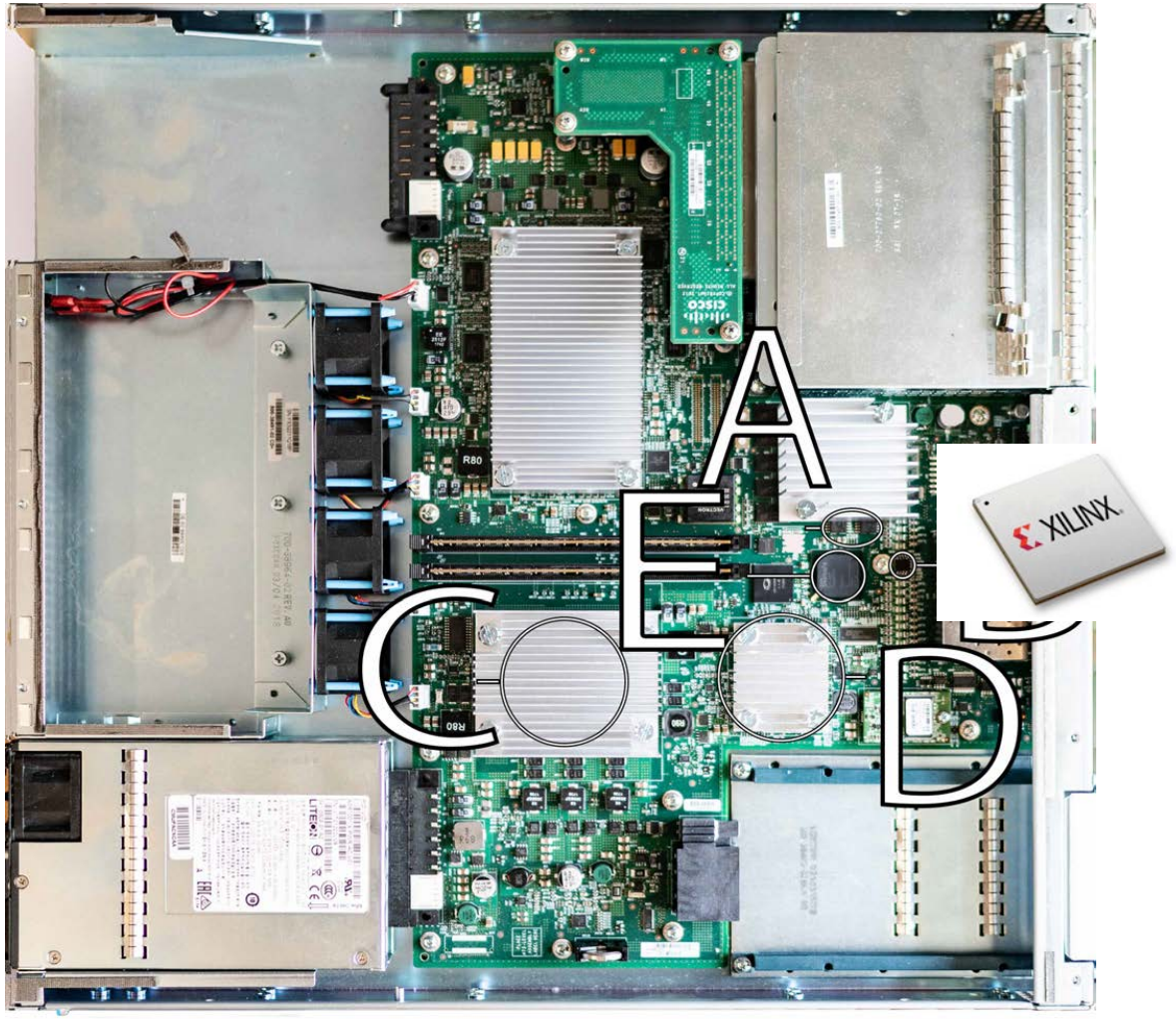
Hypotheses for 💯

- X86
- Unknown bits on SPI bus
- PRE-ROMmon
- Hijacked 1st x86_64 instruction

💡💡 RESET PULL LOW Hypotheses 💡💡

- External Entity Resets RP

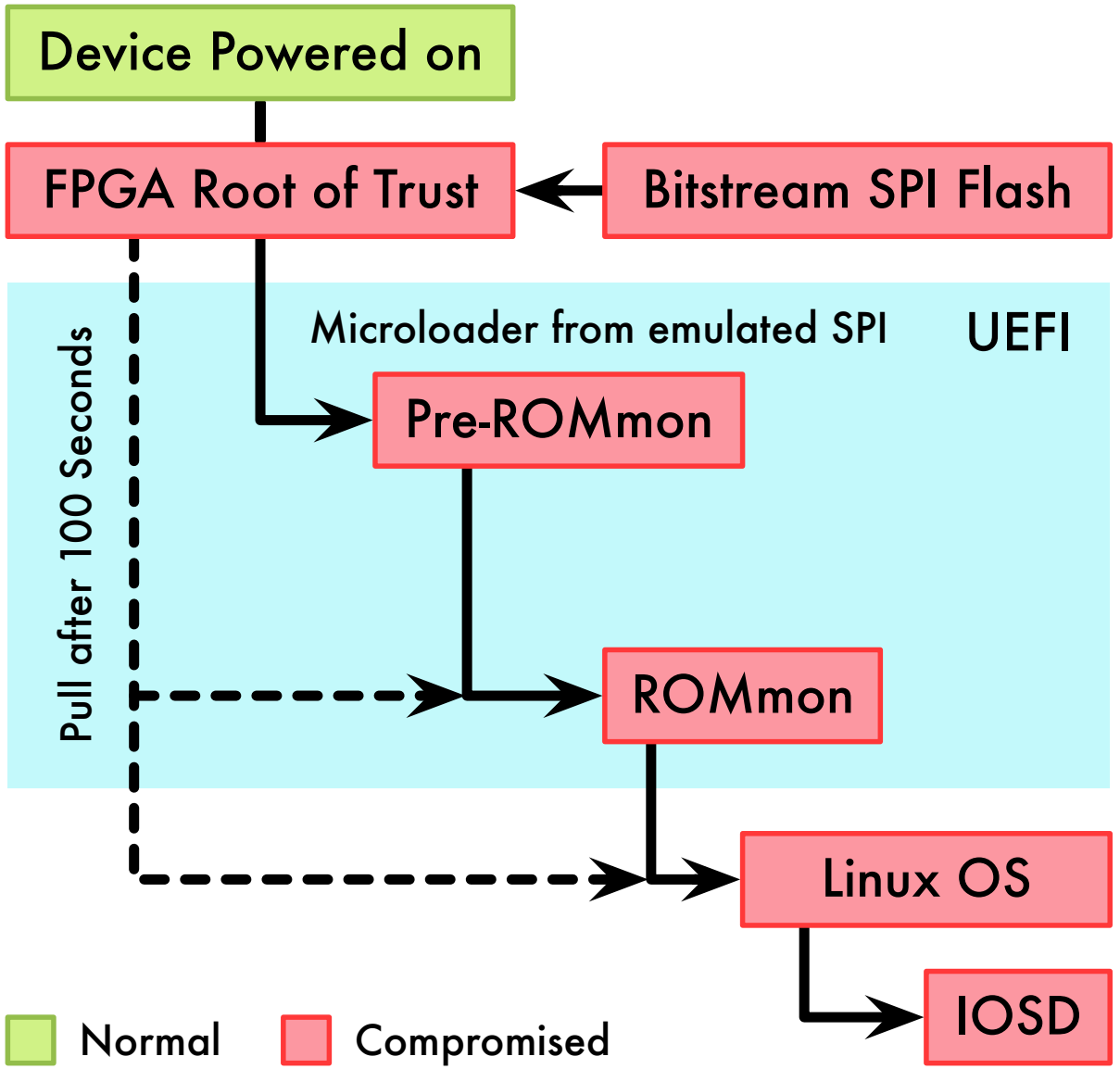
RESET PULL LOW Hypotheses



A) Bootloader Flash **B)** FPGA Bitstream SPI Flash **C)** Intel Xeon (Route Processor)

D) Intel Comunications Processor **E)** FPGA (Trust Anchor, other services)

Boot flow


Device Powered on
FPGA Root of Trust
Bitstream SPI Flash
Microloader from emulated SPI
UEFI
Pre-ROMmon
Pull after 100 Seconds
ROMmon
Linux OS
IOSD
Normal
Compromised

$$$

Cisco ASR 1001-X Router

ASR 1000 Series Aggregation Services Router

cisco Partner

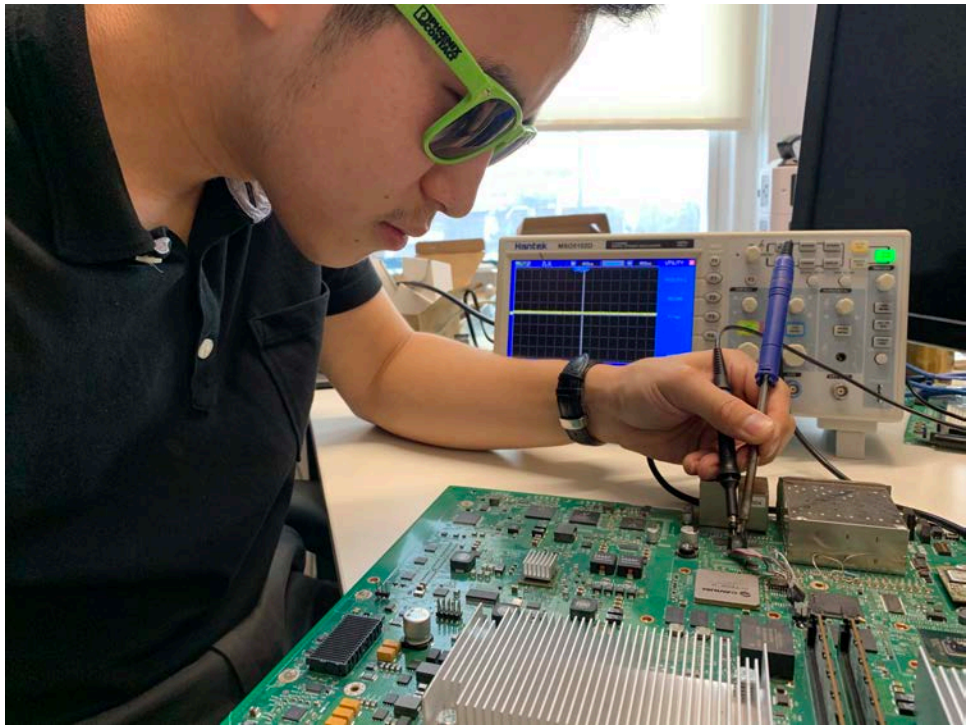
Cisco ASR1000 Series		
Cisco ASR1001-X System		
Cisco ASR1001-X System, Crypto, 6 built-in GE, Dual P/S	FREE SHIPPING #ASR1001-X List Price: ~~$17,000.00~~ **Our Price: $11,328.80**	Add to Cart
Cisco ASR1001-X System, Crypto, 6 built-in GE, Dual P/S, Spare	FREE SHIPPING #ASR1001-X= List Price: ~~$24,224.99~~ **Our Price: $16,143.53**	Add to Cart

$$$

FREE SHIPPING	#ASR1001-X List Price: ~~$17,000.00~~ **Our Price: $11,328.80**	Add to Cart
FREE SHIPPING	#ASR1001-X= List Price: ~~$24,224.99~~ **Our Price: $16,143.53**	Add to Cart

FIND RESET PIN

Counter: -$10K Analysis cost



TEST RESET HIGH
Theory!!

- RTL reconstruction is hard

TEST RESET HIGH
Theory!!

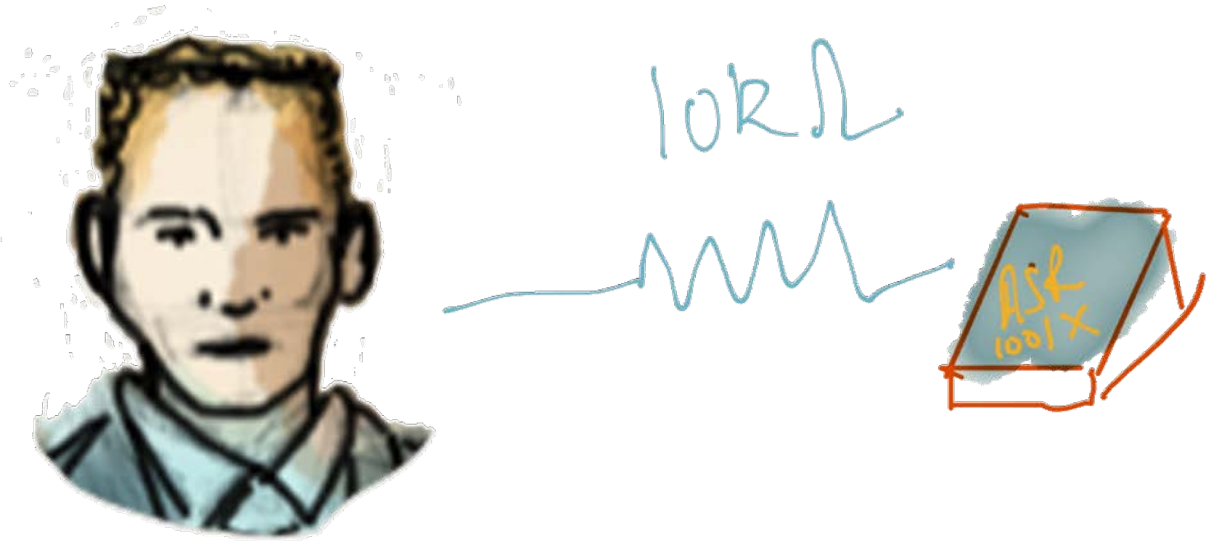
- RTL reconstruction is hard
- Test FPGA theory

TEST RESET HIGH Theory!!

- RTL reconstruction is hard
- test the FPGA theory
- Pull RESET pin high

TEST RESET HIGH Theory!!

- RTL reconstruction is hard
- test the FPGA theory
- Pull the RESET pin high
- 10k resister & Another $10k



TEST RESET HIGH Theory!!

- RTL reconstruction is hard
- test the FPGA theory
- Pull the RESET pin high
- 10k resister & Another $10k
- $1/1Ω
- Total Cost -$20k

Oh hay, look!

Joey

US 20120303941A1

(19) **United States**

(12) **Patent Application Publication**

GRIECO et al.

(10) **Pub. No.: US 2012/0303941 A1**

(43) **Pub. Date: Nov. 29, 2012**

(54) **METHOD AND APPARATUS FOR SECURING CPUS BOOTED USING ATTACHED FLASH MEMORY DEVICES**

(76) Inventors: **ANTHONY H. GRIECO**, Wake Forest, NC (US); **CHIRAG K. SHROFF**, Apex, NC (US); **ROBERT T. BELL**, Bountiful, UT (US)

(21) Appl. No.: **13/114,831**

(22) Filed: **May 24, 2011**

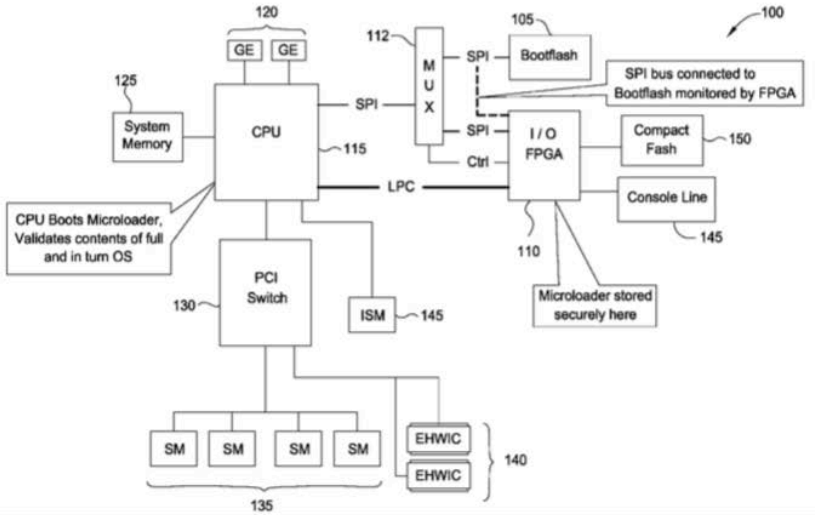
Publication Classification

(51) **Int. Cl.**
G06F 15/177 (2006.01)

(52) **U.S. Cl.** **713/2**

(57) **ABSTRACT**

The present disclosure describes techniques evaluating compute and/or thermal loads (among other things) to aid in managing a collection of one or more containerized or modular data centers. For example, forecasts (or real-time measurements) of environmental factors (as well as projected computing demands) may be used to tailor the compute loads, cooling strategies or other metric of data center operations for a network of containerized or modular data centers. Doing so allows an operator of such a data center network to manage specific operational goals in real time.



Fpga reversing too complex

Leave project in mid 2017

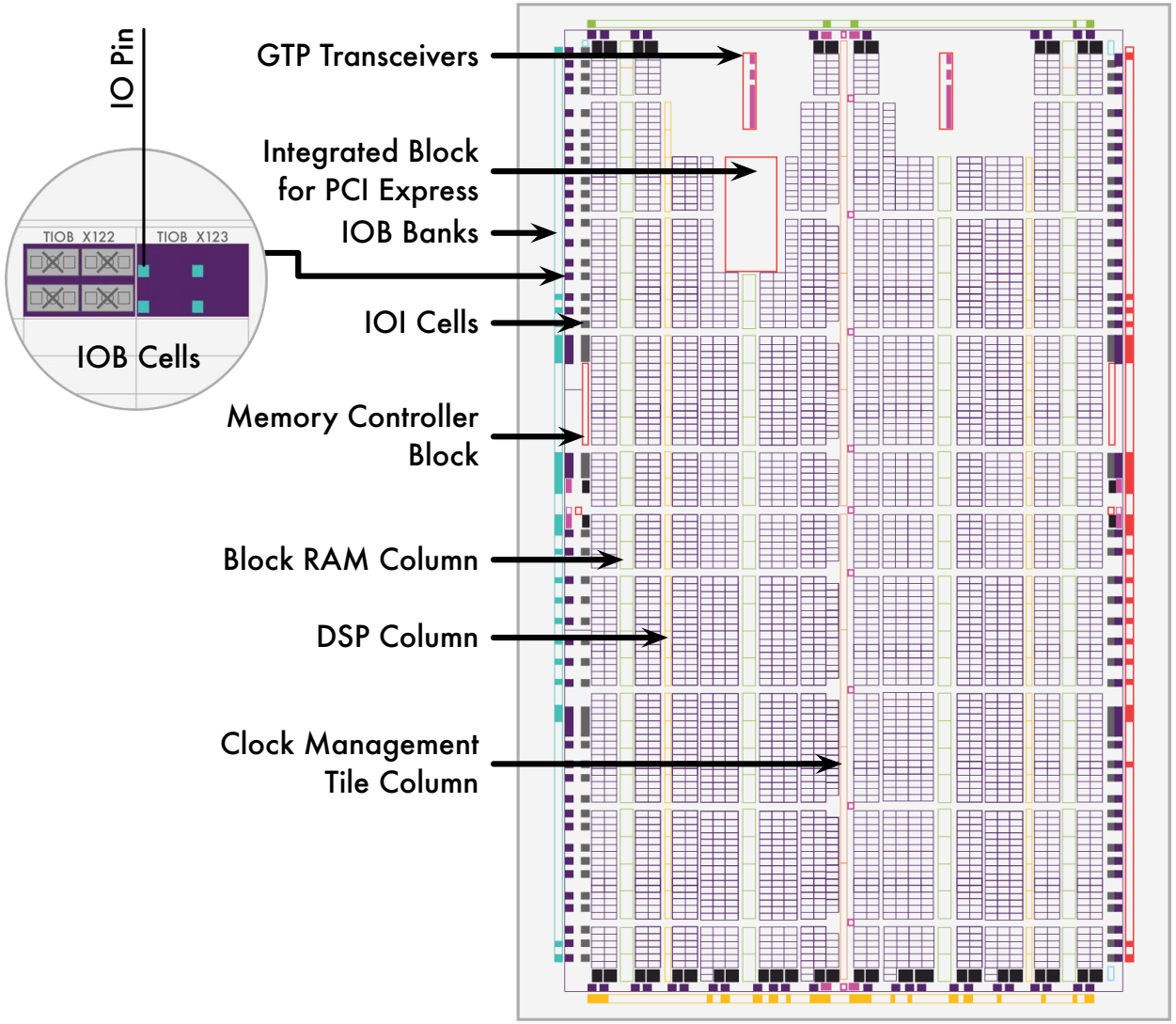
2018 summer:

JK: can hack fpga

- Counter: -$20k

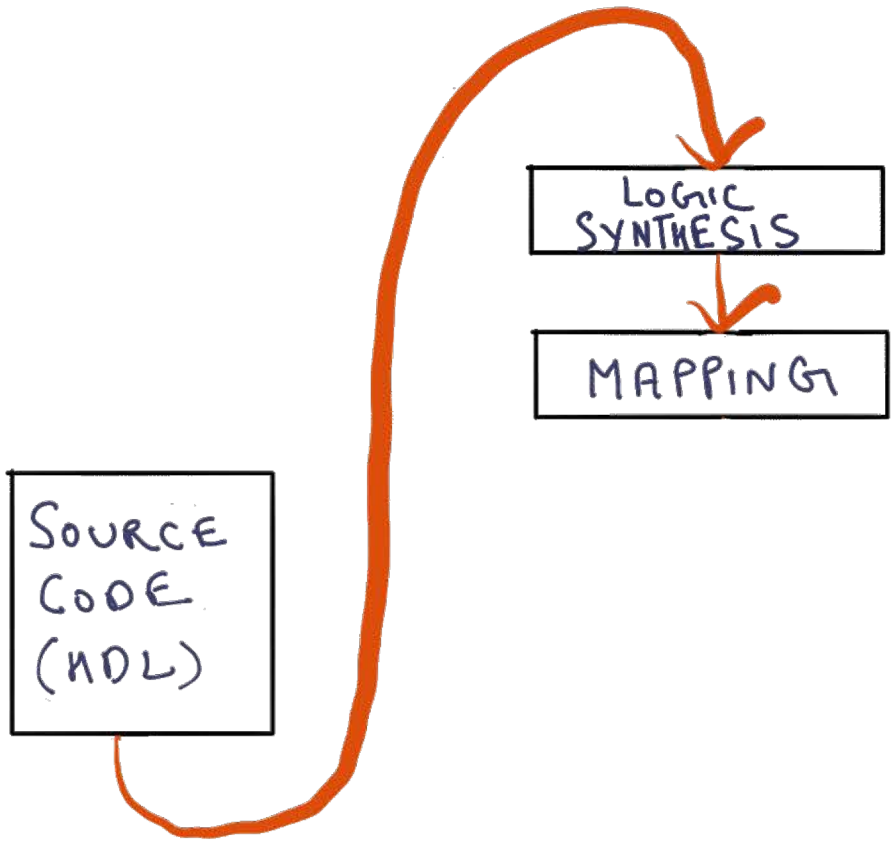
FPGA BASICS FOR Humans

FPGA ??

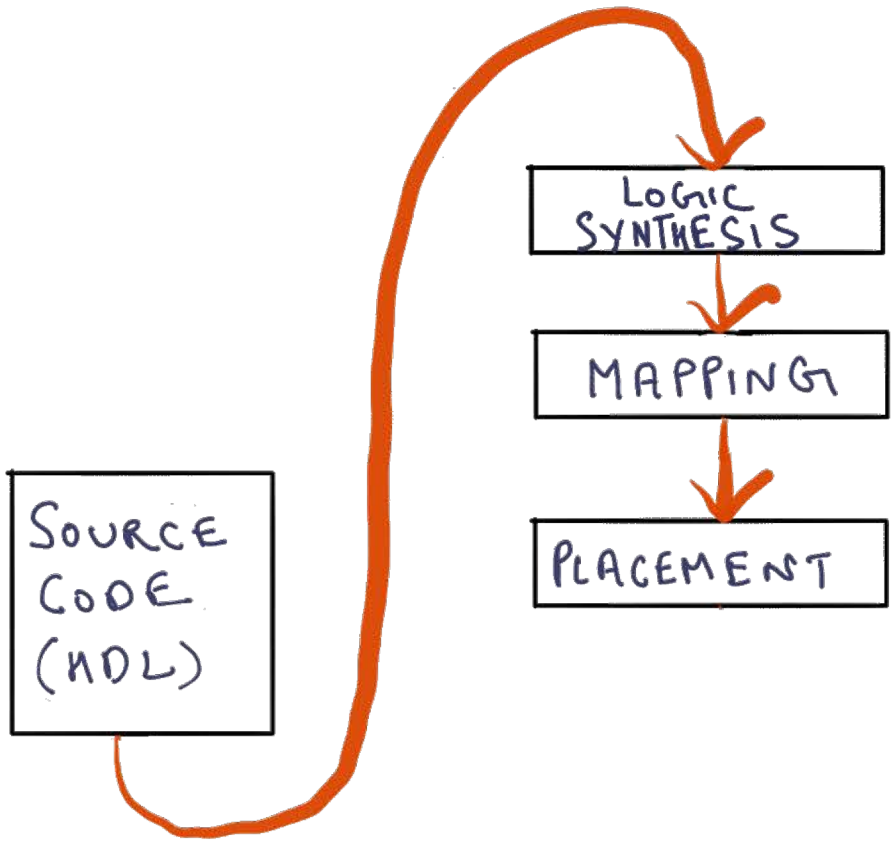

IO Pin
TIOB_X122
TIOB_X123
IOB Cells
GTP Transceivers
Integrated Block
for PCI Express
IOB Banks
IOI Cells
Memory Controller
Block
Block RAM Column
DSP Column
Clock Management
Tile Column

FPGA Design Flow

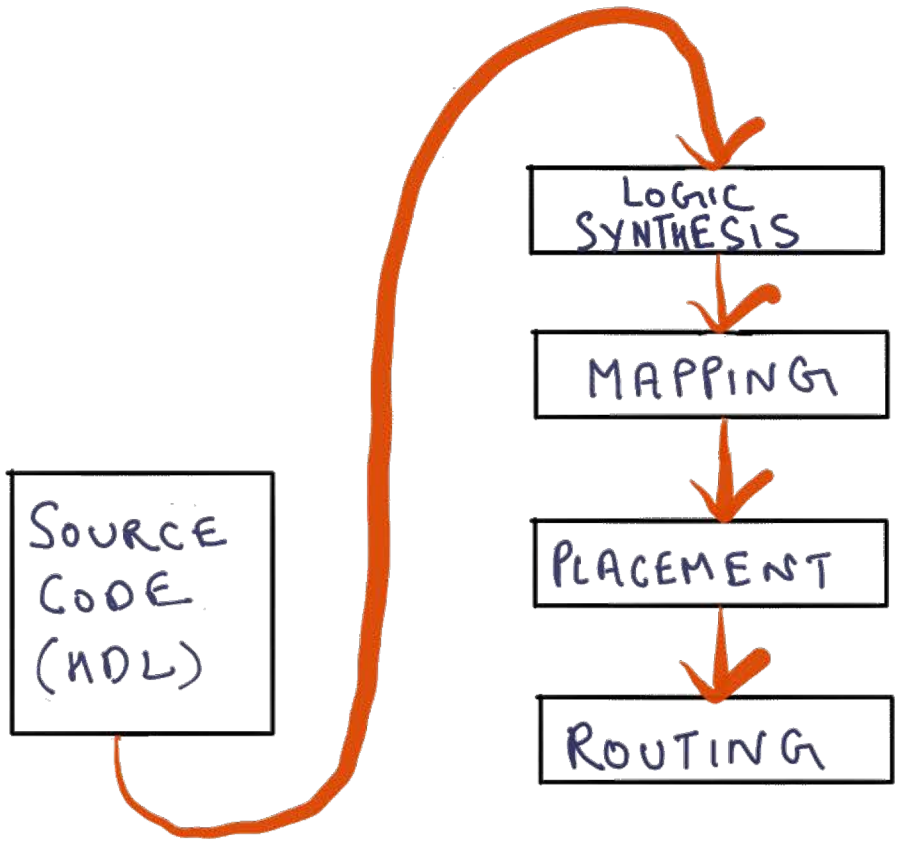
FPGA Design Flow



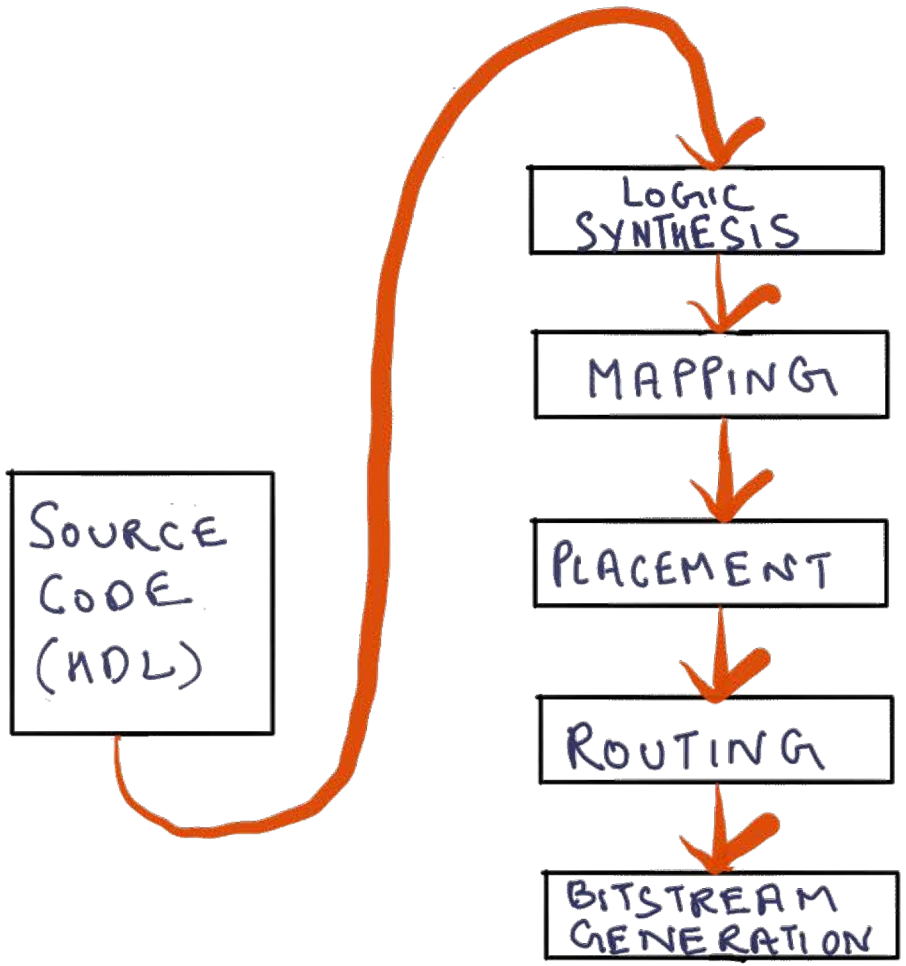
FPGA Design Flow



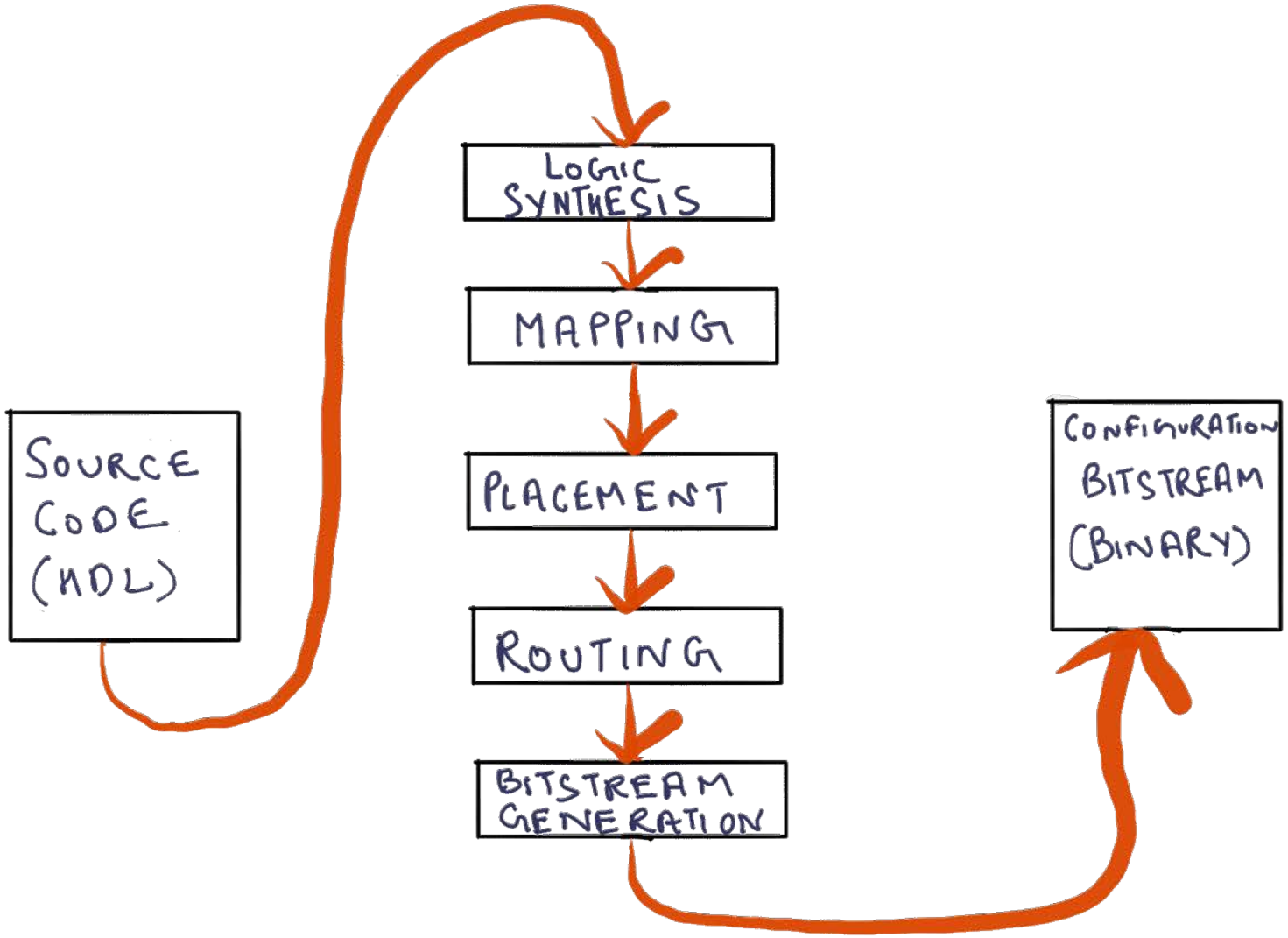
FPGA Design Flow



FPGA Design Flow



FPGA Design Flow



FPGA
Implementation TYPES

- SRAM-Based

FPGA
Implementation TYPES

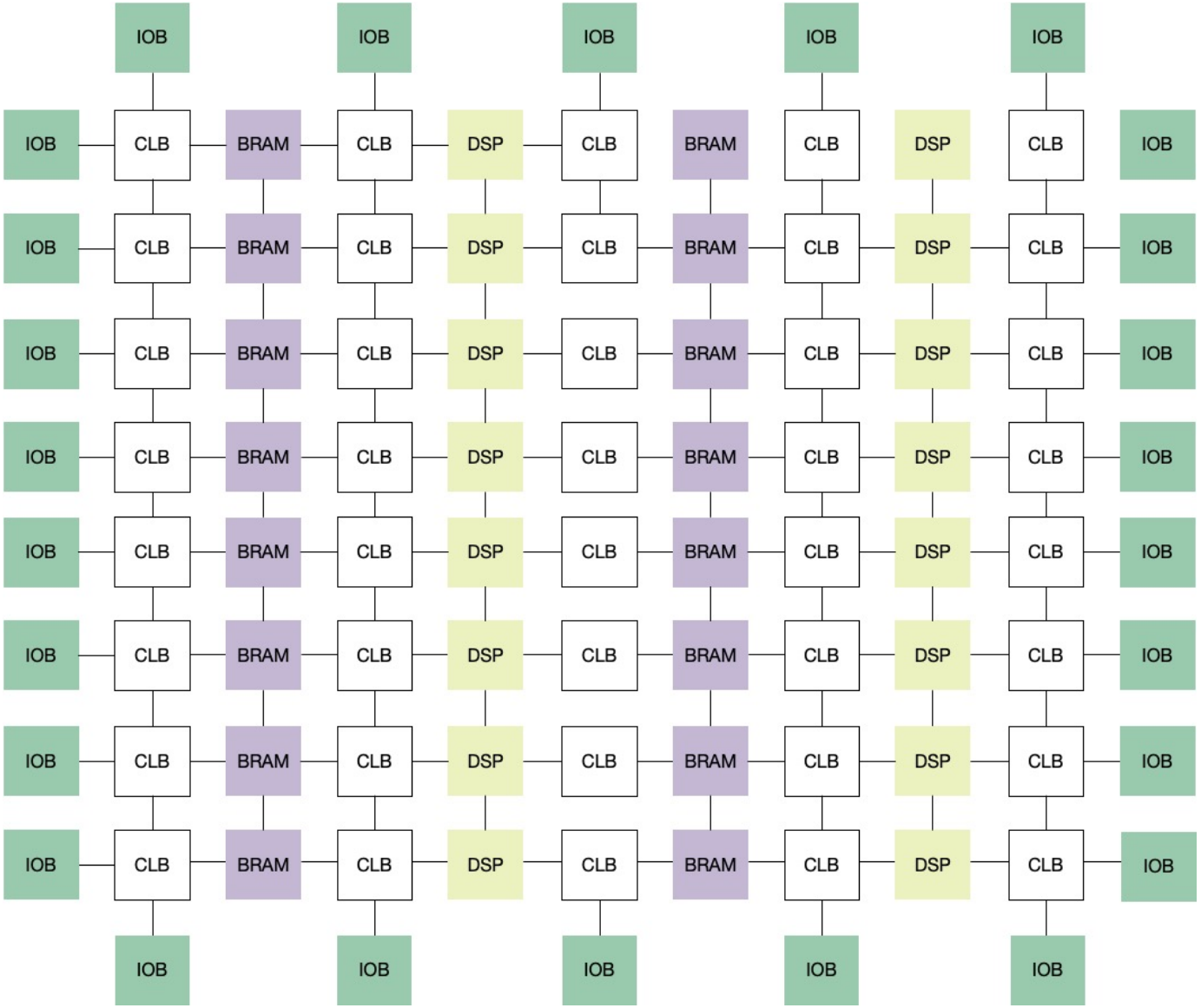
- SRAM-Based

- Flash-Based

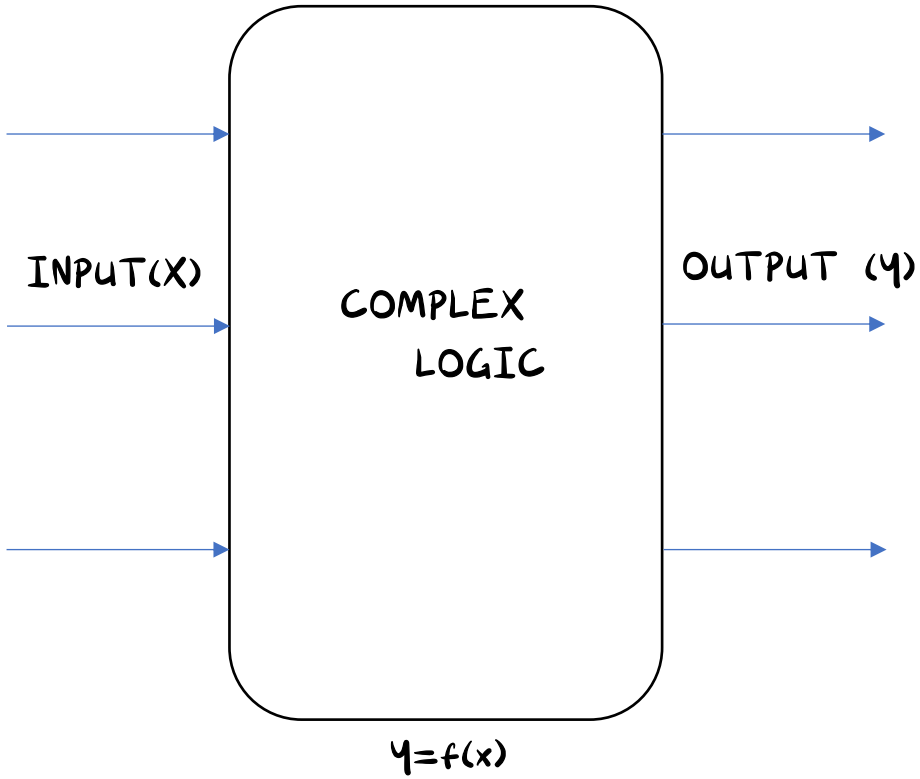
FPGA
Implementation TYPES

- SRAM-Based
- Flash-Based
- AntiFuse-Based

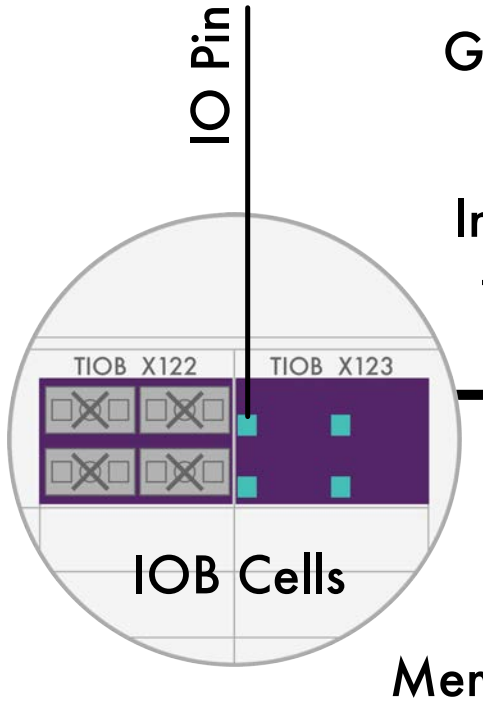
FPGA ??



FPGA !!

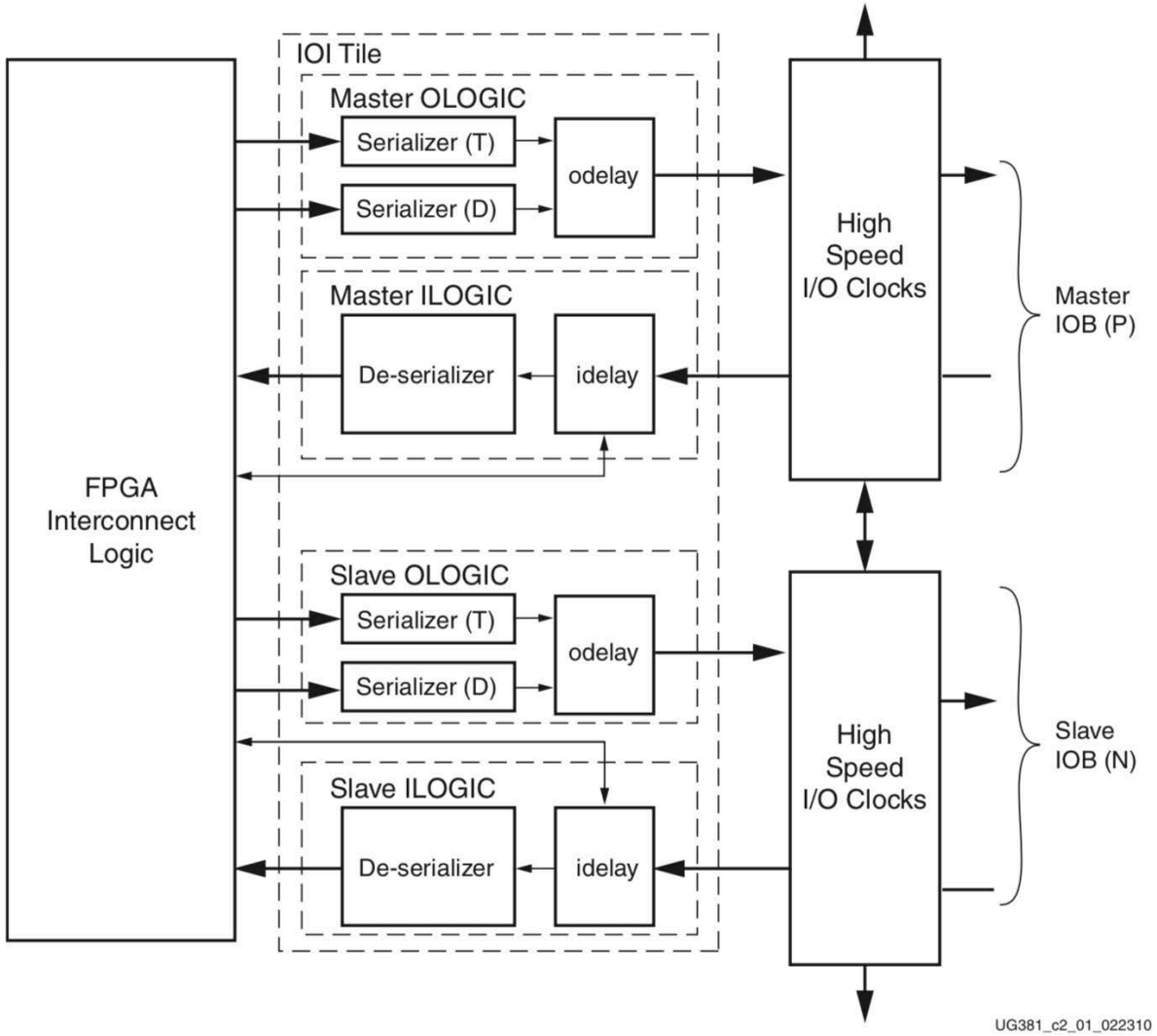


IO Block(IOB)

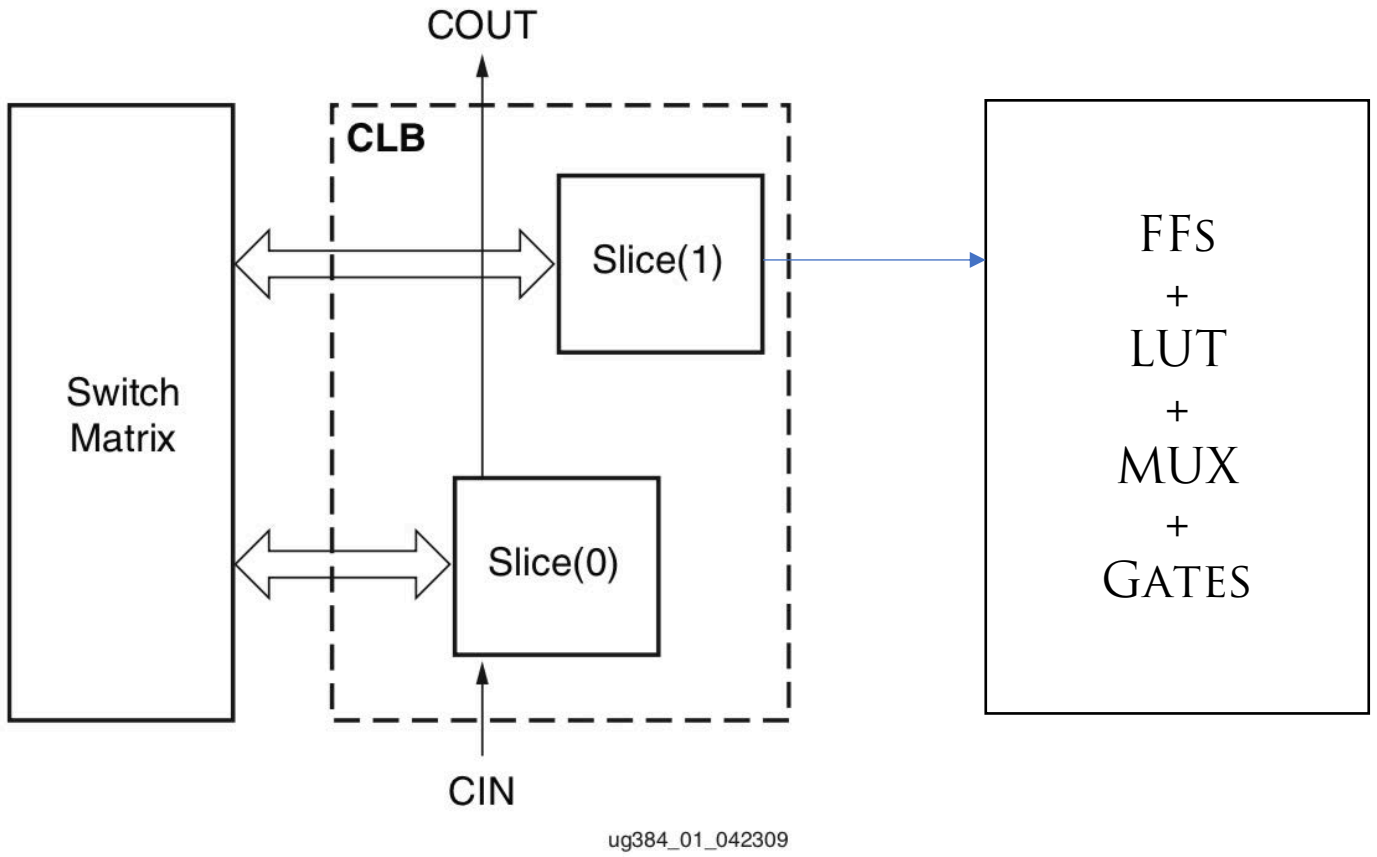


IO INTERFACE (IOI)

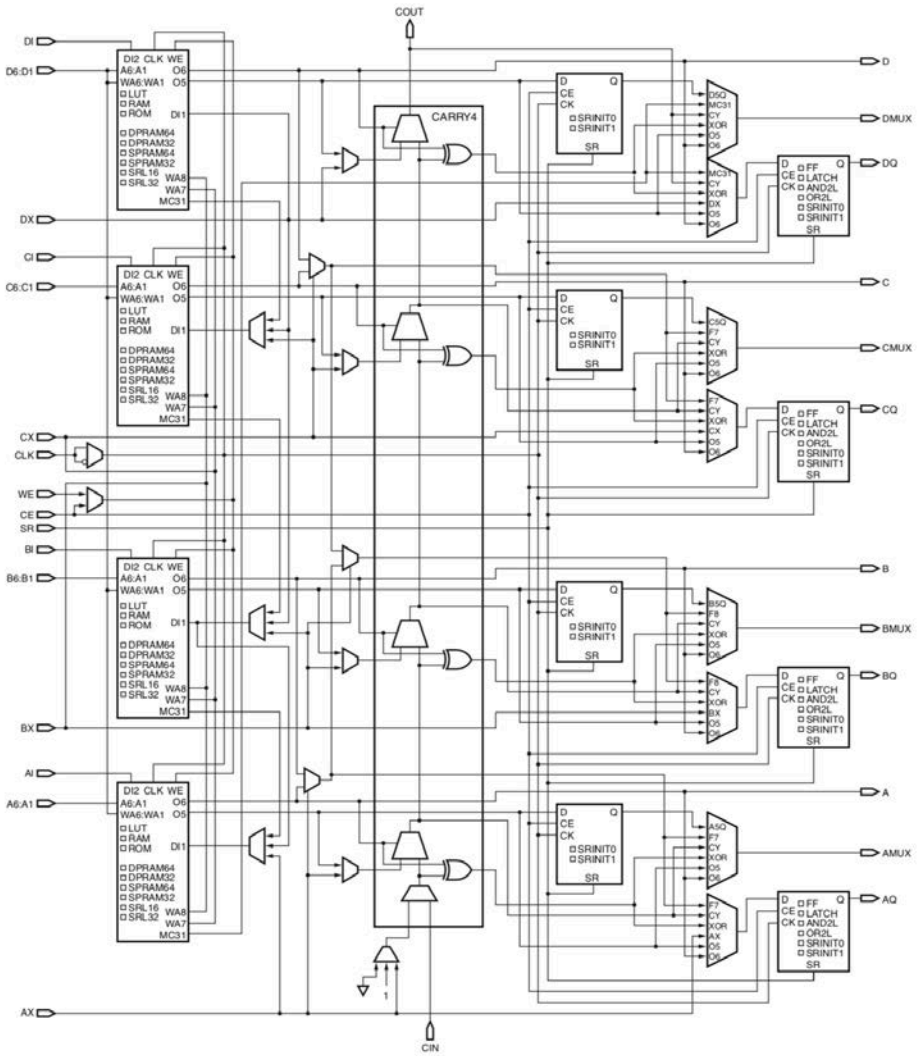
MEOW



Complex Logic Block (CLB)



Slice Complexity

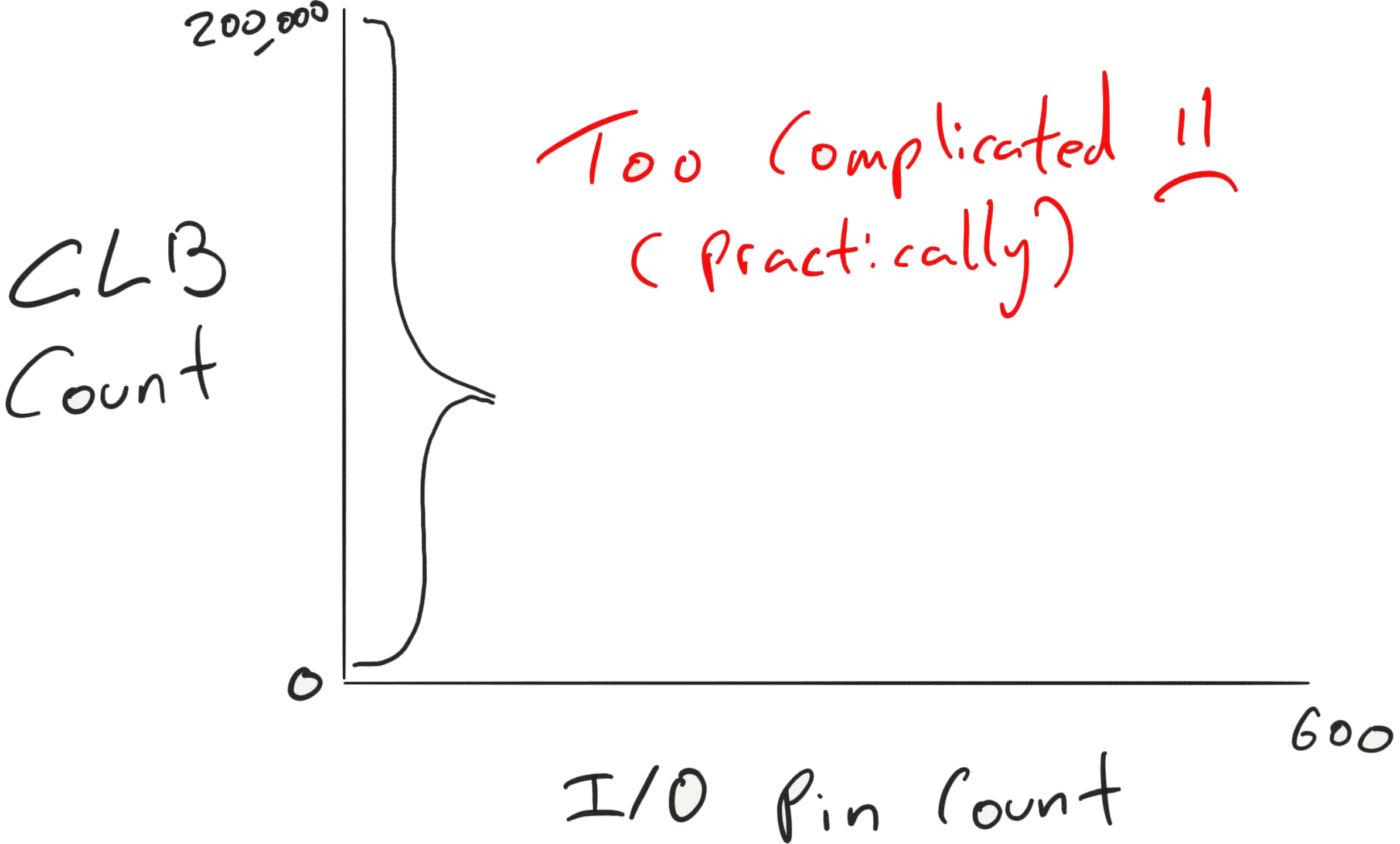


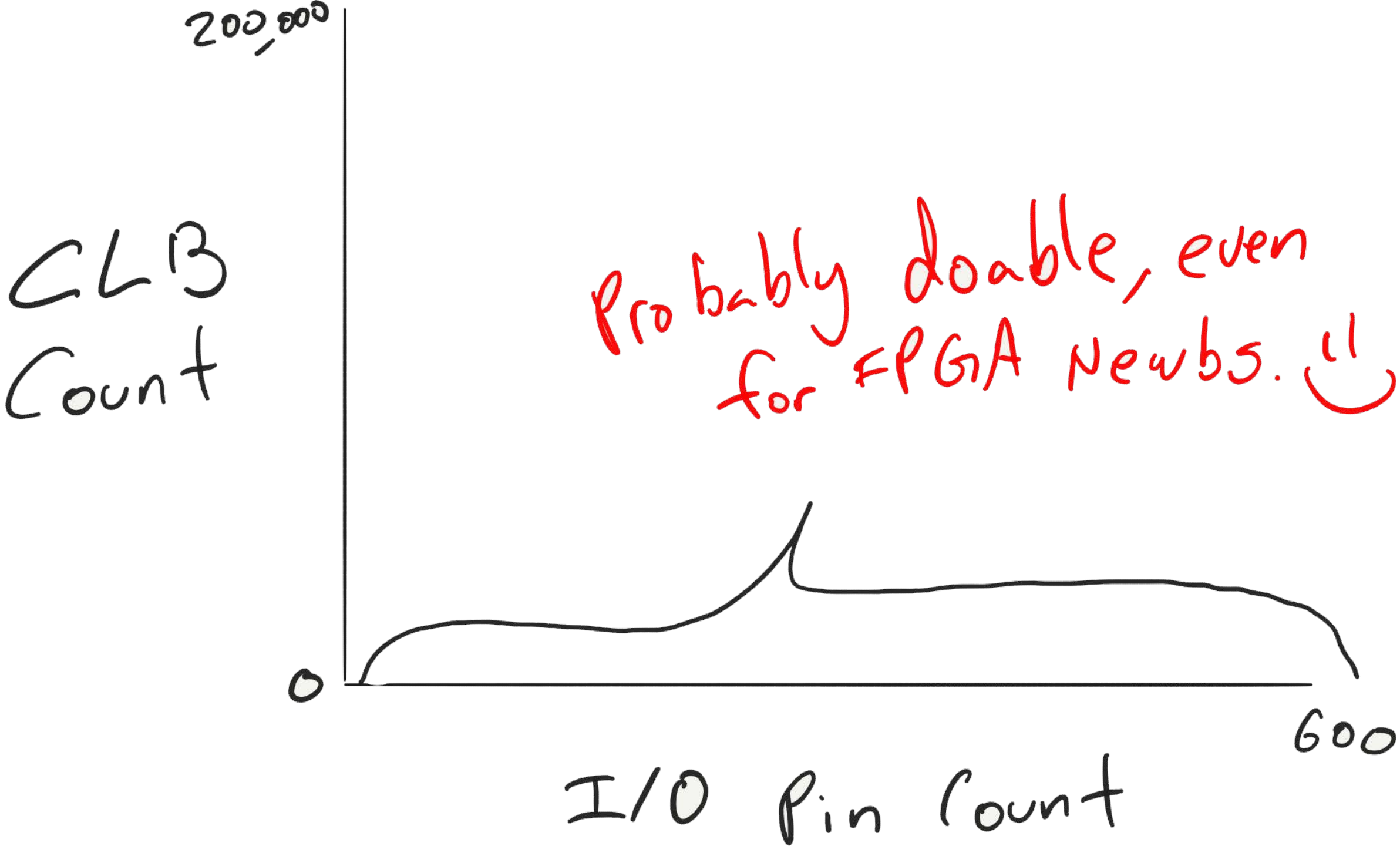
SLICEM

Reverse FPGA Bitstream

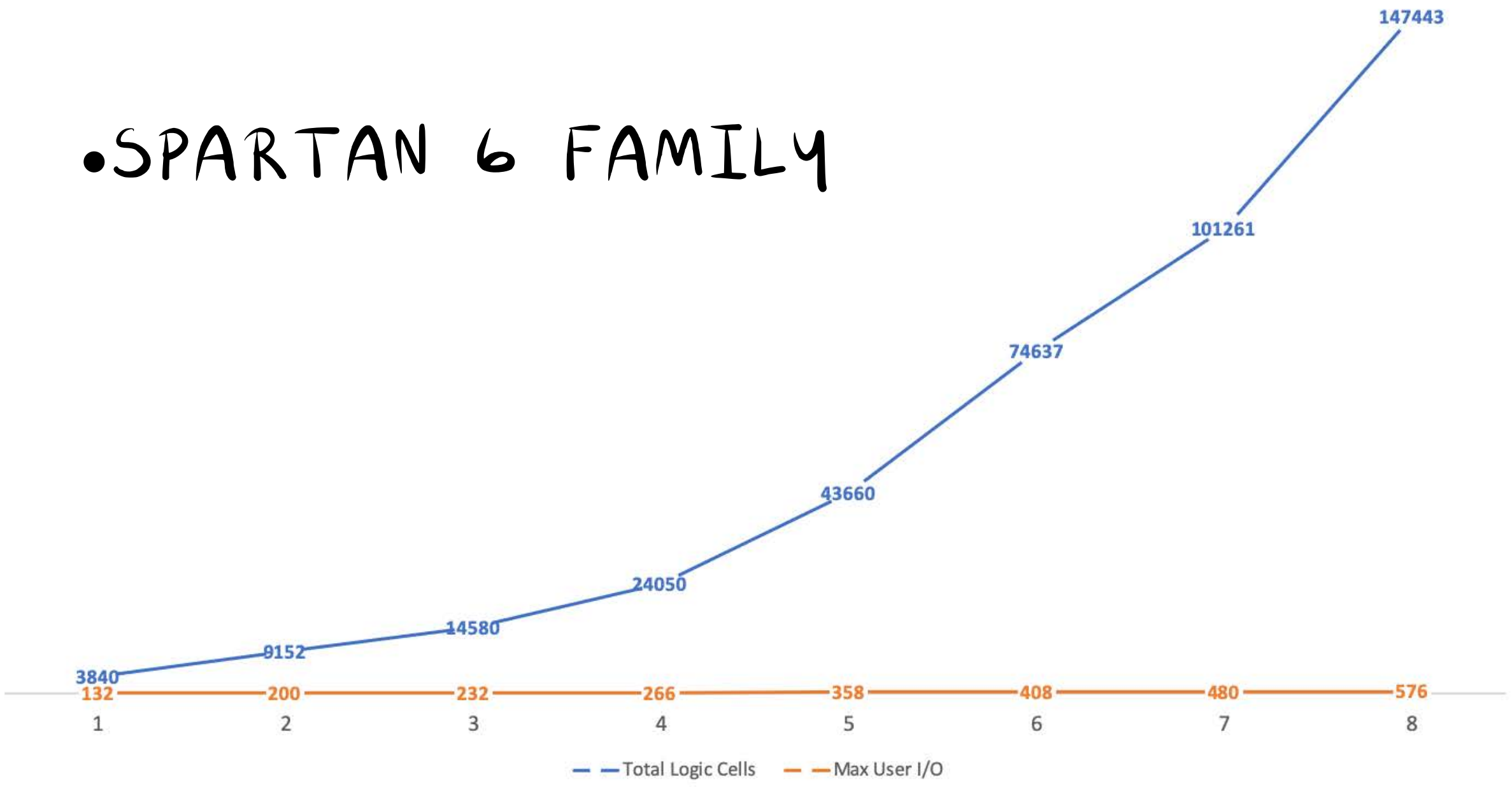
FPGA Reversing Background

- JBITS 1999
- Bil (Requires Netlist) 2012
- BITMAN 2017

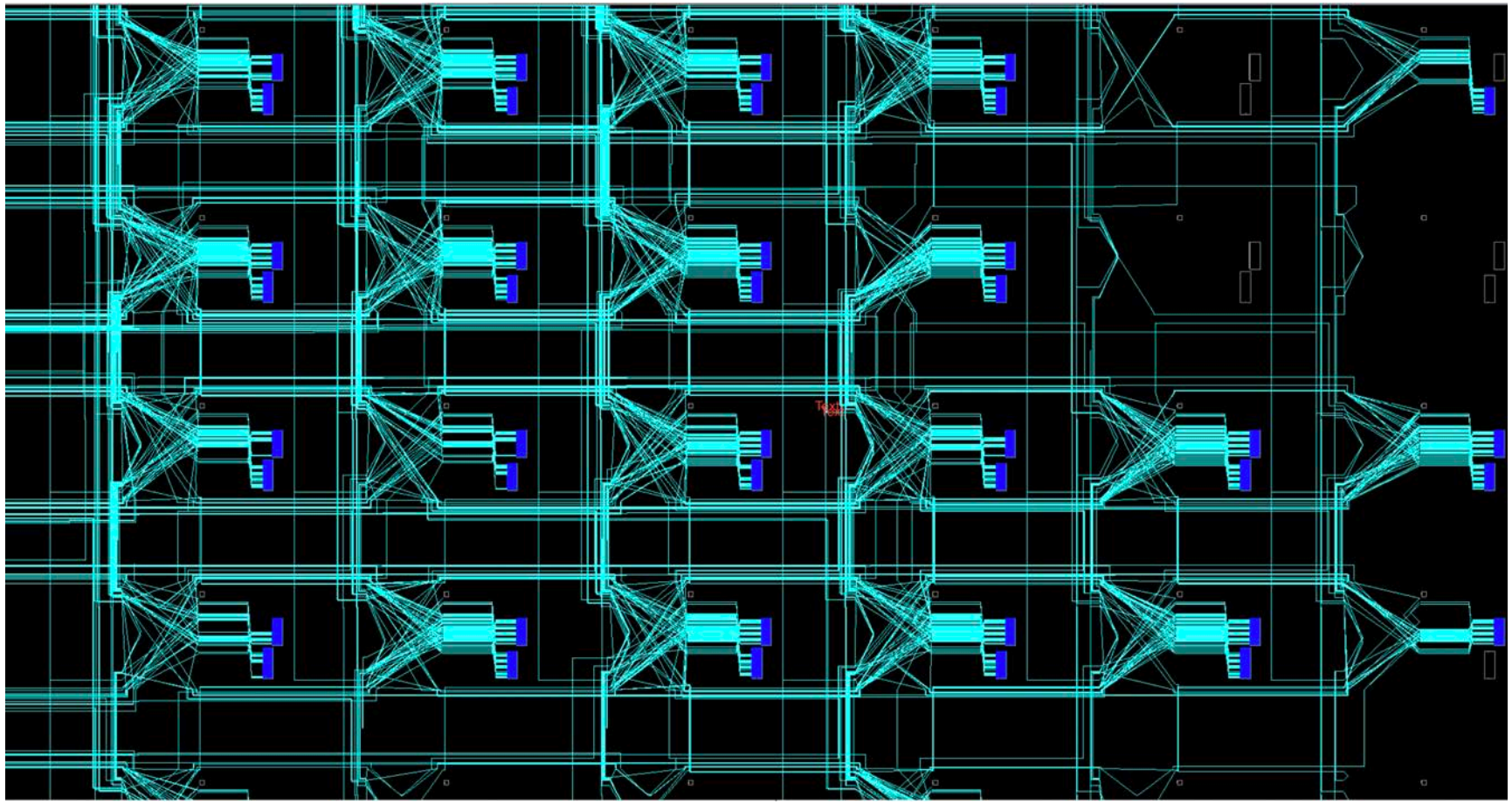

200,000
CLB
Count
0
600
I/O Pin Count
Too Complicated !!
(Practically)


200,000
CLB Count
0
600
I/O Pin Count
Probably doable, even for FPGA Newbs. :)

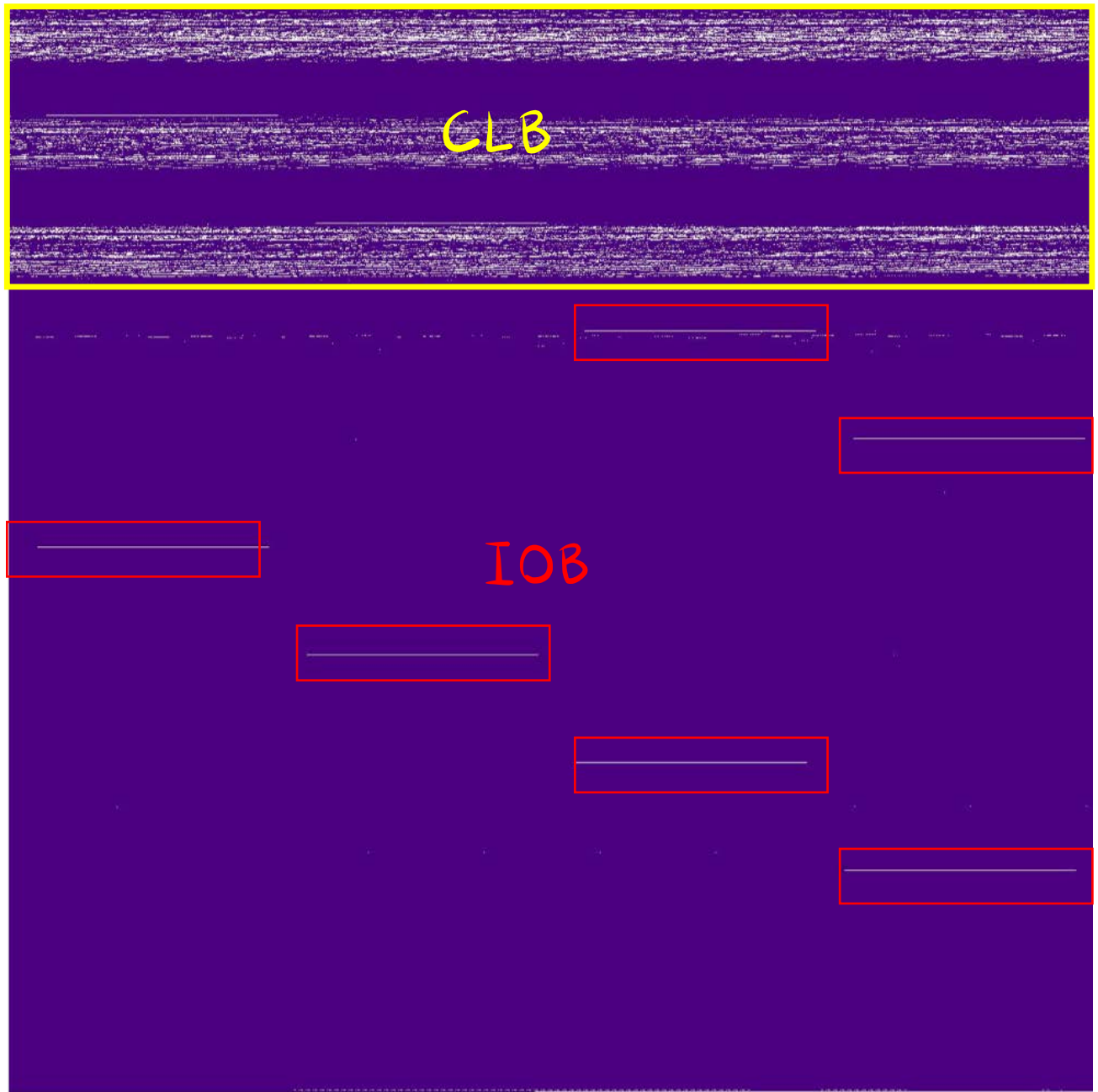
- SPARTAN 6 FAMILY



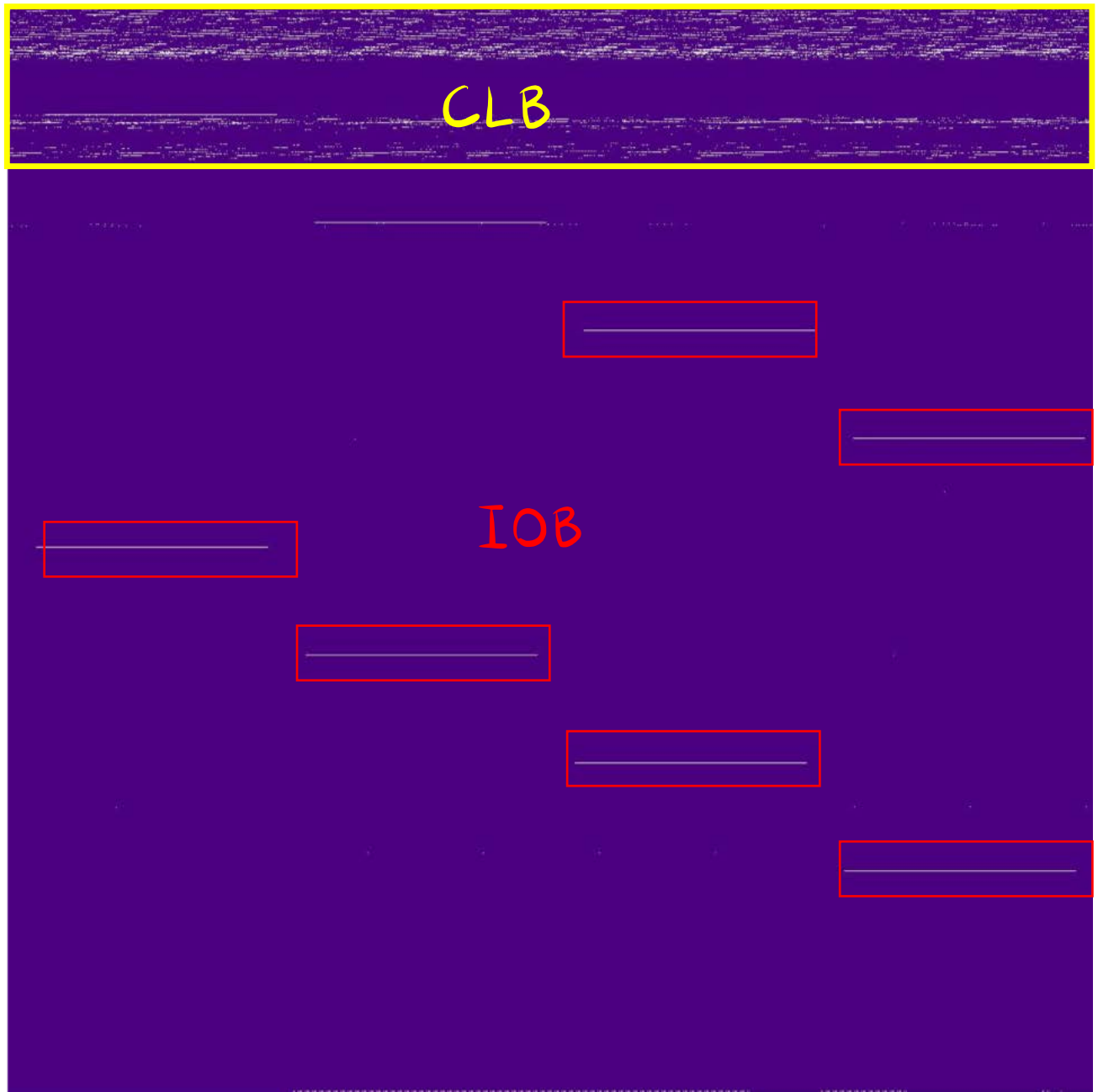
FPGA SECURITY ??



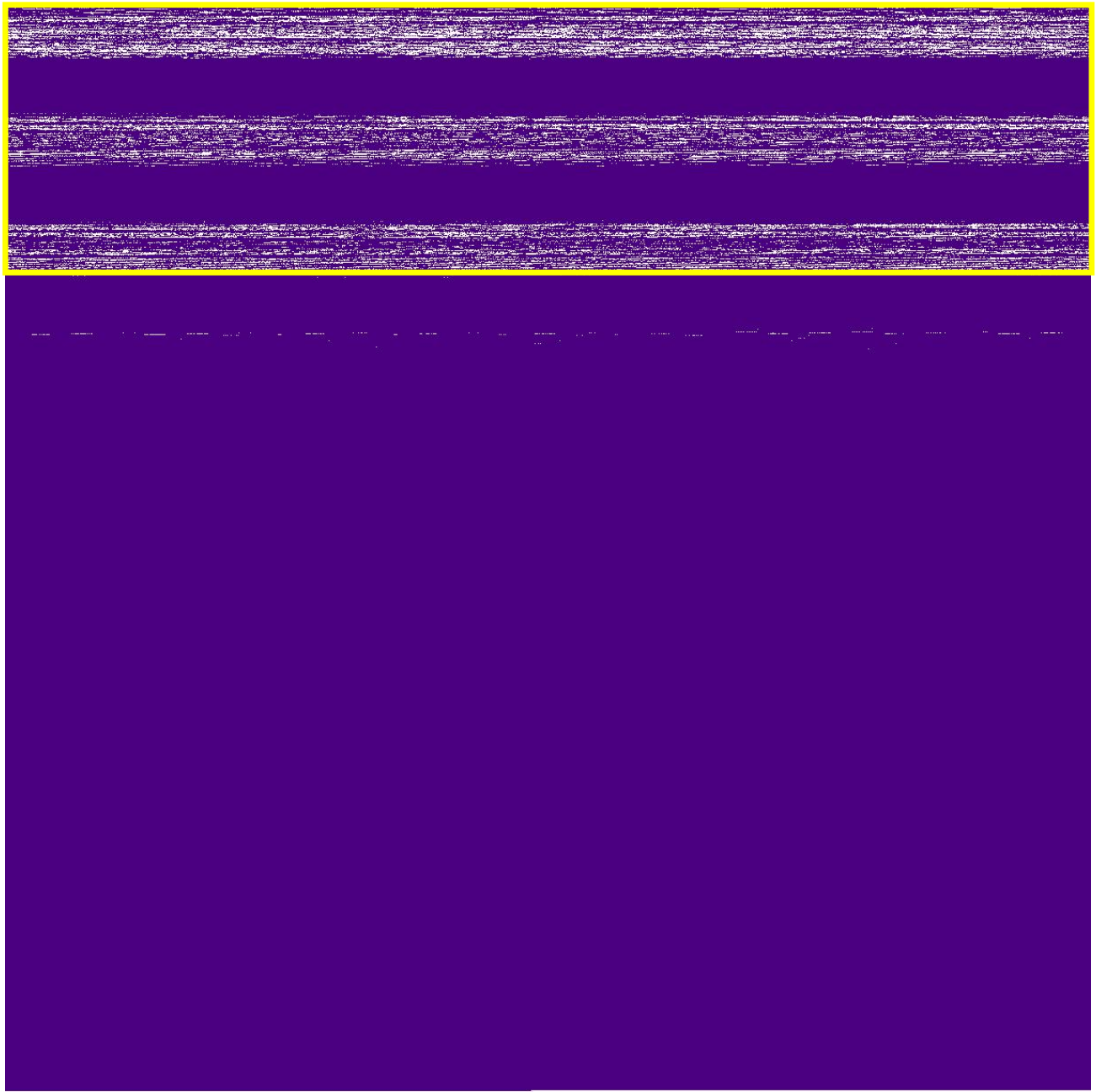
Constant IOB



Constant IOB

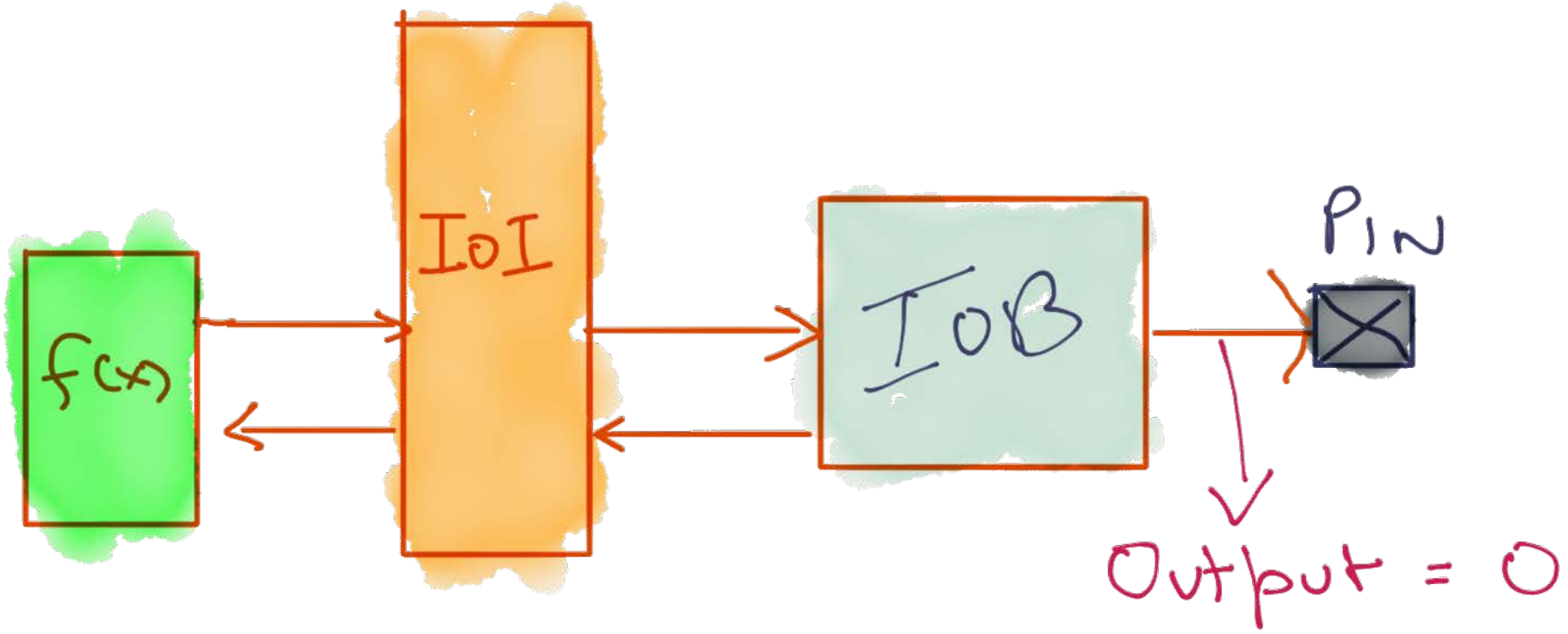


Constant IOB



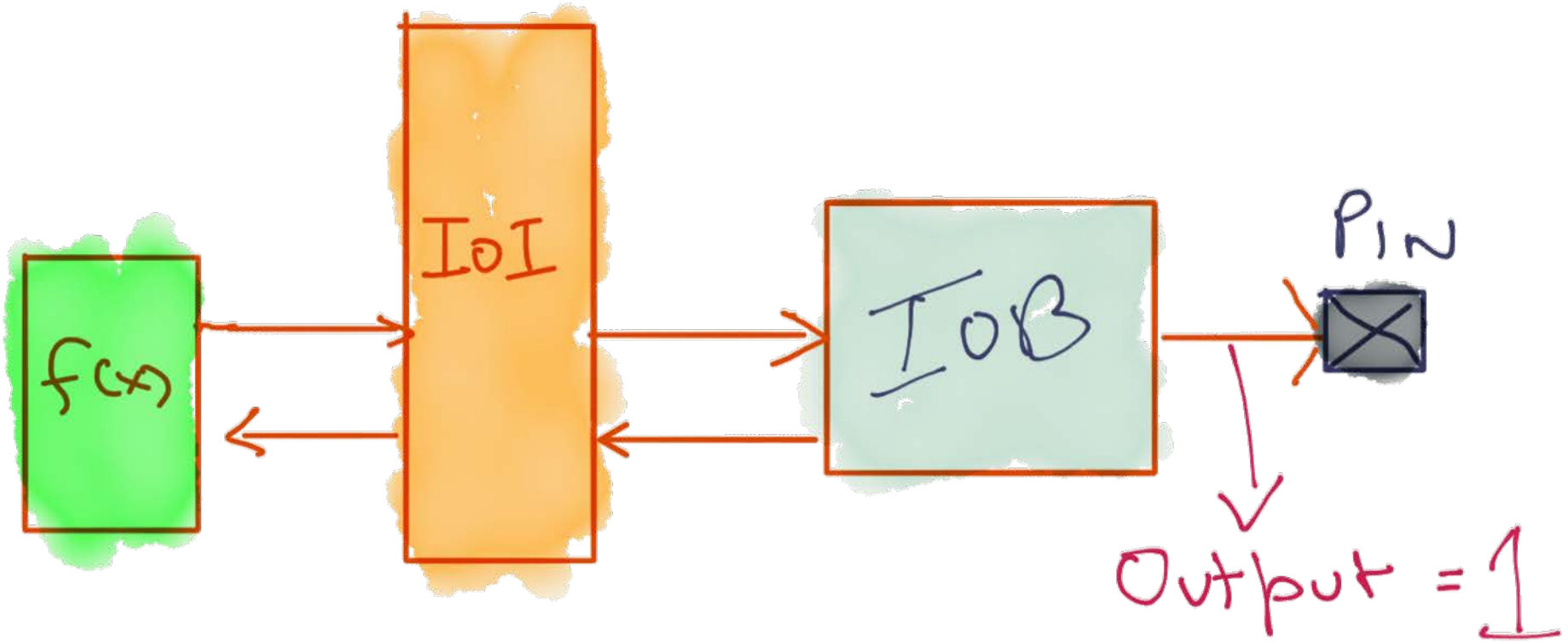
IOB Modification

Scenarios

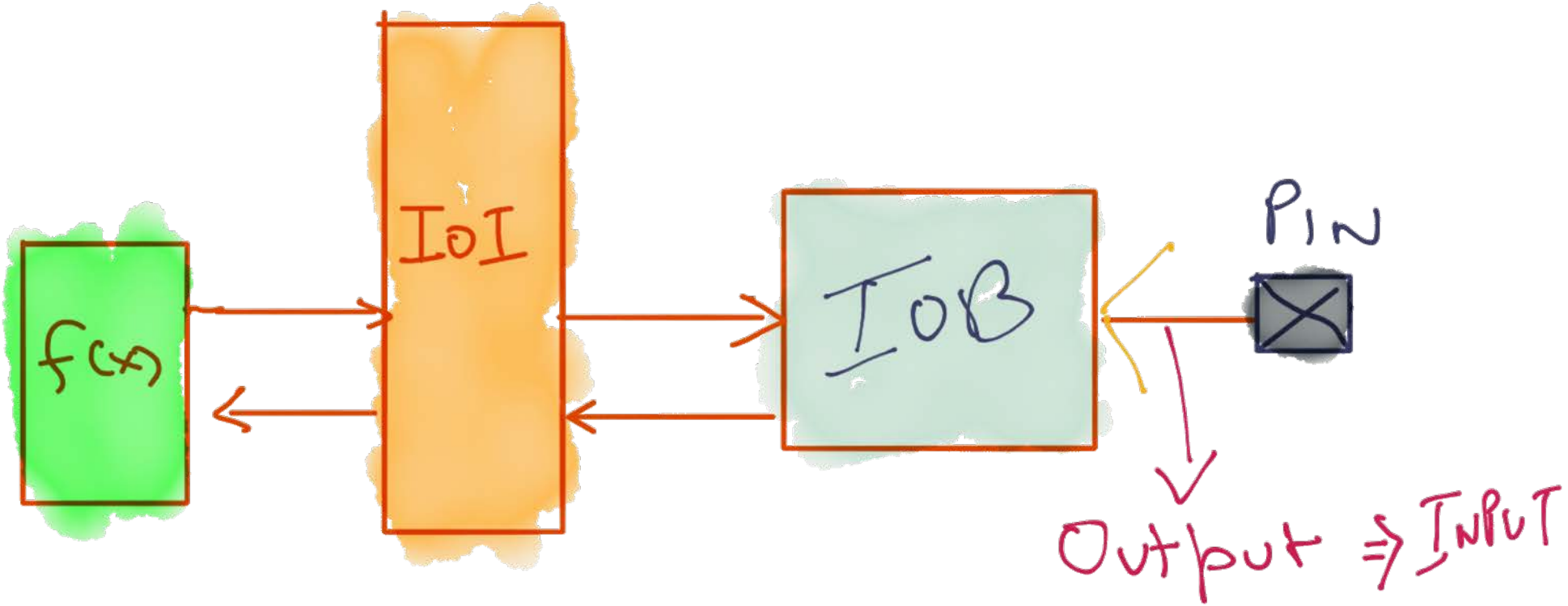


IOB Modification

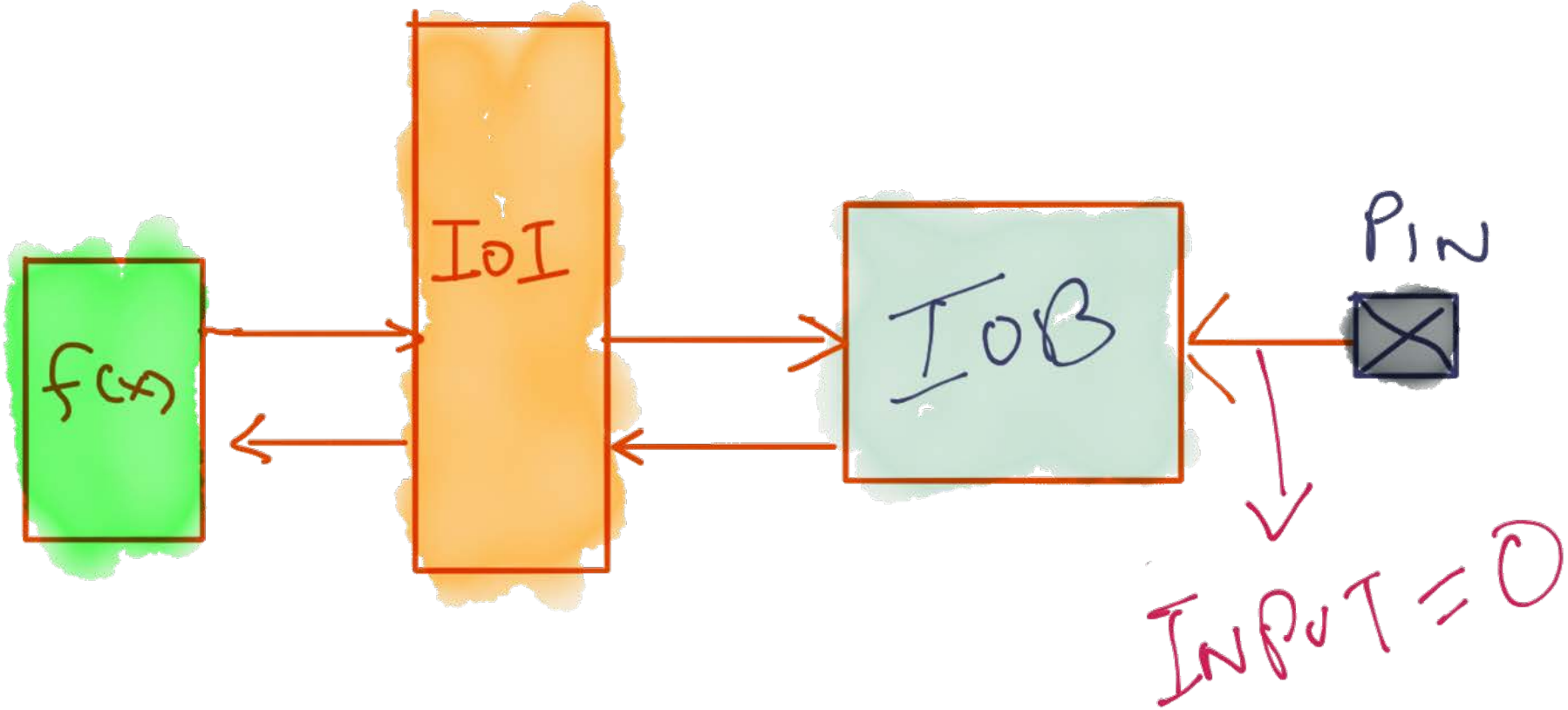
Scenarios



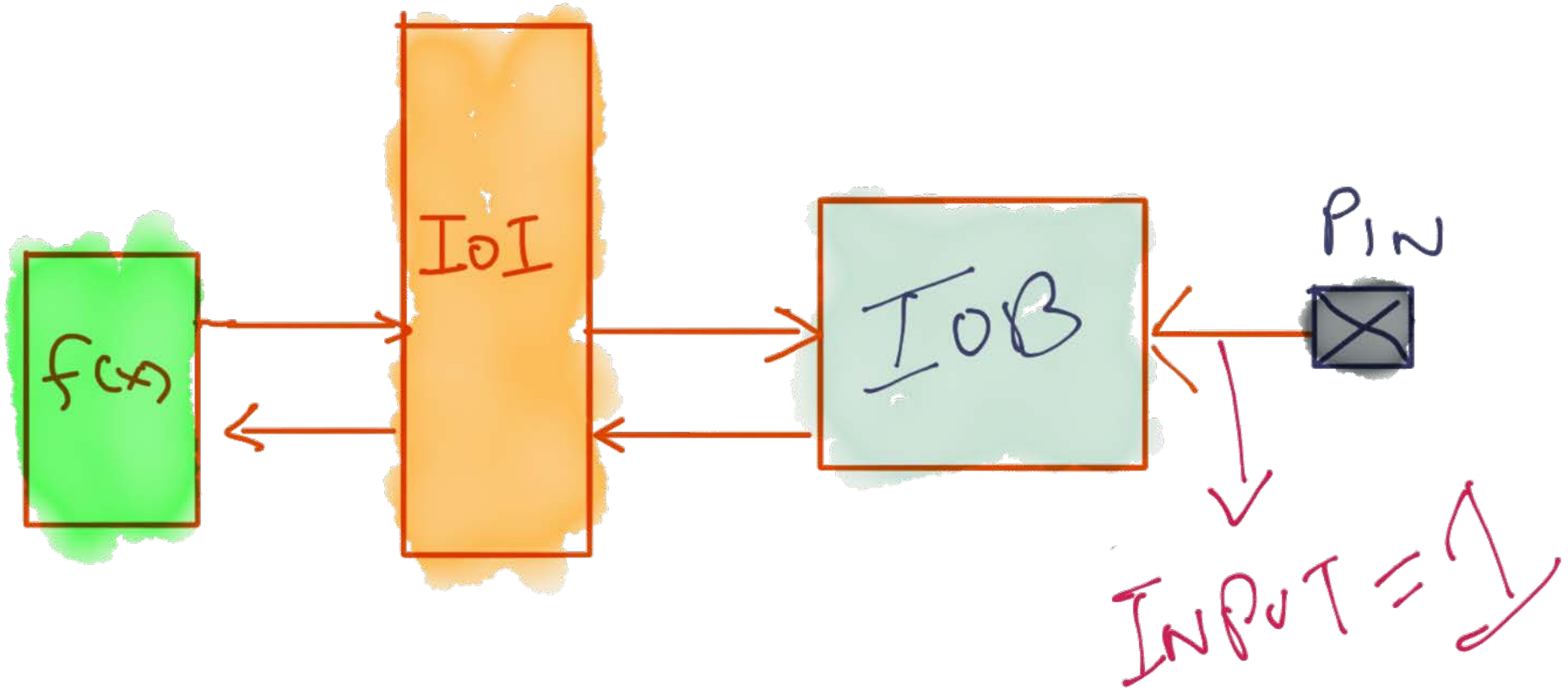
IOB Modification Scenarios



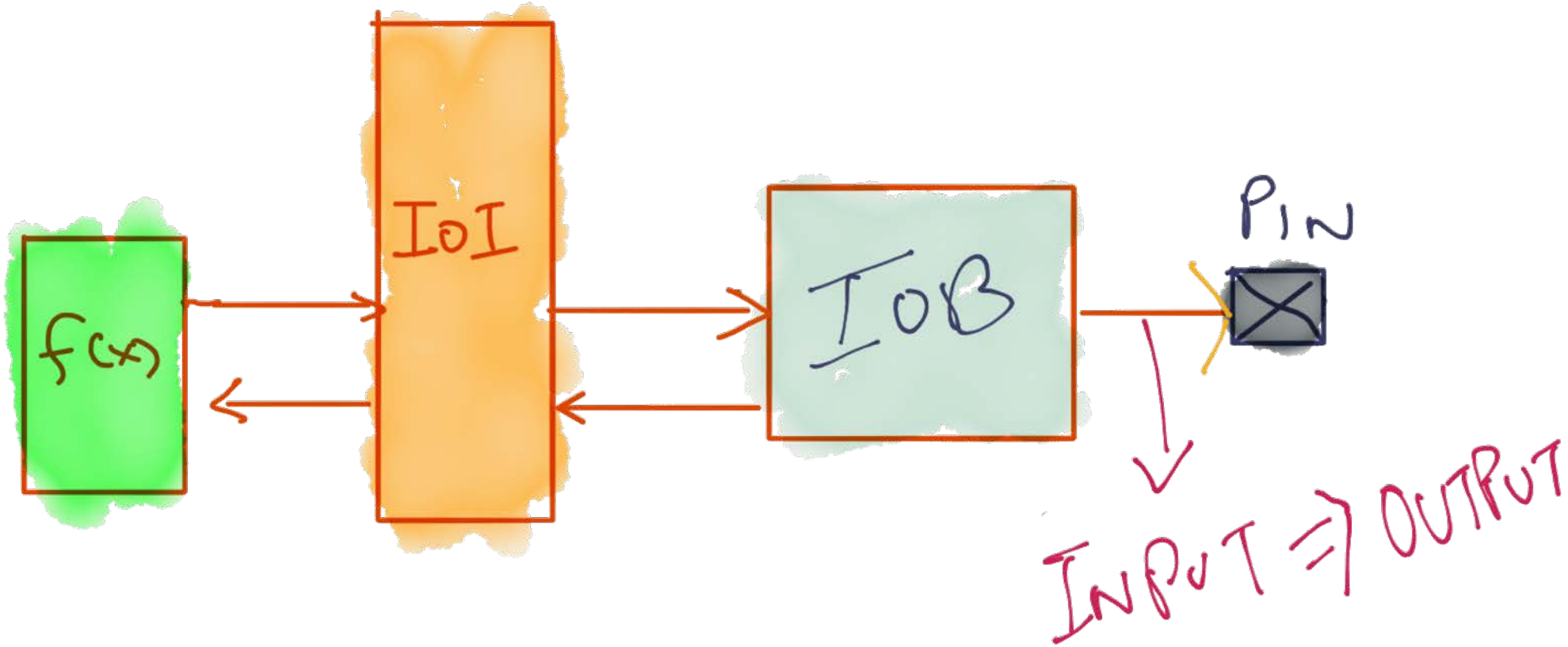
IOB Modification Scenarios



IOB Modification Scenarios

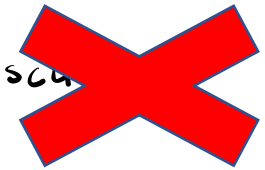


IOB Modification Scenarios



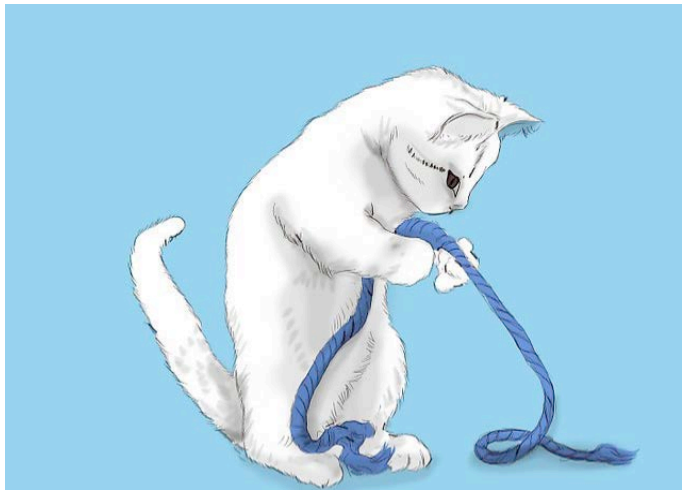
FPGA SECURITY??

FPGA Security through Obscu



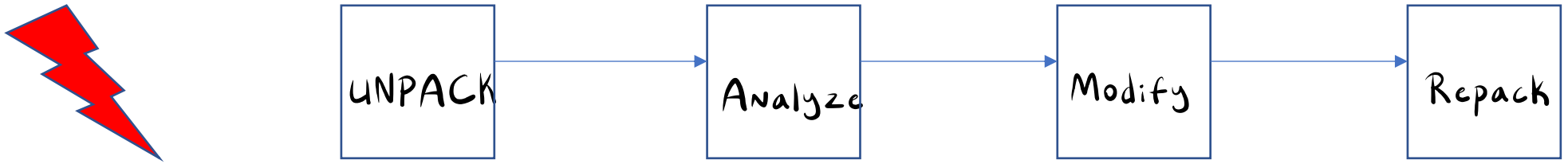
RTL RECONSTRUCTION

CHANGING IO



BITSTREAM REVERSING

BADFET



CONFIDENTIALITY
HuH!!

- Side Channel Analysis

CONFIDENTIALITY
HuH!!

- Side Channel Analysis

- Fault Injection

CONFIDENTIALITY
HuH!!

- Side Channel Analysis
- Fault Injection
- Photon Emission Analysis

Development Board

Spartan SP605

UNPACK

UNPACK
Configuration REGS

- www.xilinx.com/support/documentation/user_guides/ug380.pdf

UNPACK
Algo

- www.xilinx.com/support/documentation/user_guides/ug380.pdf
- Unpack:
  - Find SYNC WORD
  - IDCODE
  - CTL
    - Check Encryption
  - Find CMD:
    - WCFG
  - FDRI
  - DESYNC

Analyze

Configuration Frame Types

- Type 0 – Configuration Logic

Configuration Frame Types

- Type 0 – Configuration Logic
- Type 1 – BRAM

Configuration Frame Types

- Type 0 – Configuration Logic
- Type 1 – BRAM
- Type 2 – IOB (IO interface)

DEVICE LAYOUT

- 1 FRAME = 130 bytes

DEVICE LAYOUT

- 1 FRAME = 130 bytes

- 2d structure (SRAM-based FPGA)
  - ROW x COL(MAJOR x MINOR)

DEVICE LAYOUT

- 1 FRAME = 130 bytes
- 2d structure (SRAM-based FPGA)
  - ROW x COL(MAJOR => MINOR)
- Find Major info for the fpga device

DEVICE LAYOUT

- 1 FRAME = 130 bytes
- 2d structure (SRAM-based FPGA)
  - ROW x COL(MAJOR => MINOR)
- Find Major info for the fpga device
- Find Minor info for each MAJOR

Spartan6-LX9 CLB Layout

FPGA Visualizer

> XilinxBitstream > XilinxPackets > XilinxPacket > XilinxFdriPayload > XilinxFdriLogicBlock > XilinxFdriLogicRow > LClb > XilinxFdriLogicFrame

Info

Type
XilinxFdriLogicFrame

Size
0x82 bytes

Status
Packed

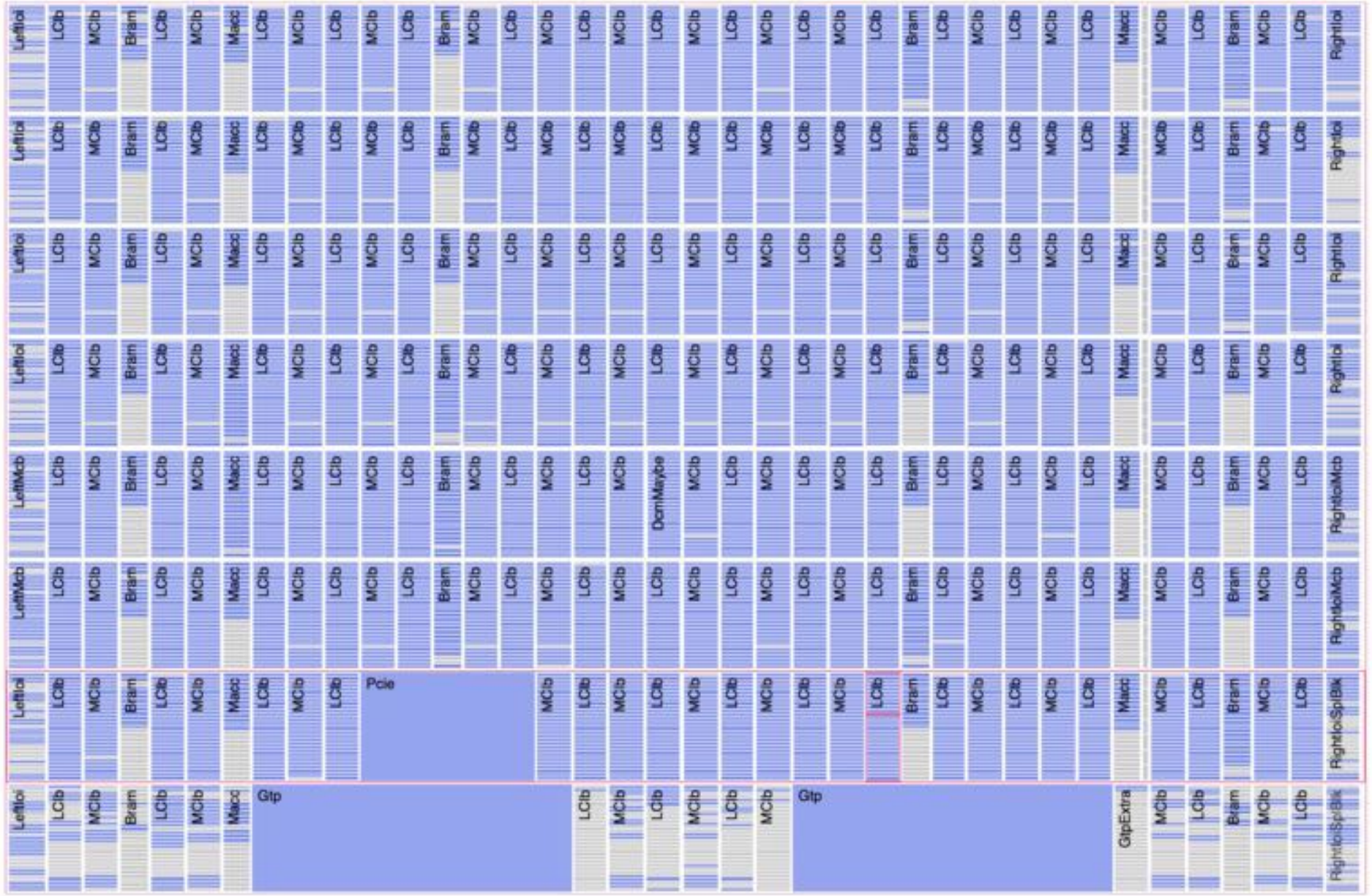
Empty
False

Children
Leaf

Description
Directional Wire Switchbox

Bytes

```
0ef7f8  21 00 11 00 00 00 00 00  !.......
0ef800  00 84 00 00 00 00 00 00  ........
0ef808  00 00 00 00 00 00 00 00  ........
0ef810  00 00 10 c0 00 a0 00 a0  ........
0ef818  00 40 00 00 00 00 00 00  .@......
0ef820  00 00 00 00 02 00 00 00  ........
0ef828  02 80 00 11 00 00 00 00  ........
0ef830  00 00 00 02 00 40 00 00  .....@..
0ef838  00 00 00 00 00 00 00 00  ........
0ef840  00 00 00 00 00 00 00 00  ........
0ef848  00 00 00 00 00 00 00 00  ........
0ef850  00 00 00 00 00 00 00 00  ........
0ef858  20 80 00 00 02 00 00 21   ......!
0ef860  00 00 00 00 00 00 00 00  ........
0ef868  00 09 90 84 00 00 00 00  ........
0ef870  00 00 90 02 00 00 00 00  ........
```



GET_IOB_Encoding

- Bitstream Layout:
  - Logic + BRAM + IOB
  - Determine Range of IOB_FRAMES

GET_IOB_Encoding

- Bitstream Layout:
  - Logic + BRAM + IOB
  - Determine Range of IOB_FRAMES

- For i (0 to #_PINS)
  - For j in PIN_CHARACTERISTIC
    - Y = GEN_BITS(ij_PIN_enable)
    - Z = GEN_BITS(Ij_pin_disable)
    - X = (y XOR Z) in IOB_RANGE

Modify

MODIFY

- IOB_MODIFY
  - Modify Extracted IOB Characteristics
  - Although setting pin=1 is tricky
    - User exercise

REPACK

REPACK

- 22 bit CRC FOR SEU

REPACK

- 22 bit CRC FOR SEU

- Propreitary Algorithm
  - Skips bunch of registers

REPACK

- 22 bit CRC FOR SEU
- Propreitary Algorithm
  - Skips bunch of registers
- CRC Mismatch
  - CRCERRORPIN => HIGH

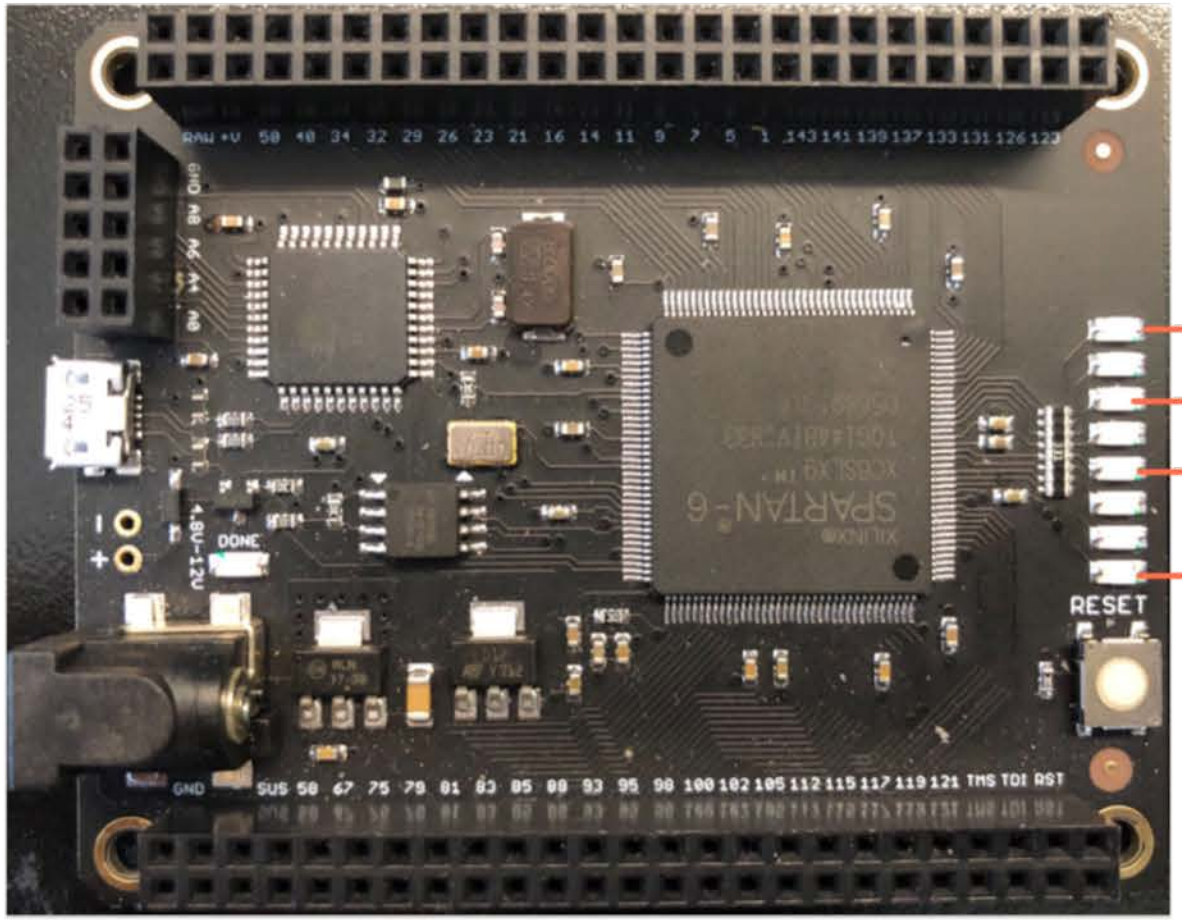
REPACK

- 22 bit CRC FOR SEU
- Propreitary Algorithm
  - Skips bunch of registers
- CRC Mismatch
  - CRCERRORPIN => HIGH
- Encrypt!!

REPACK

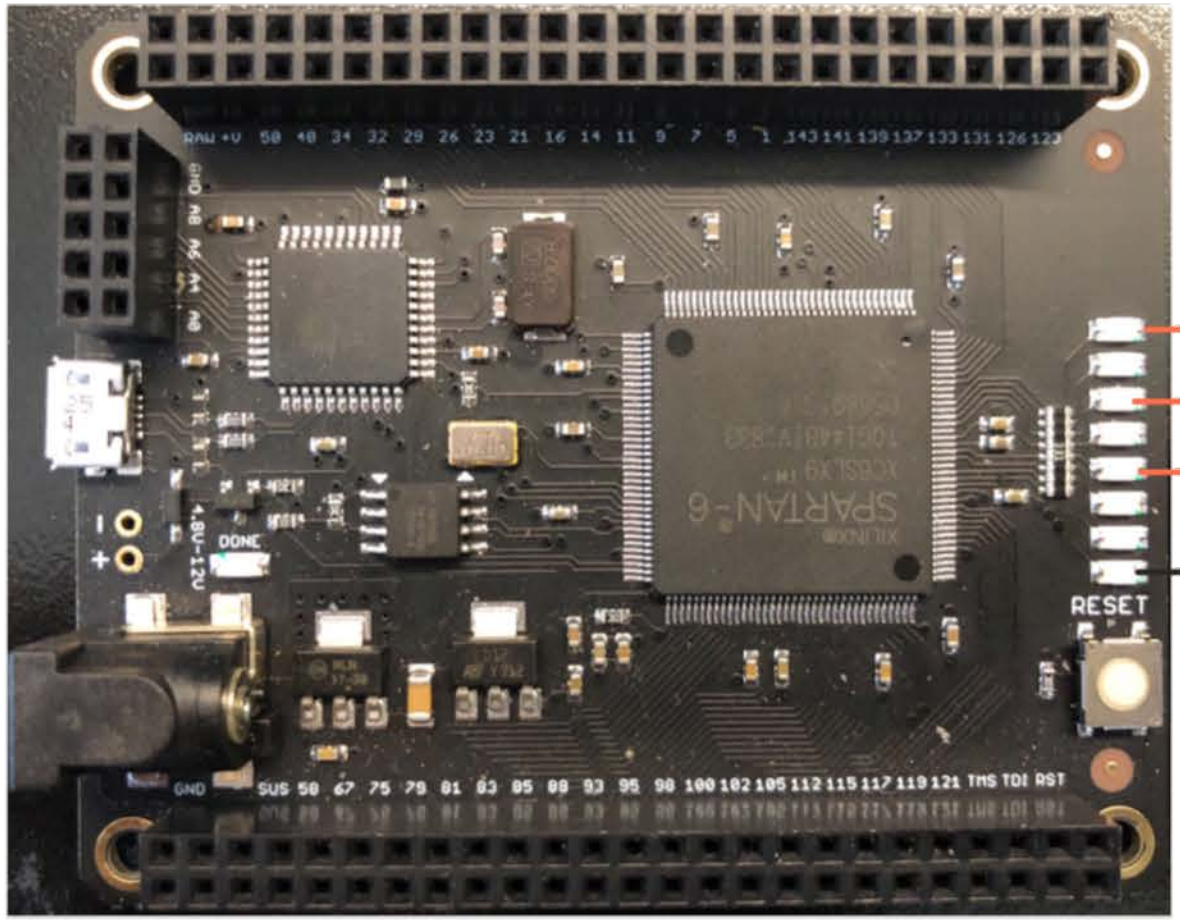
- May Be disable crc
  - Configuration Option Register (COR1)
  - CRC_BYPASS enable

MOJO Demo



SPARTAN6 - LX9

MOJO Demo


P134
P132
P127
P123
TURN OFF
RESET
DONE
SPARTAN-6
SPARTAN6-LX9

DEMO

- DEMO of the open source tool to disable any pin

PWN THE PIN
PWN THE ASR

WHICH FPGA PIN

- JTAG SCANCHAIN

WHICH FPGA PIN

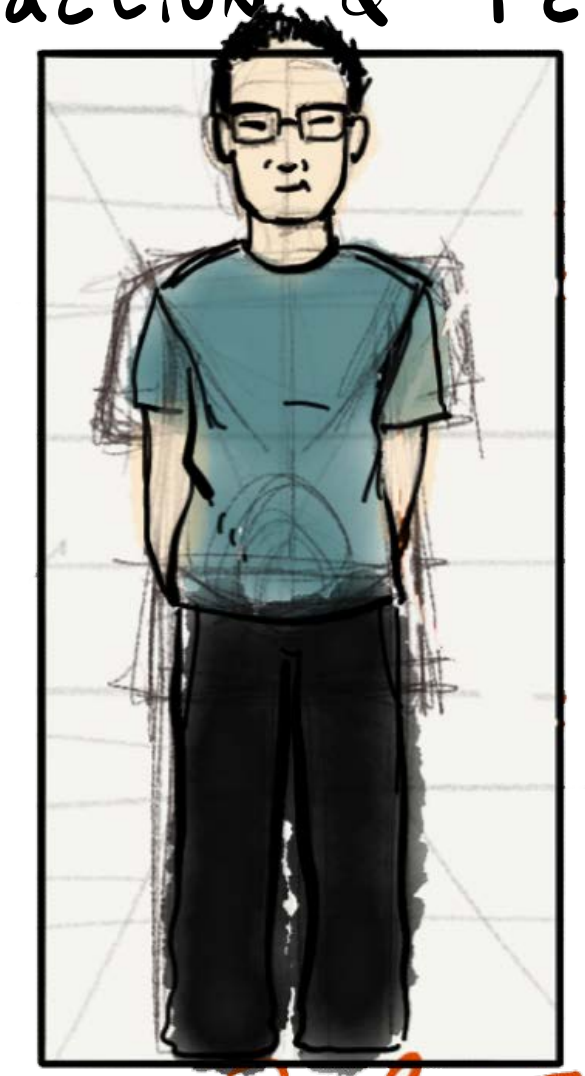
- JTAG SCANCHAIN

- Found state change in 10 pins

Automated Bitstream Extraction & Testing ASR 1001-X

Automated Bitstream Extraction & Testing

- Worst case scenario: Test 296 pins



B.R.I.A.N

PWNED THE PIN
PWNED THE ASR

How to do it remotely

How to do it remotely

- CPLD driver allows an upgrade of the FPGA bitstream.

How to do it remotely

- CPLD driver allows an upgrade of the FPGA bitstream.

- Hijacked a driver "quack.ko" & updated the spi flash containing the FPGA bitstream

How to do it remotely

- CPLD driver allows an upgrade of the FPGA bitstream.
- Hijacked a driver "quack.ko" & updated the spi flash containing the FPGA bitstream
- Need ROOT!!

Get ROOT!

- Wrote protocol fuzzers to do fuzzing
  - SNMP
  - RIP
  - DHCP
  - OSPF
  - BGP


Get ROOT!
LUA IS
EASY
TO HACK

CVE-2019-1862

Get ROOT!

CVE-2019-1904

FINAL COST

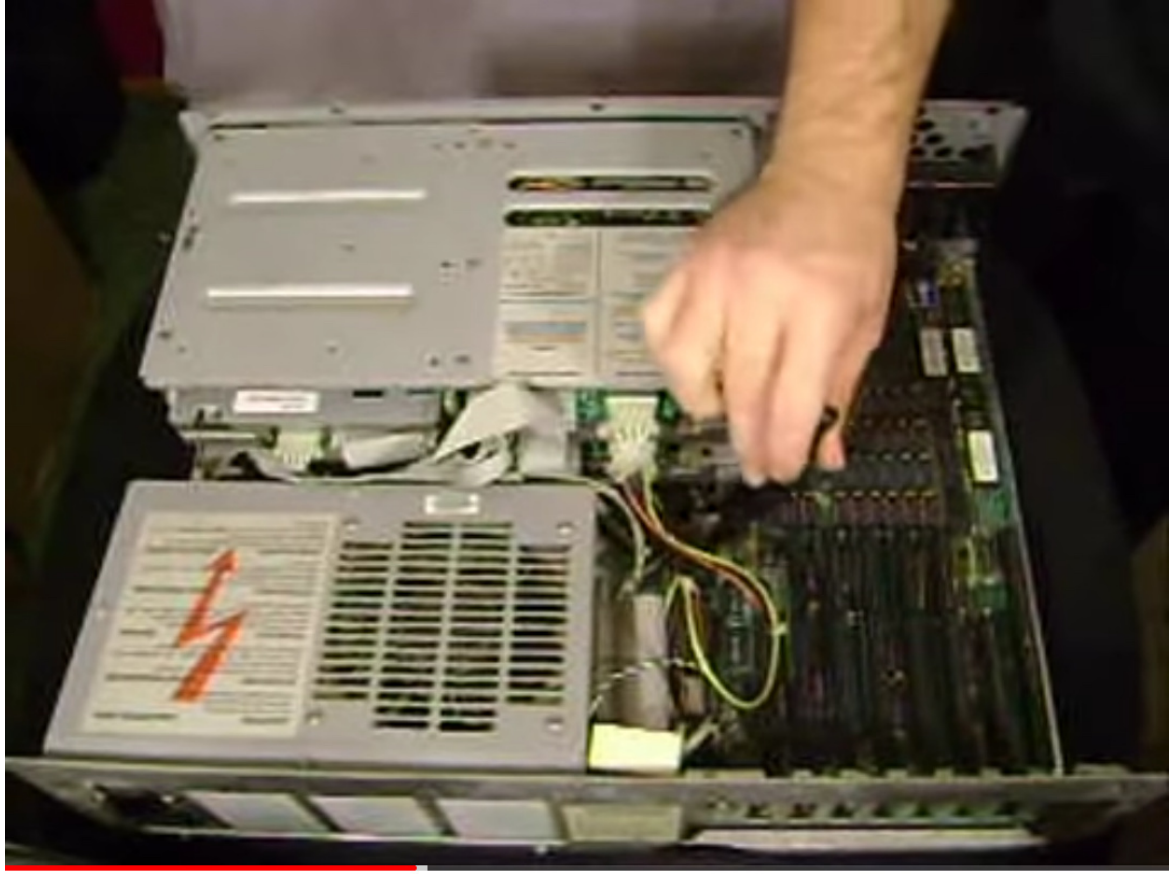
- -$30k
  - -$10K Sacrifice for Analysis
  - -$10K RESET pull high $1/1Ω
  - -$10K Testing Cost

FINAL COST

- -$~~3~~ -$40k
  - -$10K Sacrifice For Analysis
  - -$10K RESET pull high
  - -$10K Testing cost
  - -$10K LOSS
    - DEMO GODS

Mitigation

CISCO Patch



[ASMR] Field patching an FPGA trust anchor vulnerability (Soft Spoken)

218K views

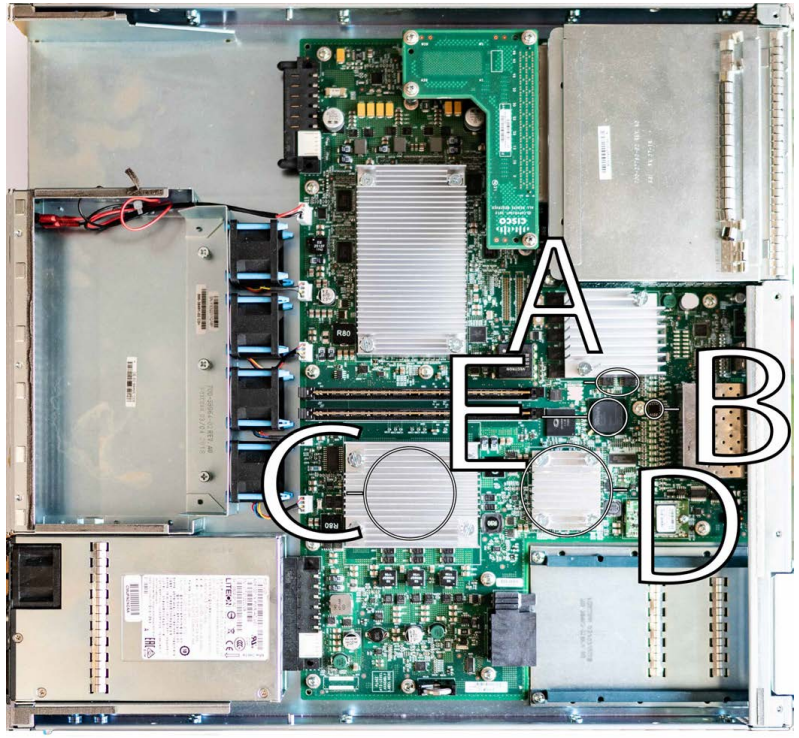
1.4K 66 Share Download Save

LLOYD'S ASMR
19K subscribers

SUBSCRIBE

CISCO Patch

- FPGA v2 forces SPI select line to be low.



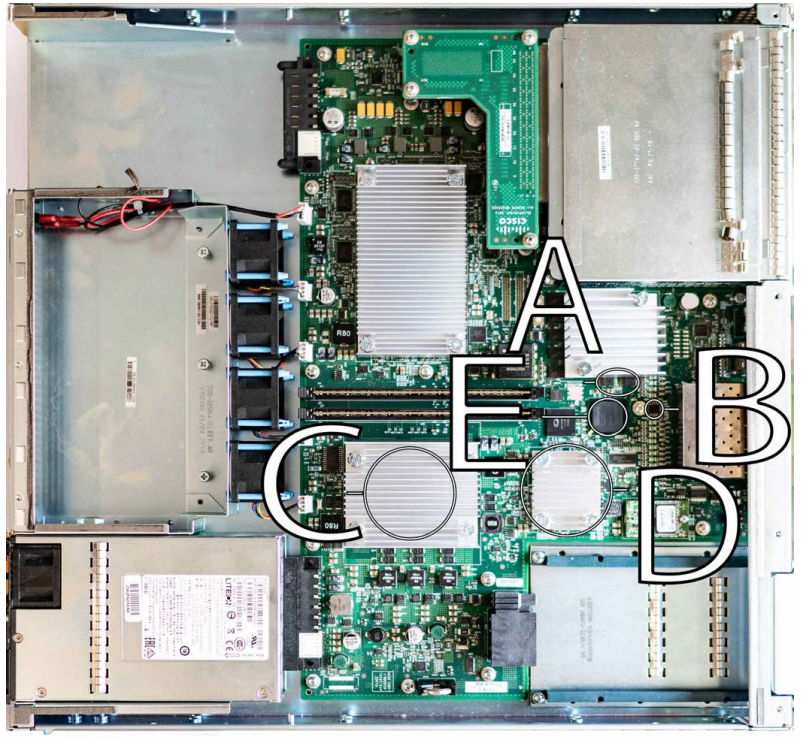
A) Bootloader Flash **B)** FPGA Bitstream SPI Flash **C)** Intel Xeon (Route Processor)

D) Intel Comunications Processor **E)** FPGA (Trust Anchor, other services)

CISCO Patch

- FPGA v2 forces SPI select line to be low.

Still MUTABLE ROOT OF TRUST



A) Bootloader Flash **B)** FPGA Bitstream SPI Flash **C)** Intel Xeon (Route Processor)

D) Intel Comunications Processor **E)** FPGA (Trust Anchor, other services)

Question for VENDORS

- What we need is tool for detection
- Just encrypting the bitstream doesn't work
- Side Channel Attacks defeats that

Our thoughts

- Adding authentication in hw improves the security but still side channel attacks are possible
- In the end whats left is poor hackers down - 40k

Future Work

- Compression/Optimization effects
- Hardware trojans
- Funtenna

Open Source Tool

https://github.com/RedBalloonShenanigans/hal-xilinx

CONTRIBUTIONS

- Rick Housley
- Joseph Pantoga
- James Chambers
- Brian the Intern
- Alex Massonneau
- ATREDIS Partners