

YouTube - The last bastion of Authenticity

HRNOG 2025

Tomaž Zaman

...for now.

Story time.



Elance®
work differently







Purpose.



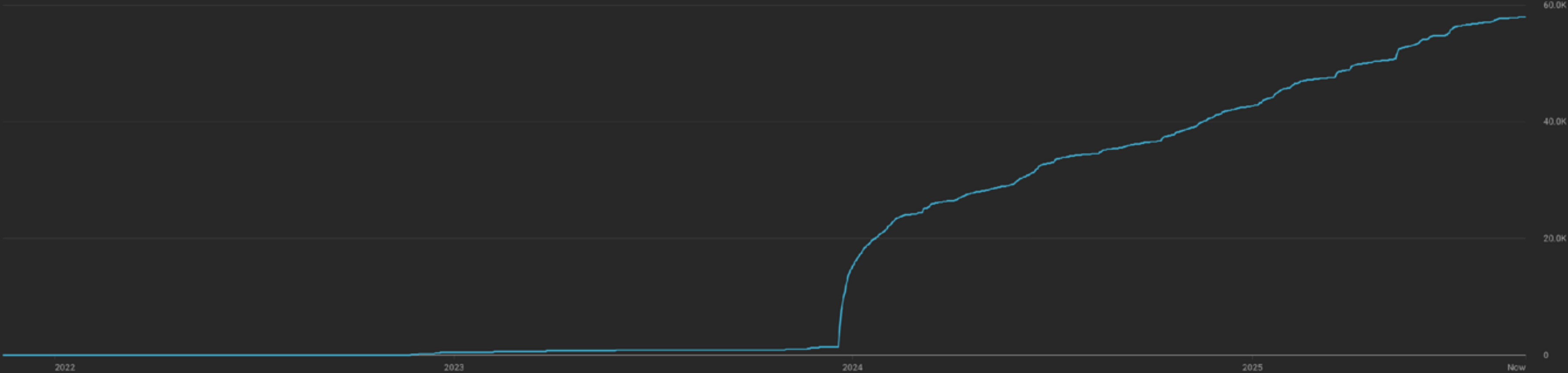


Tomaž Zaman

57,922
Subscribers

Channel growth
Total subscribers

Nov 14, 2021 – Sep 7, 2025
Lifetime





I HACKED my Internet Service Provider's router. So I could get rid of it.



Tomaž Zaman
57.9K subscribers


[Analytics](#)

[Edit video](#)

 54K



 Share

 Promote


 Download





2M views


1 year ago


SLOVENIA


 Part two is up! 🚀 🇸🇮 • [How to HACK your ISP router - step by step.](#)

 Links mentioned in the video: ...more

3,378 Comments  Sort by

- 

Add a comment...
- 

 Pinned by @tomazzaman

@tomazzaman

1 year ago (edited)

Wow. I didn't see this coming. Thanks everyone for kind words of support, i'll do my best to answer to everyone asap, but there are so many of you it'll take me a minute or two. Much love! ❤️ (And for all of you who have subscribed - or are about to - a warm welcome!)



Hi Tomas,

My name is [REDACTED] and I own and operate an ISP, based in the UK.

I have been watching your progress with regard to your router project and would like to invest.

I would like to be a founding investor and would like initially to invest £100,000 sterling into the project.

I would love come visit you guys to discuss your ideas.

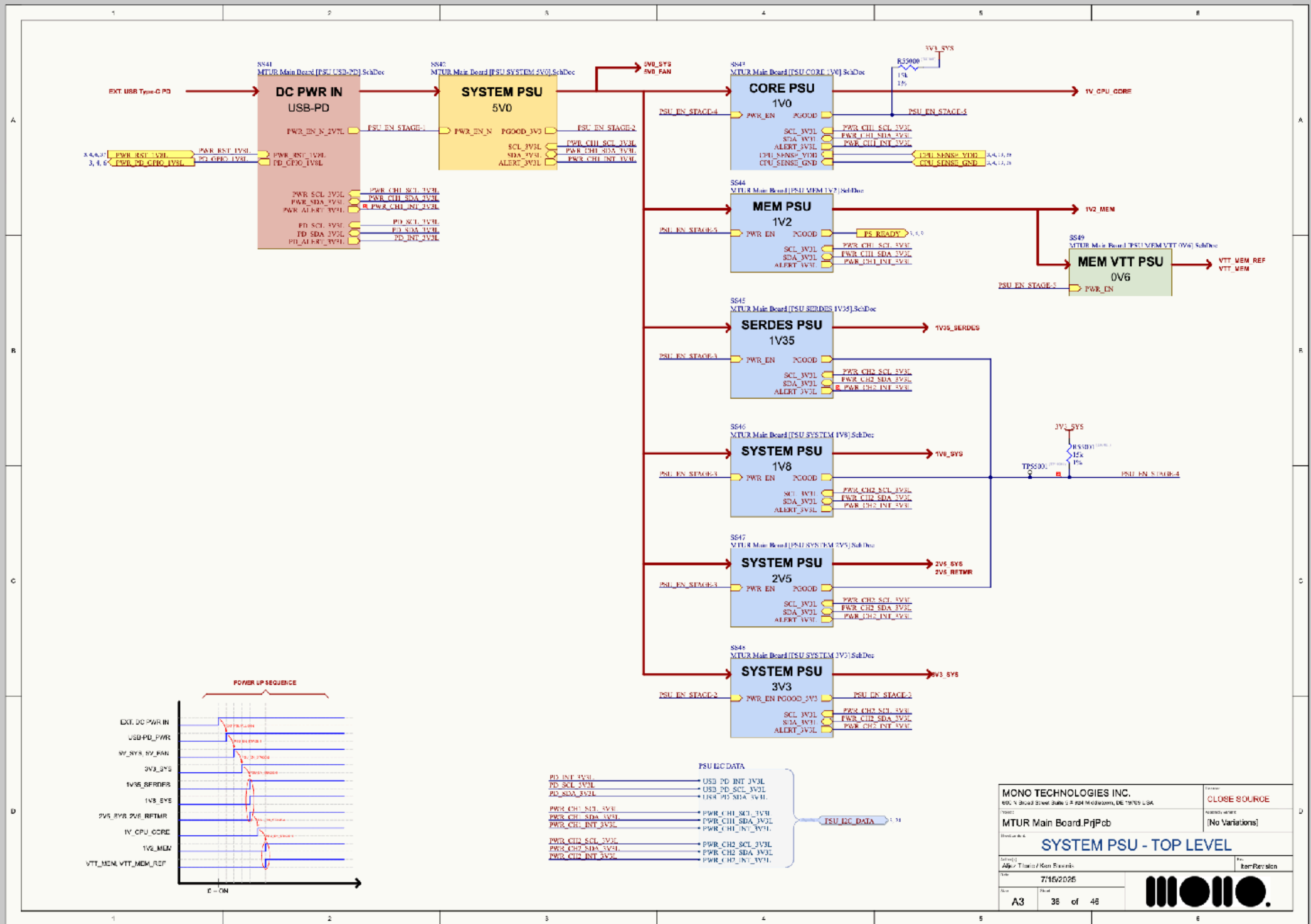
Please advise?

Regards

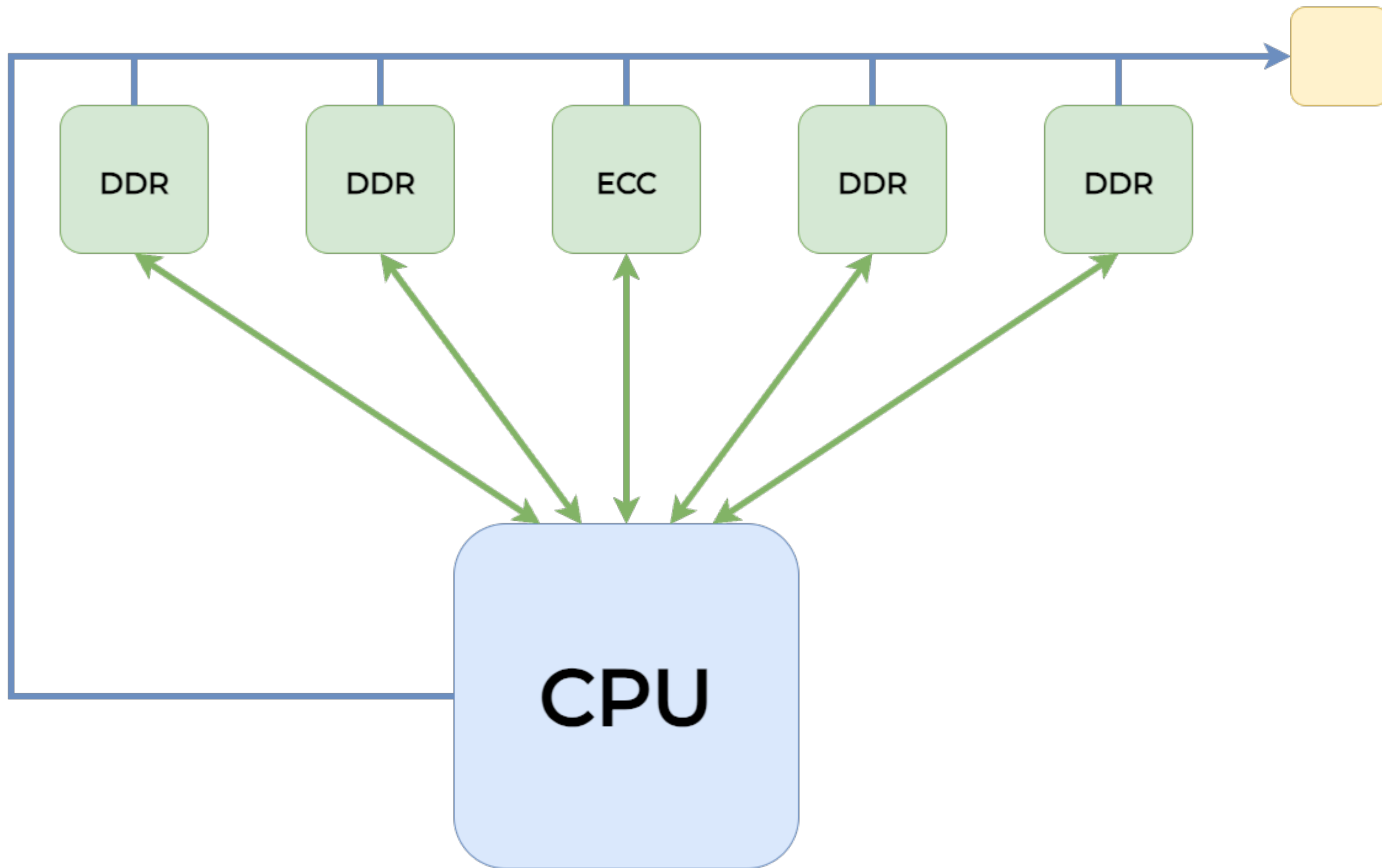
\$300,000



- **Bad power**
- **Bad clock**
- **Bad memory**

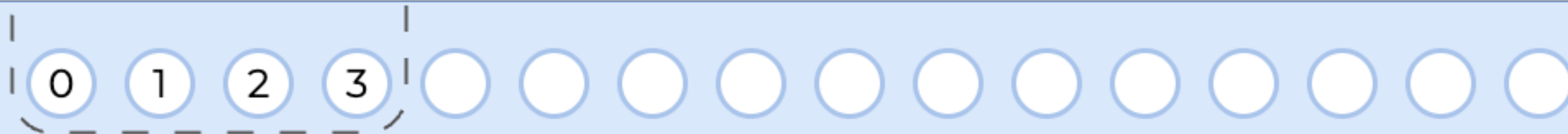


Fly-by topology



A nibble.

DDR chip



CPU

Bit *swizzling*

FileEditNavigateSearchProjectRunProcessor ExpertWindowHelp

Project ExplorerConnections View

Target connections

| Processor | Probe... | Probe A... |
|-----------|----------|------------|
| LS1046A | cvtap | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

ComponentsGatewayDevKit

Generator_Configurations

LS1046A_v1_0_cn

OSs

Processors

LS1046A_v1_0

Components

PBI-1-PBI

PinMux1-PinMux

SerialDevices1-SerDesBlocks

DDR_mc1

Component Inspector - DDR_mc1

PropertiesImportExportValidation

Scenario

Result

Validation stage

Centering the...

Read ODT or

Write ODT or

Operational DD

ResultsChoose Tests

Auto search & detect for write leveling start values

Pass / TotalSearching...01/1

Determine the best clock adjust value

| CLK_ADJ | | | | | | | | | | | | | | | | |
|---------|------|-----|------|-----|------|-----|------|-----|------|-----|-------|-----|-------|-----|-------|-----|
| 0 | 1/16 | 1/8 | 3/16 | 1/4 | 5/16 | 3/8 | 7/16 | 1/2 | 9/16 | 5/8 | 11/16 | 3/4 | 13/16 | 7/8 | 15/16 | 1 |
| 0/1 | 0/3 | 0/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 0/1 |

Determine WRLVL margin per byte lane

| Pass / Total | Lane 0 | Lane 1 | Lane 2 | Lane 3 | Lane 4 | Lane 5 | Lane 6 | Lane 7 | Lane 1 CC |
|--------------|--------|--------|--------|--------|--------|--------|--------|--------|-----------|
| 1/8 clocks | 0/3 | 3/3 | | 0/3 | | | | | |
| 1/4 clocks | 1/3 | 3/1 | 0/3 | 0/1 | | | | | |
| 3/8 clocks | 3/3 | 3/3 | 0/3 | 3/3 | | | | | 0/3 |
| 1/2 clocks | 1/3 | 3/1 | 1/3 | 3/1 | 0/3 | 0/1 | 0/3 | | 0/3 |
| 5/8 clocks | 3/3 | 3/3 | 3/3 | 3/3 | 0/3 | 0/3 | 0/3 | 0/3 | 3/3 |
| 3/4 clocks | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 0/1 | 1/3 |
| 7/8 clocks | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 |
| 1 clocks | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 |
| 9/8 clocks | 3/3 | 0/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 |
| 5/4 clocks | 0/3 | 0/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 |
| 11/8 clocks | 0/3 | | 3/3 | 0/3 | 3/3 | 3/3 | 3/3 | 3/3 | 3/3 |
| 3/2 clocks | | | 0/3 | 0/1 | 1/3 | 3/1 | 1/3 | 3/1 | 1/3 |
| 13/8 clocks | | | 0/3 | | 3/3 | 3/3 | 3/3 | 3/3 | 0/3 |
| 7/4 clocks | | | | | 0/3 | 0/1 | 0/3 | 3/1 | 0/3 |
| 15/8 clocks | | | | | 0/3 | 0/3 | 0/3 | 0/3 | |
| 2 clocks | | | | | | | | | 0/1 |
| 17/8 clocks | | | | | | | | | |
| 9/4 clocks | | | | | | | | | |
| 19/8 clocks | | | | | | | | | |
| 5/2 clocks | | | | | | | | | |
| 21/8 clocks | | | | | | | | | |
| 11/4 clocks | | | | | | | | | |
| 23/8 clocks | | | | | | | | | |
| 6/2 clocks | | | | | | | | | |
| 25/8 clocks | | | | | | | | | |
| 13/4 clocks | | | | | | | | | |
| 27/8 clocks | | | | | | | | | |

Legend: L

SummaryLogs Scripts

Test results

Passed 1 (100.0%)Failed 0 (0.0%)Queued 0 (0.0%)Skipped 0 (0.0%)

| Script | Run | Result | Fail reason |
|----------------|-----|--------|-------------|
| WRLVL START... | 1 | Passed | |

Updated configuration registers

| Name | Value |
|------|-------|
|------|-------|

Live capture registers

Script: WRLVL_START Searcher

Run: 1

| Name | Value | Details |
|--------------|------------|-------------------|
| > ERR_SUI | 0x00010... | Single-Bit ECC... |
| > ERR_INT_N | 0x00000... | Memory error... |
| > ERR_DISAB | 0x00000... | Memory error... |
| > ERR_DIT_C | 0x00000... | Memory error... |
| > CAPTURE_X1 | 0x00000... | Memory error... |
| > CAPTURE_C | 0x00000... | Memory data... |
| > CAPTURE_D | 0x00000... | Memory data... |

Configuration Registers

DDR Controller 1

| Reg. name | Init. value | After reset |
|-----------------------------|-------------|-------------|
| > Peripheral registers | | |
| > DDR1 CS0 BND | 000001FF | 00000000 |
| > DDR1 CS1 BND | 00000000 | 00000000 |
| > DDR1 CS2 BND | 00000000 | 00000000 |
| > DDR1 CS3 BND | 00000000 | 00000000 |
| > DDR1 CS0 CONF | 80810512 | 00000000 |
| > DDR1 CS1 CONF | 00000000 | 00000000 |
| > DDR1 CS2 CONF | 00000000 | 00000000 |
| > DDR1 CS3 CONF | 00000000 | 00000000 |
| > DDR1 CS0 CONF 2 | 00000000 | 00000000 |
| > DDR1 CS1 CONF 2 | 00000000 | 00000000 |
| > DDR1 CS2 CONF 2 | 00000000 | 00000000 |
| > DDR1 CS3 CONF 2 | 00000000 | 00000000 |
| > DDR1 TIMING CFG 3 | 125D1100 | 00000000 |
| > DDR1 TIMING CFG 0 | FF770018 | 00110005 |
| > DDR1 TIMING CFG 1 | 020E1265 | 00000000 |
| > DDR1 TIMING CFG 2 | 005951A0 | 00000000 |
| > DDR1 DDR SDRAM CFG | 65240008 | 07000000 |
| > DDR1 DDR SDRAM CFG 2 | 00401010 | 00000000 |
| > DDR1 DDR SDRAM MODE | 01010834 | 00000000 |
| > DDR1 DDR SDRAM MODE 2 | 00100000 | 00000000 |
| > DDR1 DDR SDRAM MD CNTL | 00000000 | 00000000 |
| > DDR1 DDR SDRAM INTERVAL | 1FFE07FF | 00000000 |
| > DDR1 DDR DATA INIT | DEAD8EEF | 00000000 |
| > DDR1 DDR SDRAM CLK CNTL | 02400000 | 02000000 |
| > DDR1 DDR INIT ADDR | 00000000 | 00000000 |
| > DDR1 DDR INIT EXT ADDRESS | 00000000 | 00000000 |
| > DDR1 TIMING CFG 4 | 0000D502 | 00000000 |
| > DDR1 TIMING CFG 5 | 06401400 | 00000000 |
| > DDR1 TIMING CFG 7 | 26G00000 | 00000000 |
| > DDR1 DDR ZO CNTL | 8A090705 | 00000000 |
| > DDR1 DDR WRLVL CNTL | 86750605 | 00000000 |
| > DDR1 DDR SR CNTR | 00000000 | 00000000 |
| > DDR1 DDR SDRAM RCW 1 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM RCW 2 | 00000000 | 00000000 |
| > DDR1 DDR WRLVL CNTL 2 | 05070709 | 00000000 |
| > DDR1 DDR WRLVL CNTL 3 | 00000A08 | 00000000 |
| > DDR1 DDR SDRAM RCW 3 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM RCW 4 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM RCW 5 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM RCW 6 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 3 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 4 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 5 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 6 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 7 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 8 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 9 | 00000500 | 00000000 |
| > DDR1 DDR SDRAM MODE 10 | 08E40000 | 00000000 |
| > DDR1 DDR SDRAM MODE 11 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 12 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 13 | 00000000 | 00000000 |
| > DDR1 DDR SDRAM MODE 14 | 00000000 | 00000000 |

ProblemsPBI Configuration RegistersTarget ConnectionsDisassemblyConsoleMemoryConnection Diagnostics

List of available target configurations, only one can be active at a certain moment

Type filter text

| Board | Device | Connection Det... | Probe | Path |
|--------------|---------|-------------------|-----------------|------|
| GatewayDevKi | LS1046A | USB:00:04:9f:07: | CodeWarrior TAP | |
| LA1575_UB | LA1575 | | CodeWarrior TAP | |
| LS1012A_FRDM | LS1012A | | CodeWarrior TAP | |
| LS1012A_LRWY | LS1012A | | CodeWarrior TAP | |

Configuration details:

Target Configuration Name: GatewayDevKi

Deactivate

Add

Edit

Duplicate

Remove

Export

Import

GatewayDevKit

No editor descriptor for id:org.eclipse.ui.internal.emptyEditor

Details >>

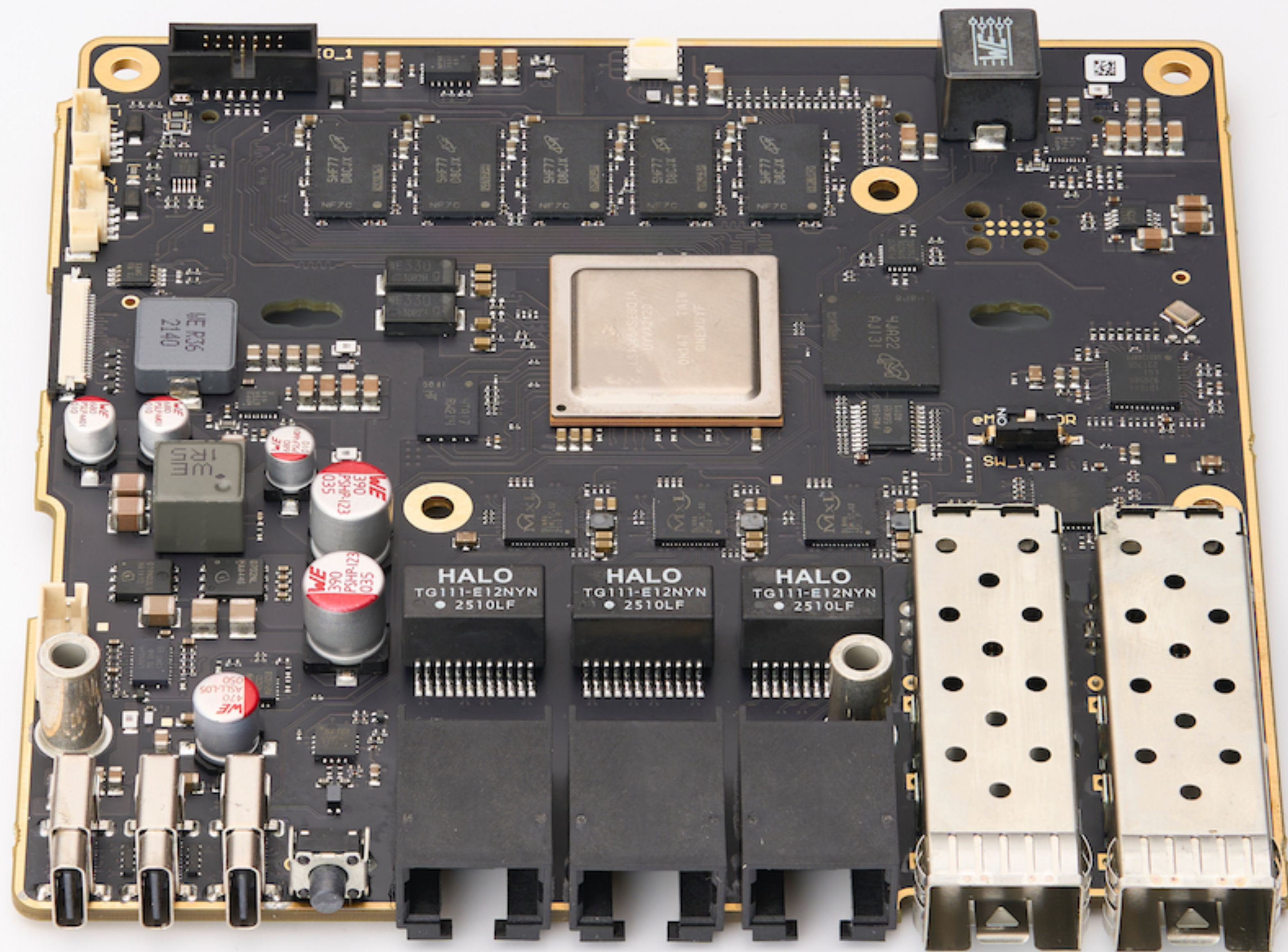
231M of 287M

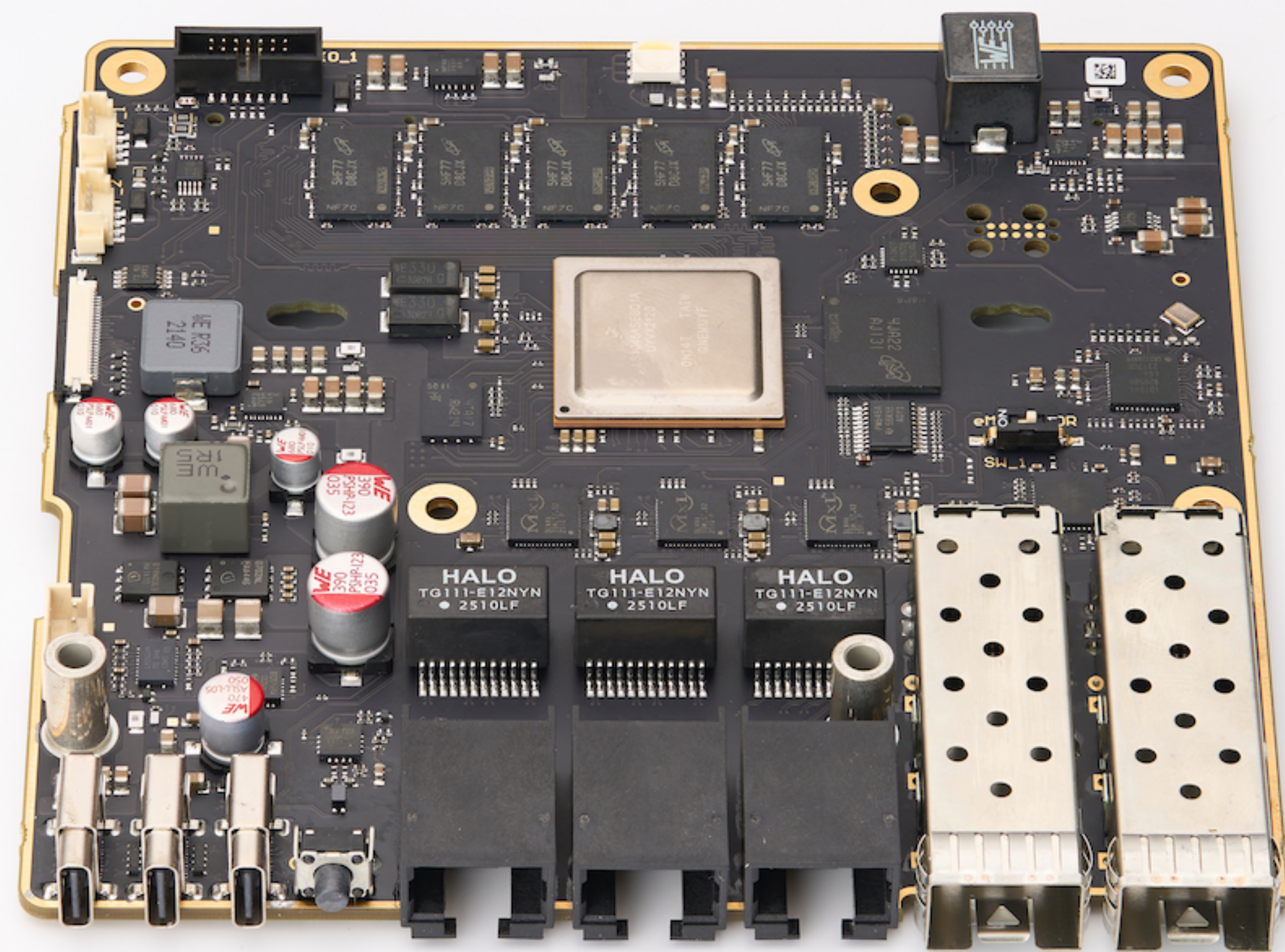
21°C Mostly cloudy

ENG SL

12:43 PM 9/11/2025

\$500,000



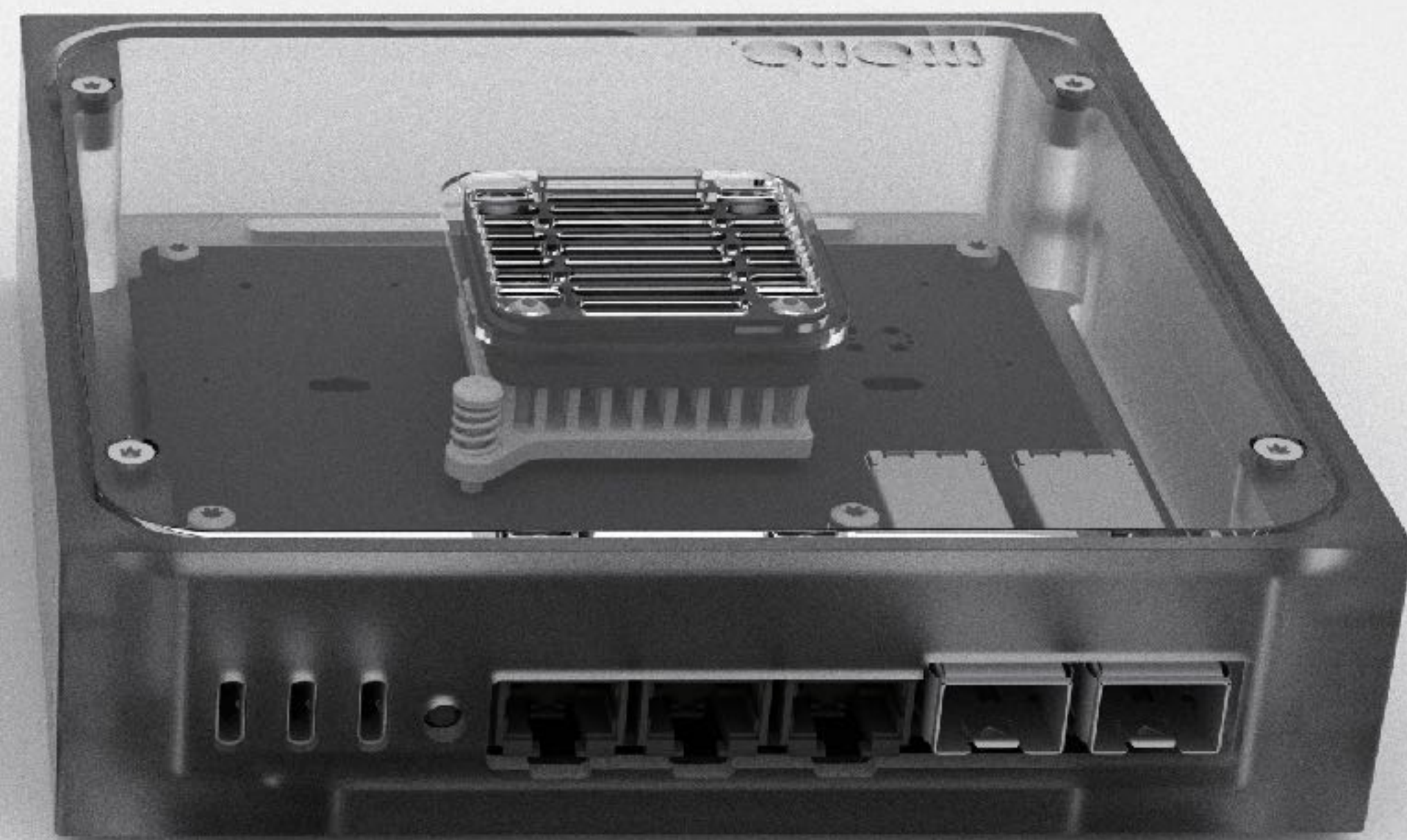
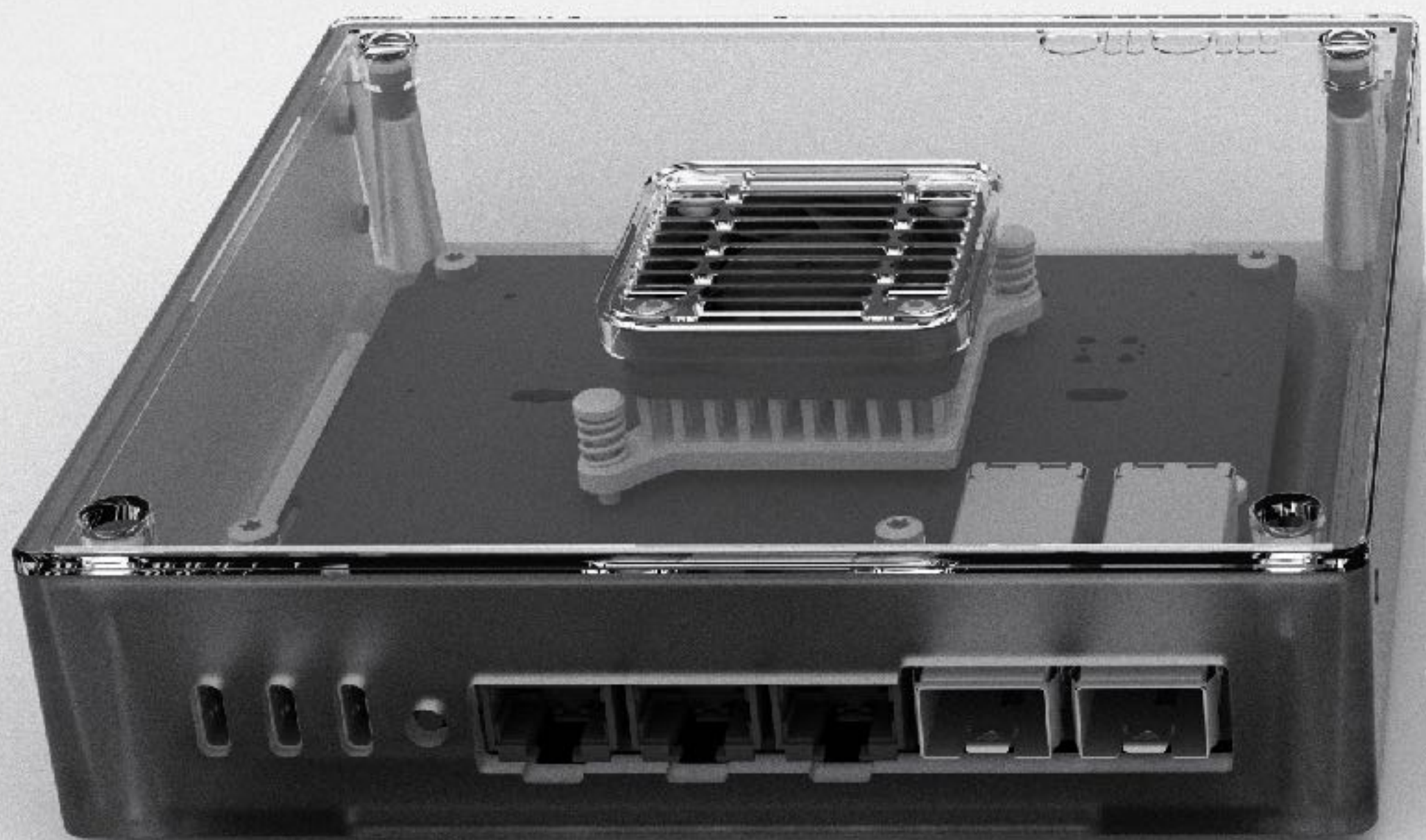



```
screen /dev/tty.usbserial-DK0HCF20 115200

e2fsck          htop          nandflipbits    sulogin          zmore
e2image         hwclock        nandtest        sulogin.util-linux znew
e2mmpstatus     i2cdetect       nandwrite       swapoff

root@recovery:~# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: fm1-mac2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 02:4d:4f:4e:4f:01 brd ff:ff:ff:ff:ff:ff
3: fm1-mac5: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 02:4d:4f:4e:4f:02 brd ff:ff:ff:ff:ff:ff
4: fm1-mac6: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 02:4d:4f:4e:4f:03 brd ff:ff:ff:ff:ff:ff
5: fm1-mac9: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 02:4d:4f:4e:4f:04 brd ff:ff:ff:ff:ff:ff
6: fm1-mac10: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
   link/ether 02:4d:4f:4e:4f:05 brd ff:ff:ff:ff:ff:ff
7: sit0@NONE: <NOARP> mtu 1480 qdisc noop qlen 1000
   link/sit 0.0.0.0 brd 0.0.0.0
root@recovery:~# ip link set fm1-mac2 up
root@recovery:~# ip addr add 10.0.0.90/24 dev fm1-mac2
root@recovery:~# ip route add default via 10.0.0.1 dev fm1-mac2
root@recovery:~# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: seq=0 ttl=59 time=19.234 ms
64 bytes from 1.1.1.1: seq=1 ttl=59 time=16.200 ms
64 bytes from 1.1.1.1: seq=2 ttl=59 time=16.750 ms
64 bytes from 1.1.1.1: seq=3 ttl=59 time=16.869 ms
64 bytes from 1.1.1.1: seq=4 ttl=59 time=18.253 ms
64 bytes from 1.1.1.1: seq=5 ttl=59 time=16.064 ms
64 bytes from 1.1.1.1: seq=6 ttl=59 time=53.825 ms
64 bytes from 1.1.1.1: seq=7 ttl=59 time=18.268 ms
64 bytes from 1.1.1.1: seq=8 ttl=59 time=19.076 ms
^C
--- 1.1.1.1 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 16.064/21.615/53.825 ms
root@recovery:~# _
```

950 preorders!



Thank you!

