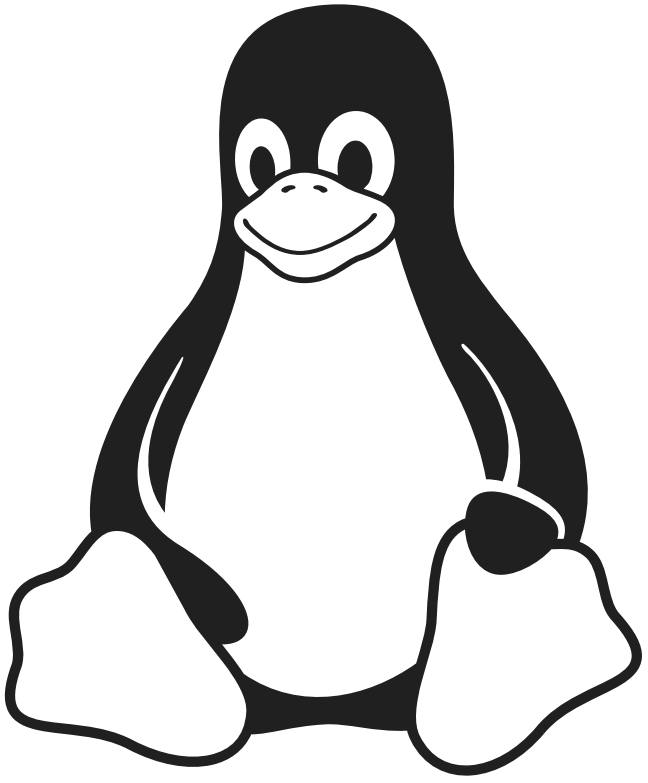
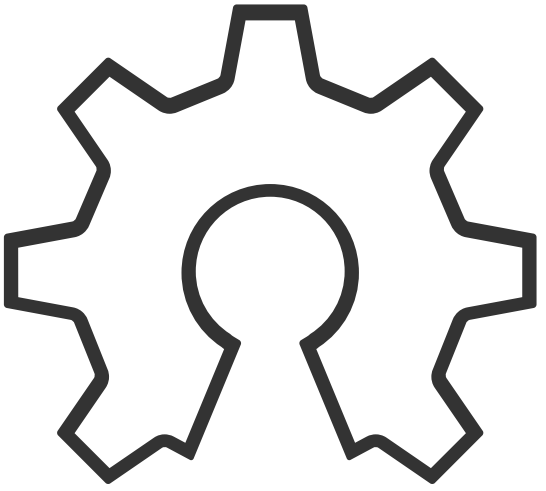
The Road to
Fully Open Hardware
Mobile Computing

Keynote by Lukas F. Hartmann
MNT Research GmbH — https://mntre.com
FSIC2023, Paris

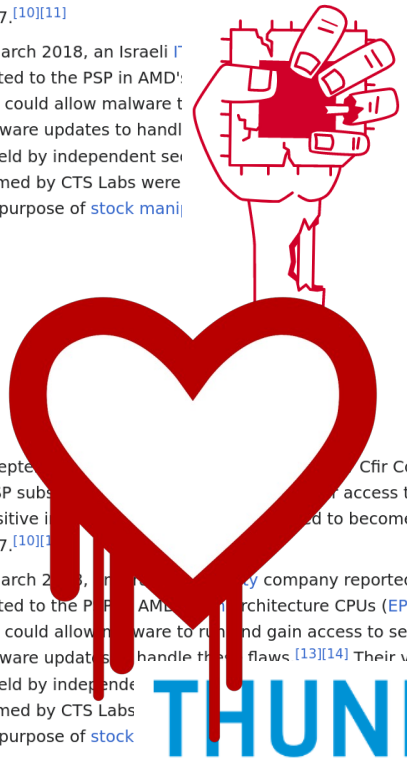




open source
hardware

In September 2017, Google security researcher Cfir Cohen reported a vulnerability to AMD of a PSP subsystem that could allow an attacker access to passwords, certificates, and other sensitive information; a pa
2017.[10][11]

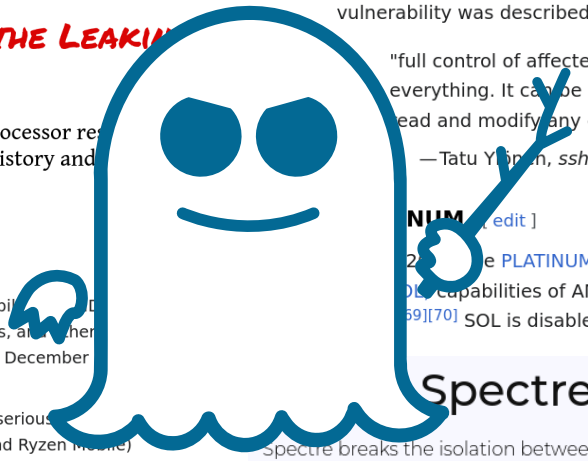
In March 2018, an Israeli I
related to the PSP in AMD'
that could allow malware t
firmware updates to handl
upheld by independent se
claimed by CTS Labs were
the purpose of stock mani



ZombieLoad Attack

Return of the Leakin Dead

Watch out! Your processor re
private browsing-history and
data.



In Septe Cfir Cohen reported a vulnerabil
a PSP subs r access to passwords, certificates, a her
sensitive i d to become available to vendors in December
2017.[10][

In March 2 y company reported a handful of allegedly seriou
related to the P AMD rchitecture CPUs (EPYC, Ryzen, Ryzen Pro, and Ryzen Mobile)
that could allow ware to ru nd gain access to sensitive information.[12] AMD announced
firmware updat handle th flaws.[13][14] Their validity from a technical standpoint was
upheld by indepe
claimed by CTS Labs
the purpose of stock

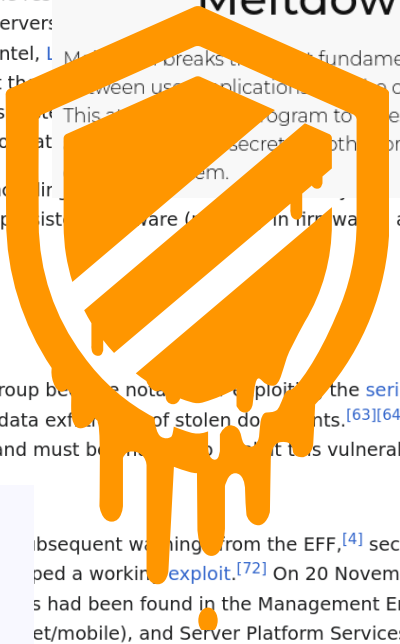
SA-00075 (a.k.a. Silent Bob is Silent) [edit]

In May 2017, Intel confirmed that many computers with AMT have had an unpatched critical privilege escalation vulnerability (CVE-2017-568 [38][51][36][52][53] The vulnerability, which was nicknamed "Silent Bob is Silent" by the res
affects numerous laptops, desktops and server
Hewlett Packard Enterprise and HP Inc.), Intel,
[58][59][60] Those researchers claimed that th
Other reports claimed the bug also affects
vulnerability was described as giving remo at

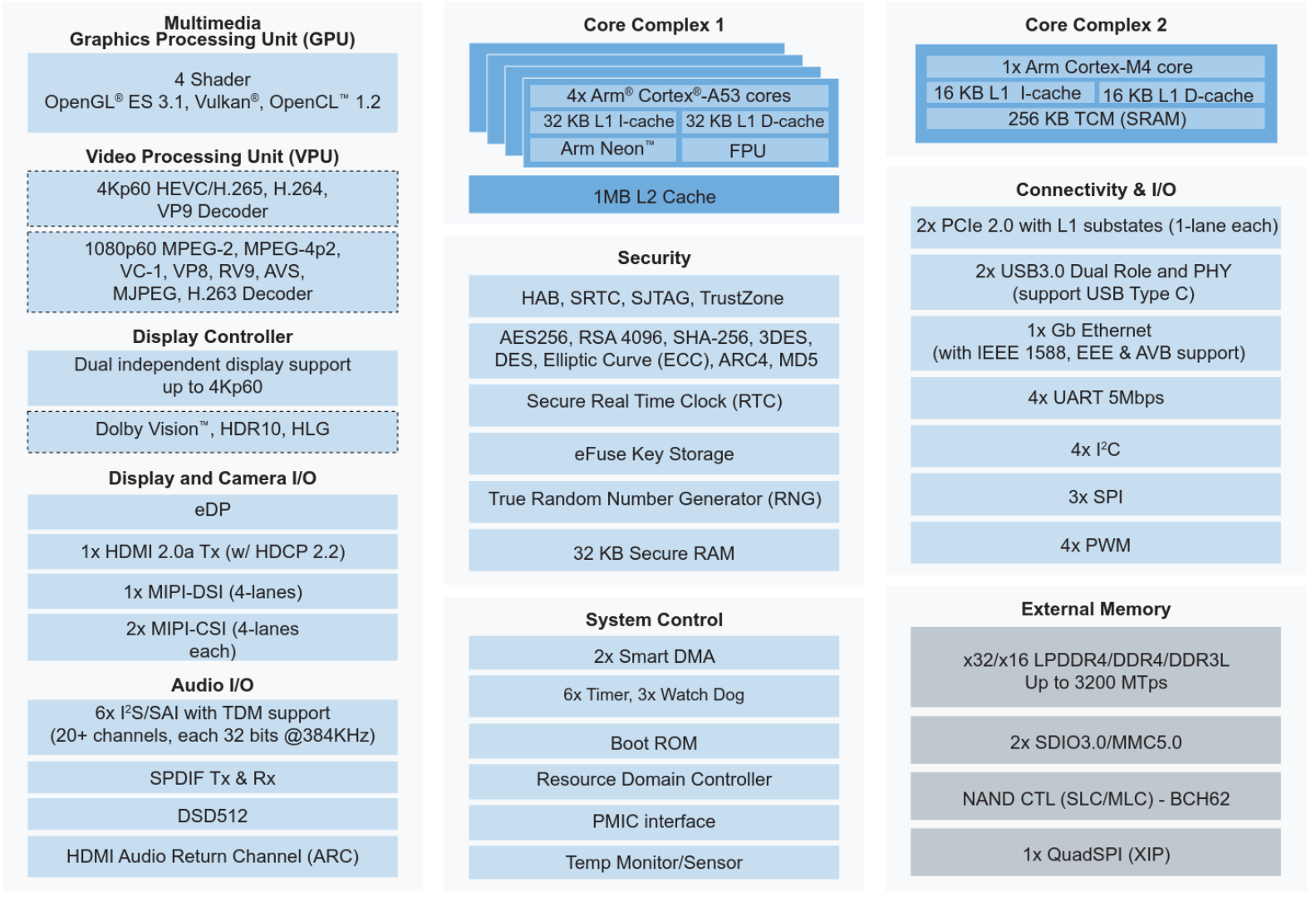
> "full control of affected machines, inc ir
> everything. It can be used to install p ist ware (in firm wa and
> ead and modify any data."
>
> —Tatu Y n, *ssh.com*[54]

NUM [edit]

2 e PLATINUM cybercrime group be e nota exploit the serial over
O capabilities of AMT to perform data exf of stolen do nts.[63][64][65][66]
9][70] SOL is disabled by default, and must b t this vulnerability.[71]



bsequent w ing from the EFF,[4] security firm
ed a workin exploit.[72] On 20 November, 2017
s had been found in the Management Engine
et/mobile), and Server Platform Services (high
firmware update".[73][74] Essentially every Intel-
cluding most desktops and servers, were found
promised, although all the potential routes of
exploitation were not entirely known.[74] It is not possible to patch the problems from the operating system, and a firmware (UEFI, BIOS) update to the motherboard is required, which was anticipated to take quite some time for the many individual manufacturers to accomplish, if it ever would be for many systems.[42]


Multimedia
Graphics Processing Unit (GPU)
4 Shader
OpenGL® ES 3.1, Vulkan®, OpenCL™ 1.2
Video Processing Unit (VPU)
4Kp60 HEVC/H.265, H.264, VP9 Decoder
1080p60 MPEG-2, MPEG-4p2, VC-1, VP8, RV9, AVS, MJPEG, H.263 Decoder
Display Controller
Dual independent display support up to 4Kp60
Dolby Vision™, HDR10, HLG
Display and Camera I/O
eDP
1x HDMI 2.0a Tx (w/ HDCP 2.2)
1x MIPI-DSI (4-lanes)
2x MIPI-CSI (4-lanes each)
Audio I/O
6x I²S/SAI with TDM support (20+ channels, each 32 bits @384KHz)
SPDIF Tx & Rx
DSD512
HDMI Audio Return Channel (ARC)
Core Complex 1
4x Arm® Cortex®-A53 cores
32 KB L1 I-cache
32 KB L1 D-cache
Arm Neon™
FPU
1MB L2 Cache
Security
HAB, SRTC, SJTAG, TrustZone
AES256, RSA 4096, SHA-256, 3DES, DES, Elliptic Curve (ECC), ARC4, MD5
Secure Real Time Clock (RTC)
eFuse Key Storage
True Random Number Generator (RNG)
32 KB Secure RAM
System Control
2x Smart DMA
6x Timer, 3x Watch Dog
Boot ROM
Resource Domain Controller
PMIC interface
Temp Monitor/Sensor
Core Complex 2
1x Arm Cortex-M4 core
16 KB L1 I-cache
16 KB L1 D-cache
256 KB TCM (SRAM)
Connectivity & I/O
2x PCIe 2.0 with L1 substates (1-lane each)
2x USB3.0 Dual Role and PHY (support USB Type C)
1x Gb Ethernet (with IEEE 1588, EEE & AVB support)
4x UART 5Mbps
4x I²C
3x SPI
4x PWM
External Memory
x32/x16 LPDDR4/DDR4/DDR3L Up to 3200 MTps
2x SDIO3.0/MMC5.0
NAND CTL (SLC/MLC) - BCH62
1x QuadSPI (XIP)
Optional Capability

9.4.3 Memory Map and Register Definition

This section includes the DDRC PHY module memory map and detailed descriptions of all registers.

NOTE

Synopsys Proprietary. Used with permission.

13.3.3 Usage Mode

The GPU should be programmed through the NXP provided driver. NXP does not provide support for software that directly programs the GPU registers. APIs for programming the GPU through the software driver are described in separate driver documentation.

Panfrost

Group ID: 1345

FOSS driver for Mali Txxx and Gxx GPUs

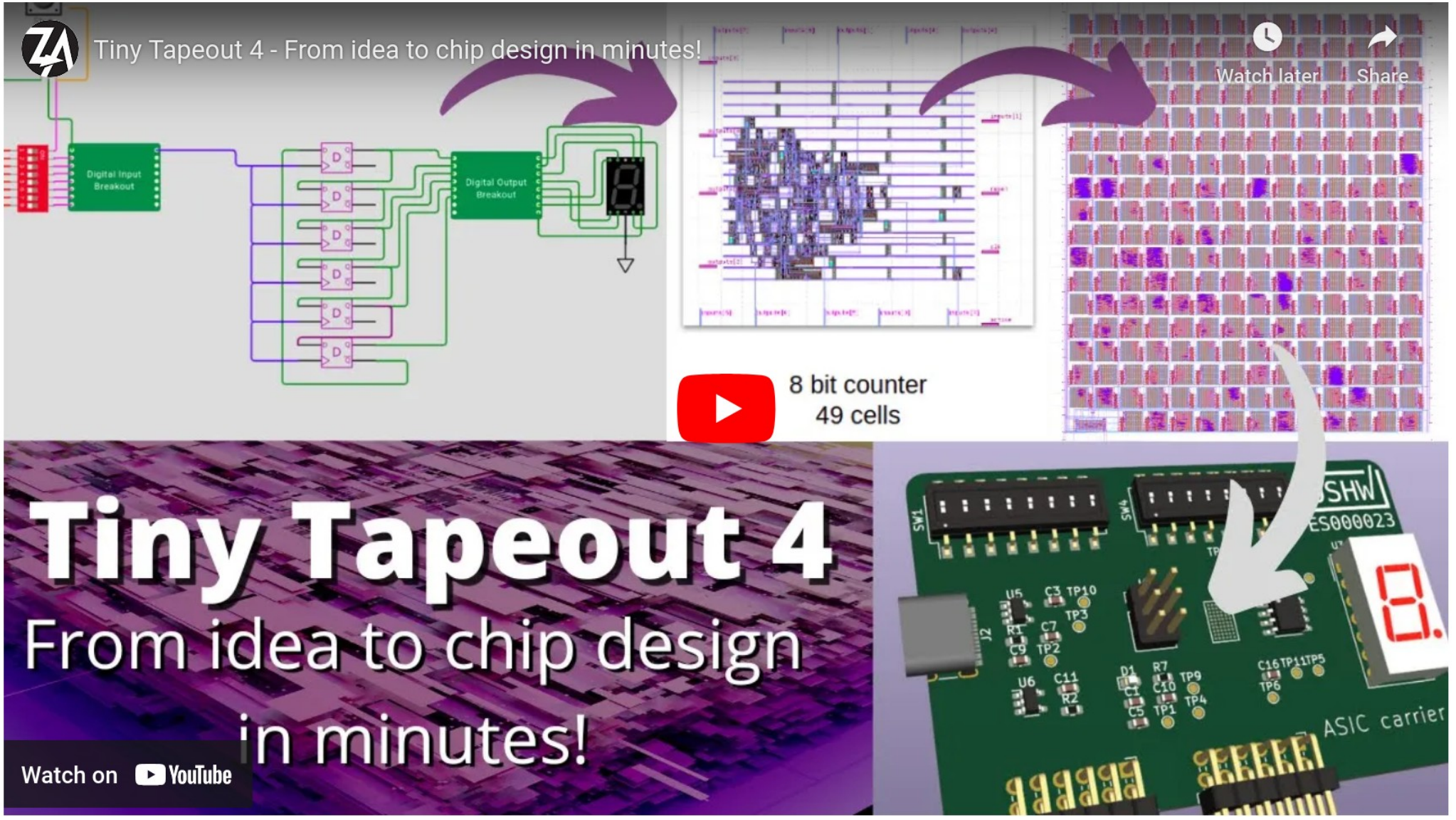
Nouveau: Accelerated Open Source driver for nVidia cards

The **nouveau** project aims to build high-quality, free/libre software drivers for nVidia cards. “Nouveau” [*nuvo*] is the French word for “new”. Nouveau is composed of a Linux kernel KMS driver (nouveau), Gallium3D drivers in Mesa, and the Xorg DDX (xf86-video-nouveau). The kernel components have also been ported to NetBSD.

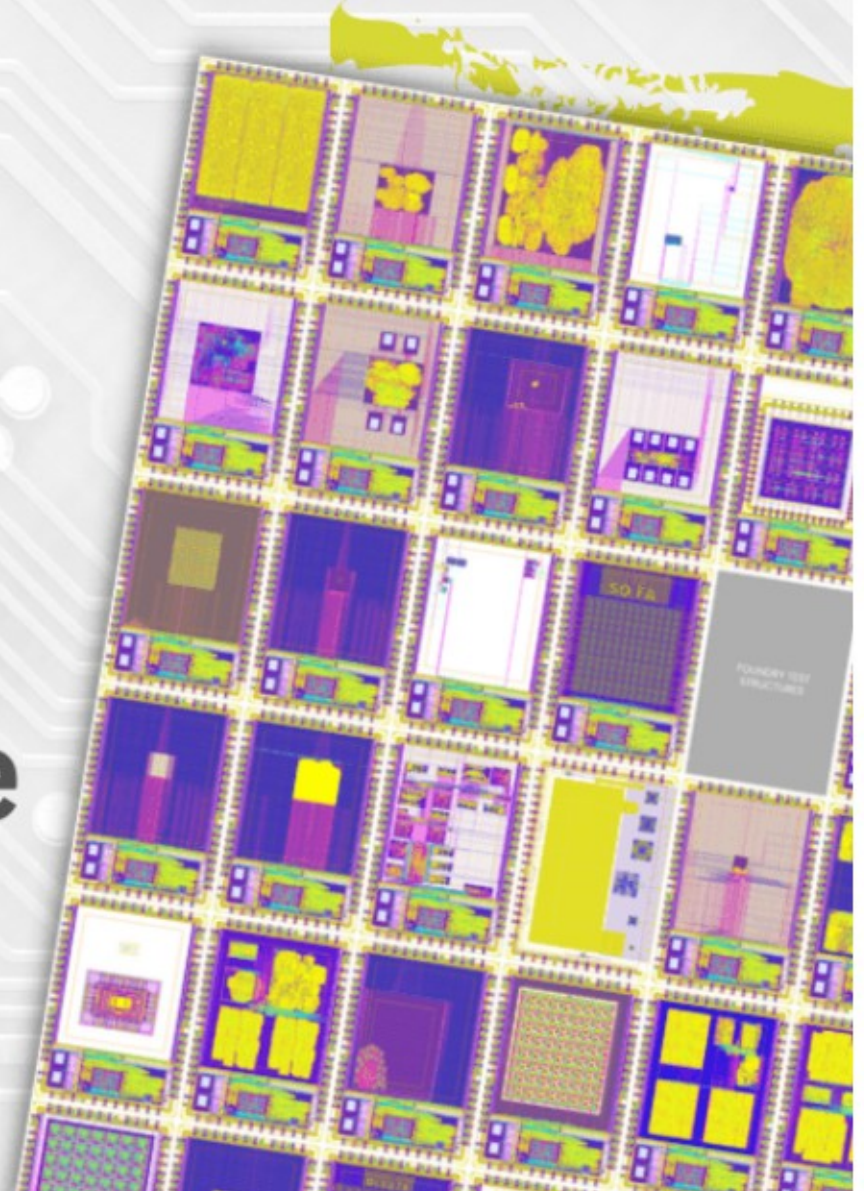
Project Etnaviv is an open source user-space driver for the Vivante GCxxx series of embedded GPUs.

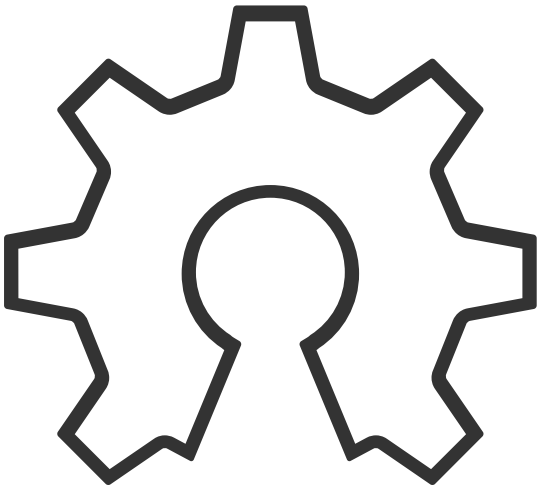
This repository contains reverse-engineering and debugging tools, and `rnndb` register documentation. It is not necessary to use this repository when building the driver.

```
433   if (counter_x >= vga_h_max) begin
434     counter_x <= 0;
435     if (counter_y >= vga_v_max) begin
436       counter_y <= 0;
437       sprite_px <= 0;
438       sprite_py <= 0;
439     end else begin
440       counter_y <= counter_y + 1'b1;
441     end
442   end else begin
443     counter_x <= counter_x + 1'b1;
444   end
445
446   if (counter_x==vga_h_rez) begin
447     if (counter_y<vga_v_rez-1'b1)
448       need_line_fetch <= counter_y + 1'b1;
449     else
450       need_line_fetch <= 0;
451   end
452
453   // signal synchronization point to fetch process
454   if (counter_x<8 && counter_y==vga_v_sync_start)
455     need_frame_sync <= 1;
456   else
457     need_frame_sync <= 0;
458
459   // rasterline interrupt:
460   // - first time on vblank start (1 pixel long)
461   // - second time on report_y (1 pixel long)
462   if (counter_y == vga_v_sync_start || (vga_report_y != 0 && (counter_y == vga_report_y - 1'b1))) begin
463     // i tested the position of the interrupt relative to vdma_init,
464     // there's a wide window where a buffer switch is ok, and
```


Tiny Tapeout 4 - From idea to chip design in minutes!
Watch later
Share
Digital Input Breakout
Digital Output Breakout
8 bit counter
49 cells
Tiny Tapeout 4
From idea to chip design
in minutes!
Watch on YouTube
ASIC carrier

Introducing the GF180 Open MPW Shuttle





open source
hardware

I'm building my own reform!

MNT Reform

jacqueline 1 Feb '22

Hey all!

I got a bit carried away, and now I'm building my own Reform. You might have seen pictures on twitter, but people have been telling me that you fine folks here might like to have some updates as well!

It's no fun to just straight up build the perfectly good, well-designed thing, so I have added my own take on things 🙂

First up, I've replaced the barrel jack input with a USB-C port, and am going to be relying on USB-PD for external power. I'm happy with my schematic and layout for this, and am now just waiting for PCBs from my fab to come back so I can see if it actually works. Here is a rendering of my gay pcb:


MKT BASED
REFORM
lily58


F1
On
F2
Wake
F3
F4
Off
F5
Reset
F6
F7
DFU
F8
F9
RGB
F10
F11
F12
Del
Tab
Q
W
7 <
F
8 $
P
9 >
G
J
L
[
U
_
Y
]
; :
Bksp
A
\
R
4 (
S
5 "
T
6)
D
#
H
%
N
{
E
=
I
}
O
|
Esc
Z
0
X
1 :
C
2 *
V
3 +
B
K
M
&
, !
^
. @
~
/ ?
Enter
Click
Shift
Super
Alt
Ctrl
Num
Shift
Symb
Nav

reform2-keyboard-fw	release version 2023-07-03	Jul 3, 2023, 9:13 PM
reform2-keyboard-lettering/visicut	keyboard-lettering: add v6 qwertz	Nov 1, 2022, 5:44 PM
reform2-keyboard-pcb	keyboard: add WIP R-2D version, atmega RC notes	Jul 21, 2022, 12:17 PM
reform2-keyboard3-pcb	keyboard3 rc snapshot	May 16, 2023, 6:28 PM
reform2-lpc-driver	replace delay with sleep per kernel doc recomendations	Jun 24, 2022, 4:17 PM
reform2-lpc-fw	release version 2023-07-03	Jul 3, 2023, 9:13 PM
reform2-motherboard-pcb	reform2: update PCBs incl. badges to production revs, a...	Jun 10, 2021, 1:20 PM
reform2-motherboard25-pcb	actual MB2.5 snapshot WIP	May 16, 2023, 6:27 PM
reform2-oled-pcb	reform2: update PCBs incl. badges to production revs, a...	Jun 10, 2021, 1:20 PM
reform2-protected-batterypack-pcb	reform2-protected-batterypack production update	May 16, 2023, 6:29 PM
reform2-safety	reform2: update PCBs incl. badges to production revs, a...	Jun 10, 2021, 1:20 PM
reform2-speakers	speakers: updated design for better fit	May 20, 2020, 2:01 PM
reform2-trackball-fw	trackball: dont force send report	Oct 5, 2022, 6:01 PM
reform2-trackball-pcb	reform2: update PCBs incl. badges to production revs, a...	Jun 10, 2021, 1:20 PM
reform2-trackball-sensor-pcb	reform2: update PCBs incl. badges to production revs, a...	Jun 10, 2021, 1:20 PM
reform2-trackball2-fw	trackball2 flash tool: make interactive loop	May 16, 2023, 6:22 PM
reform2-trackball2-pcb	trackball pcb: add v2 with rp2040 mcu	Aug 22, 2022, 3:40 PM

Run

Vol 97% 23:01

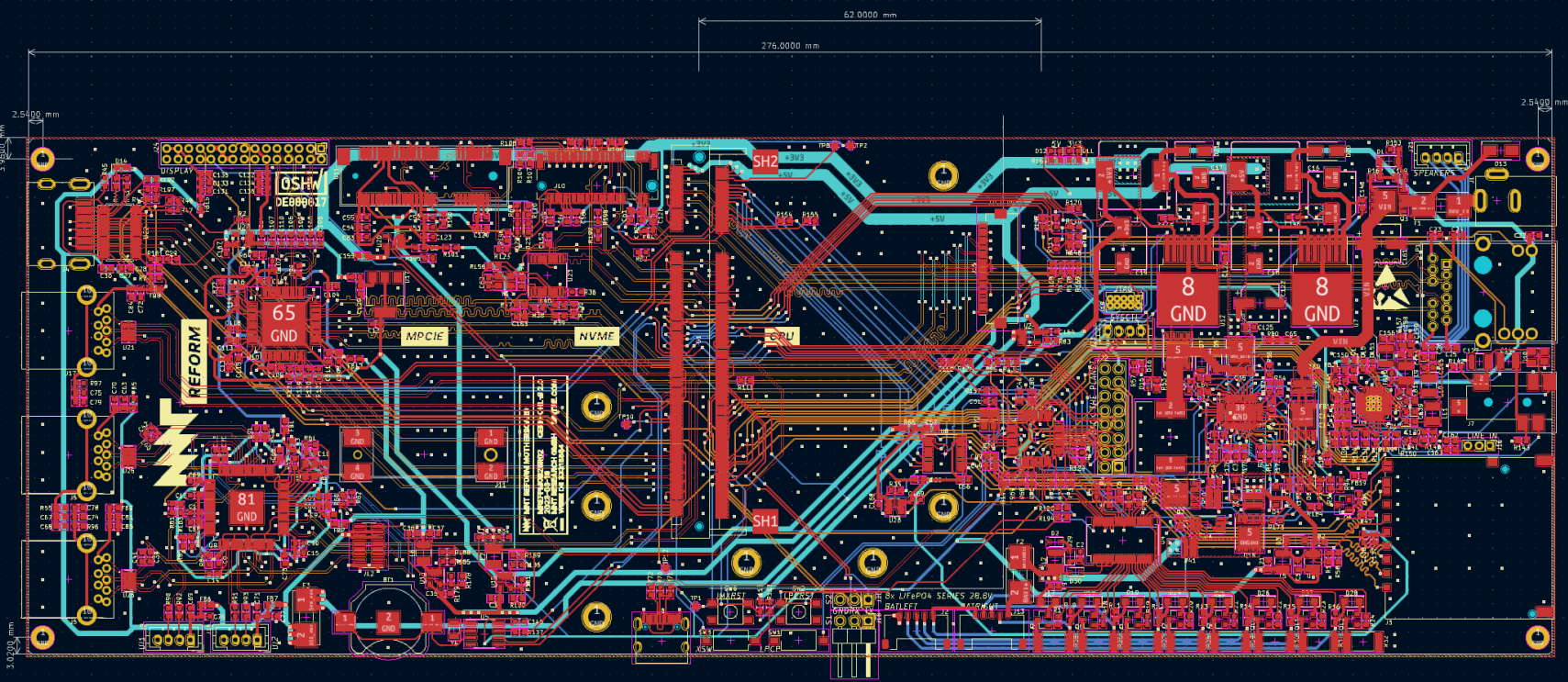
reform2-motherboard25 — PCB Editor

File Edit View Place Route Inspect Tools Preferences Help

F.Cu (PgUp)

Track: use netclass width | Via: use netclass sizes | Grid: 2.5400 mm (0.1000 in) | Zoom 2.20

This file was created by an older version of KiCad. It will be converted to the new format when saved.



Appearance

Layers

- F.Cu
- GND.Cu
- Signal.Cu
- Power.Cu
- GND2.Cu
- B.Cu
- F.Adhesive
- B.Adhesive
- F.Paste
- B.Paste
- F.Silkscreen
- B.Silkscreen
- F.Mask
- B.Mask
- User.Drawings
- User.Comments
- User.Eco1
- User.Eco2
- Edge.Cuts
- Margin
- F.Courtyard
- B.Courtyard
- F.Fab
- B.Fab

Layer Display Options

Presets (Ctrl+Tab): ---

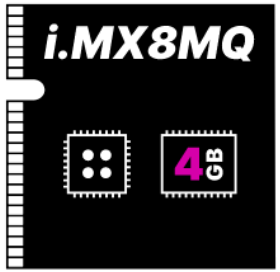
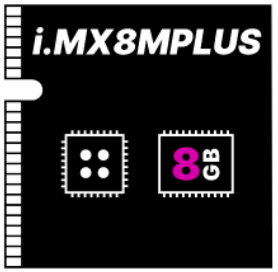
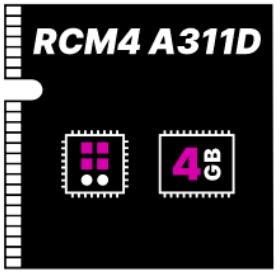
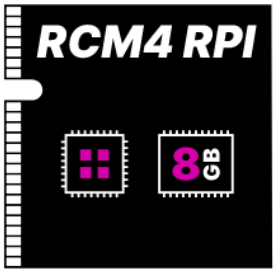
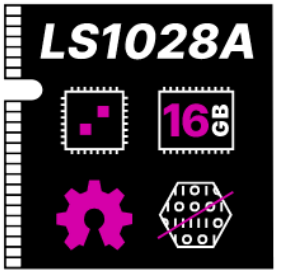
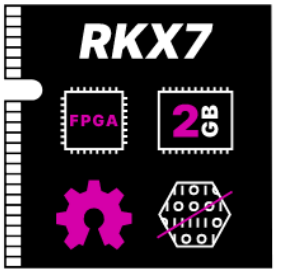
Viewports (Shift+Tab): ---

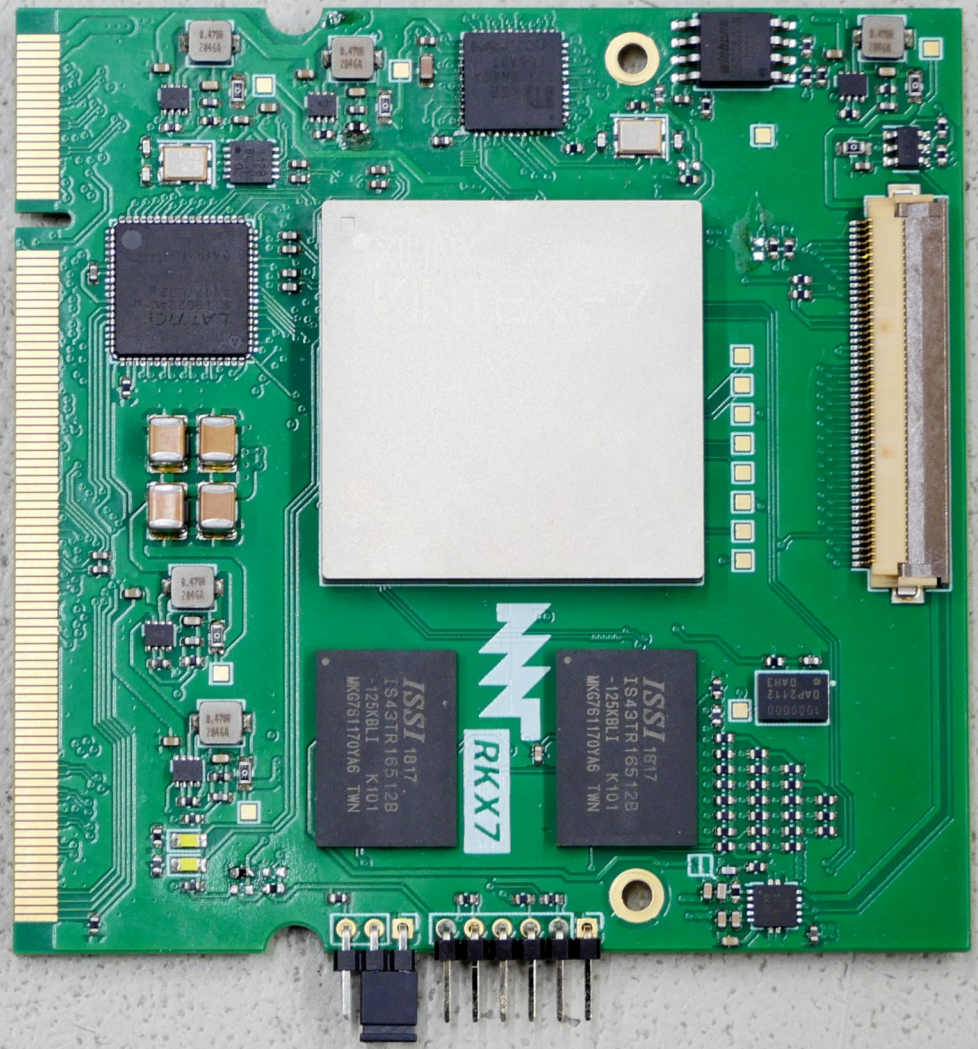
Selection Filter

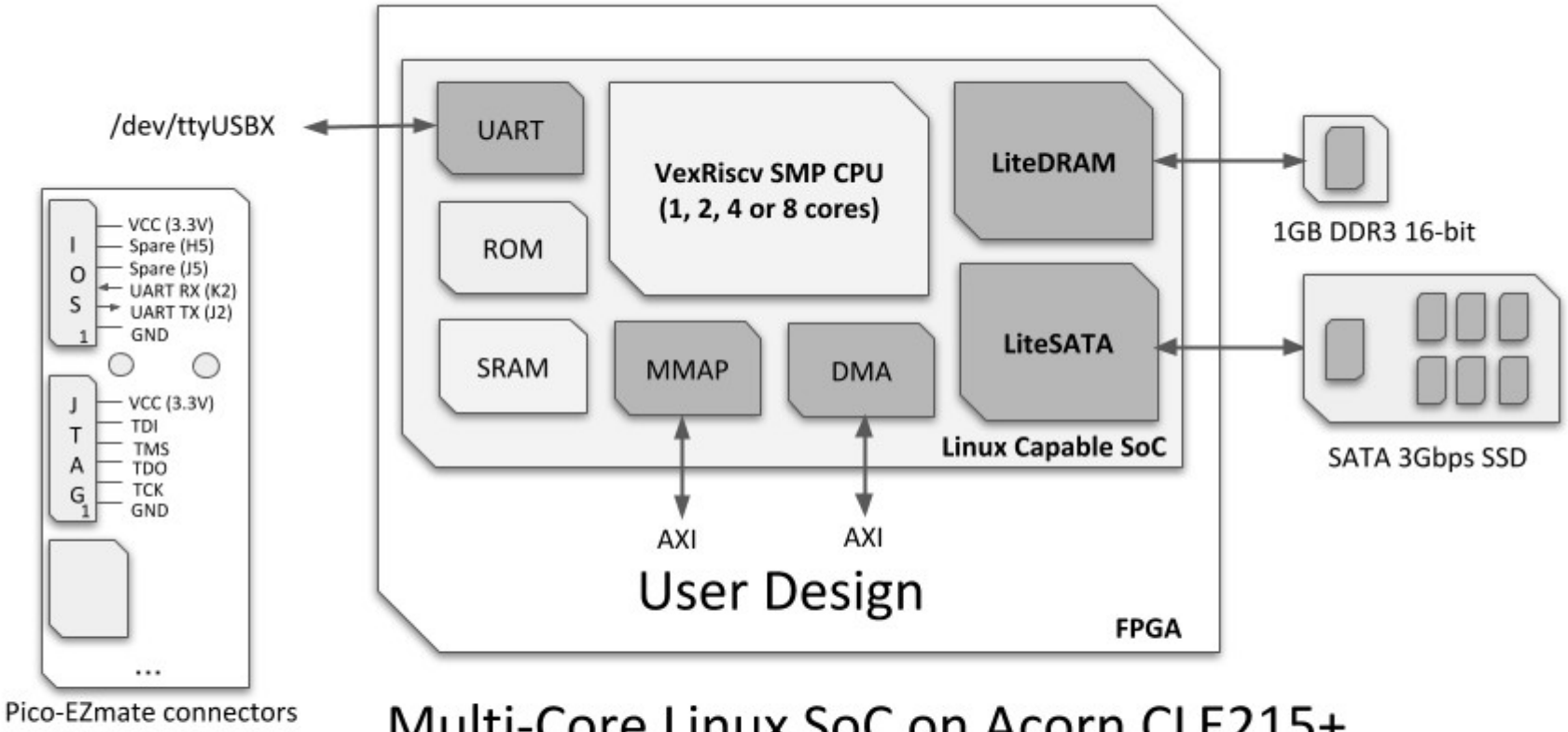
- All items
- Footprints
- Tracks
- Pads
- Zones
- Dimensions
- Lock
- Text
- Vias
- Grap
- Rule
- Othe

Pads	Vias	Track Segments	Nets	Unrouted
2109	1081	11113	647	0

Z 2.02 X 205.7400 Y 144.7800 dx 205.7400 dy 144.7800 dist 251.5754 grid X 2.5400 Y 2.5400 mm

						
CPU	4× 1.5GHz Cortex-A53	4× 1.8GHz Cortex-A53 (2GHz overclocked)	4× 2.2 GHz Cortex-A73 + 2× 1.8 GHz Cortex-A53	4× 1.5 GHz Cortex-A72 (2 GHz overclocked)	2× 1.5 GHz Cortex-A72	Kintex-7 FPGA (i.e. VexRiscV/LiteX)
GPU	Vivante GC7000L (OpenGL/ES 2.1 with Etnaviv)	Vivante GC7000UL (OpenGL/ES 2.1 with Etnaviv)	ARM Mali G52 MP4 (OpenGL/ES 3.1 with Panfrost)	VideoCore 4 (OpenGL/ES 3.1, Vulkan 1.0)	Vivante GC7000UL (OpenGL/ES 2.1 with Etnaviv)	User defined
RAM	4 GB LPDDR4	8 GB LPDDR4	4 GB LPDDR4	8GB LPDDR4	16 GB DDR4	2 GB DDR3
Wi-Fi	via mPCIe card	Integrated QCA9377 (WiFi 5)	Integrated RTL8822CS (WiFi 5)	Integrated BCM43455 (WiFi 5)	via mPCIe card	No
Bluetooth	No	Integrated QCA9377 (BT 5.0)	Integrated RTL8822CS (BT 5.0)	Integrated BCM43455 (BT 5.0)	No	No
Ethernet	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s
PCIe	2 Slots	1 Slot	1 Slot	1 Slot	1 Slot + 1 external + 1 SATA-III	2 Slots
Dual Display	Yes	Yes	No (either internal or HDMI display at a time)	Yes	No (external GPU possible)	Yes
Open Source Firmware	DDR4C and HDMI (optional) have closed source firmware.	DDR4C and WiFi/BT have closed source firmware.	Part of boot/TF-A and Wi-Fi firmware is closed source.	Closed boot blob.	eDP has closed source firmware (required only in laptop).	Yes
Open Source Drivers	Yes	Yes	Yes	Yes	Yes	Yes
PDF Schematics	Yes, full	Yes, full	Yes, partial	Yes, partial	Yes	Yes
KiCAD Sources	No	Adapter only	Adapter only	Adapter only	Yes, full	Yes, full
USB	USB 3.0	USB 3.0	USB 2.0	USB 2.0	USB 3.0	USB 1.0 (user defined)
HDMI	HDMI 2.0a	HDMI 2.0a	HDMI 2.1	HDMI 2.0	No (external PCIe for eGPU	HDMI 1.4


ISSI
IS43TR16512B
-125KBLI
MKG61170YA6
RKX7

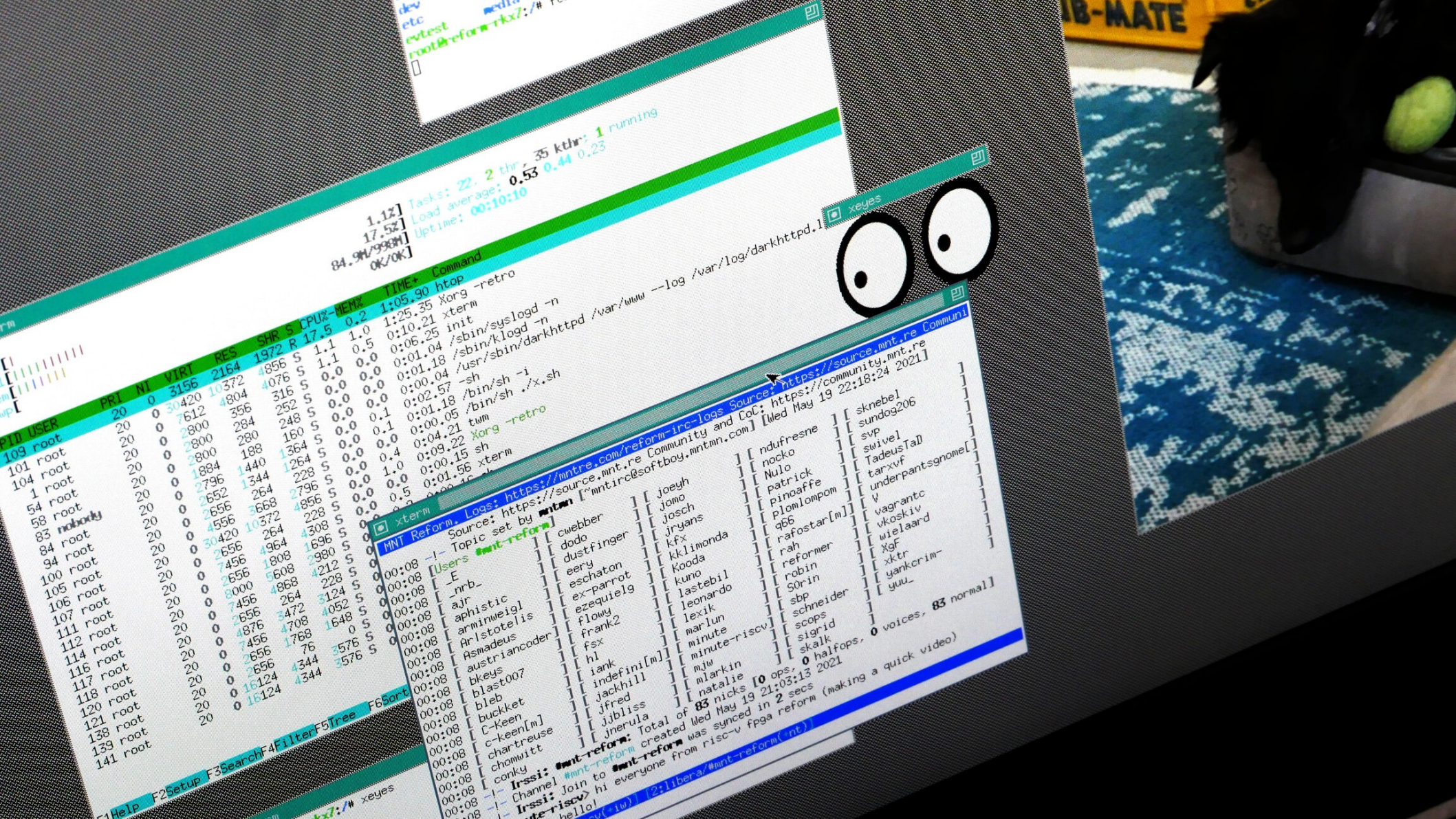


Multi-Core Linux SoC on Acorn CLE215+

EnjoyDigital

Built with LiteX
Build your hardware, easily!


LiFePO4 18650 3.2V
Rechargeable 1800mAh
REFORM
RK3588
NVME
MPCIE


xeyes
xterm
MNT Reform Logs: https://mntre.com/reform-irc-logs Source: https://source.mnt.re Communi
Source: https://source.mnt.re Community and CoC: https://community.mnt.re
Topic set by mntan ["mntirc@softboy.mntmn.com] [Wed May 19 22:18:24 2021]
#mnt-reform
[Users
-E
nrb
ajr
aphistic
arminweigl
Ar|stotelis
Asmadeus
austriancoder
bkeys
blast007
bleb
buckket
C-Keen
c-keen[m]
chartreuse
chomwitt
conky
cwebber
dodo
dustfinger
eery
eschaton
ex-parrot
ezequielg
flowy
frank2
fsx
hl
iank
indefini[m]
jackhill
jfred
jjbliss
jnerula
joeyh
jomo
josch
jryans
kfx
kklimonda
Kooda
kuno
lastebil
leonardo
lexik
marlun
minute
minute-riscv
mju
mlarkin
natalie
ndufresne
nocko
Nulo
patrick
pinoaffe
Plomlompom
q66
rafostar[m]
rah
reformer
robin
S0rin
sbp
schneider
scops
sigrid
skalk
sknebel
sundog206
svp
swivel
TadeusTal
tarxvf
underpantsgnome[
V
vagrantc
vkoskiv
wielaard
XgF
xktr
yankcrim-
yuu_
Irssi: #mnt-reform: Total of 83 nicks [0 ops, 0 halfops, 0 voices, 83 normal]
Irssi: Join to #mnt-reform created Wed May 19 21:03:13 2021
hi everyone from risc-v fpga reform (making a quick video)
hello!
[2:libera/#mnt-reform(+nt)]
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
109 root 20 0 3156 2164 1972 R 17.5 0.2 1:05.90 htop
101 root 20 0 30420 10372 4856 S 1.1 1.0 1:25.35 Xorg -retro
104 root 20 0 7612 4804 4076 S 1.1 0.5 0:10.21 xterm
1 root 20 0 2800 356 316 S 0.0 0.0 0:06.25 init
54 root 20 0 2800 284 252 S 0.0 0.0 0:01.04 /sbin/syslogd -n
58 root 20 0 2800 280 248 S 0.0 0.0 0:01.18 /sbin/klogd -n
83 nobody 20 0 1884 188 160 S 0.0 0.1 0:00.04 /usr/sbin/darkhttpd /var/www --log /var/log/darkhttpd.l
84 root 20 0 2796 1344 1364 S 0.0 0.1 0:02.57 -sh
94 root 20 0 2652 264 1264 S 0.0 0.0 0:01.18 /bin/sh -i
100 root 20 0 2656 3668 228 S 0.0 0.4 0:00.05 /bin/sh ./x.sh
105 root 20 0 4556 10372 2796 S 0.0 1.0 0:04.21 twm
106 root 20 0 30420 264 4856 S 0.0 0.0 0:09.22 Xorg -retro
107 root 20 0 2656 4964 228 S 0.0 0.5 0:00.15 sh
111 root 20 0 7456 1808 4308 S 0.0 0.0 0:01.56 xterm
112 root 20 0 2656 5608 1696 S 0.0 0.0
114 root 20 0 8000 868 2980 S 0.0 0.0
116 root 20 0 7456 264 4212 S 0.0 0.0
117 root 20 0 2656 3472 228 S 0.0 0.0
118 root 20 0 4876 4708 4052 S 0.0 0.0
120 root 20 0 7456 1768 1648 S 0.0 0.0
121 root 20 0 2656 76 0 S 0.0 0.0
138 root 20 0 2656 4344 3576 S 0.0 0.0
139 root 20 0 16124 4344 3576 S 0.0 0.0
141 root 20 0 16124
F1Help F2Setup F3SearchF4FilterF5Tree F6Sort
1.1%] Tasks: 22, 2 thr, 35 kthr; 1 running
17.5%] Load average: 0.53 0.44 0.23
84.9M/990M] Uptime: 00:10:10
0K/0K]
xeyes
/# xeyes


Starting network: OK
Starting darkhttpd: OK
Welcome to Buildroot
reform-rkx7 login: root
32-bit RISC-V Linux running on LiteX / VexRiscv-SMP.
root@reform-rkx7:~#

Skybox: Open-Source Graphic Rendering on Programmable RISC-V GPUs

Blaise Tine
Georgia Institute of Technology
USA
btine3@gatech.edu

Varun Saxena
Georgia Institute of Technology
USA
vsaxena36@gatech.edu

Santosh Srivatsan
Georgia Institute of Technology
USA
ssrivatsan30@gatech.edu

Joshua R. Simpson
California Polytechnic State
USA
simps03@calpoly.edu

Fadi Alzammar
California Polytechnic State
USA
falzamma@calpoly.edu

Liam Cooper
Georgia Institute of Technology
USA
lcooper43@gatech.edu

Hyesoon Kim
Georgia Institute of Technology
USA
hyesoon.kim@gatech.edu

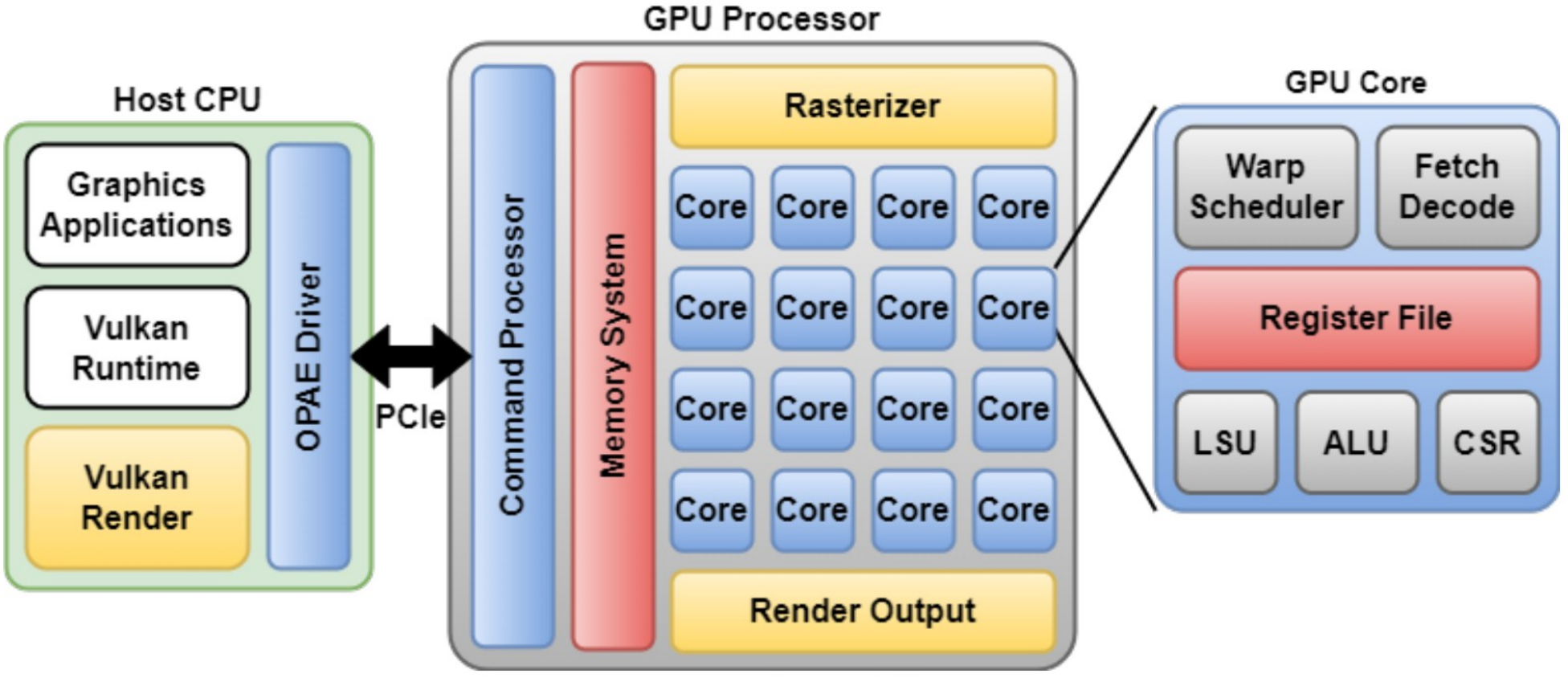
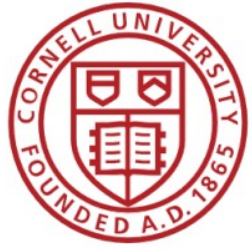


Figure 1: Skybox framework overview.

Celerity: An Open Source 511-core RISC-V Tiered Accelerator Fabric

Prof. Michael Taylor
Bespoke Silicon Group
University of Washington

http://www.opencelerity.org

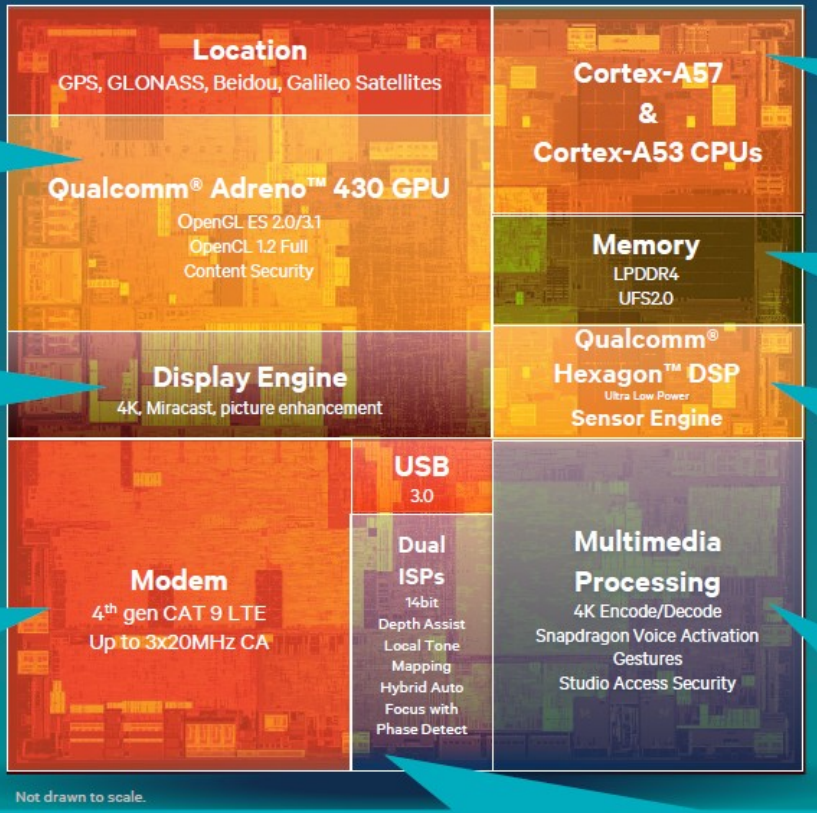


Introducing the Snapdragon 810 Processor

Advanced Graphics & Compute with the Adreno 430 – the best GPU Qualcomm Technologies' has ever made

4K primary & external display support with ecoPix and TruPalette and 3:1 pixel compression

Mobile industry's FIRST announced multi-channel 4G LTE SoC supporting Category 9 Carrier Aggregation



Not drawn to scale.

FIRST Announced ARM®v8-A/64-bit using Cortex®-A57+ Cortex®-A53

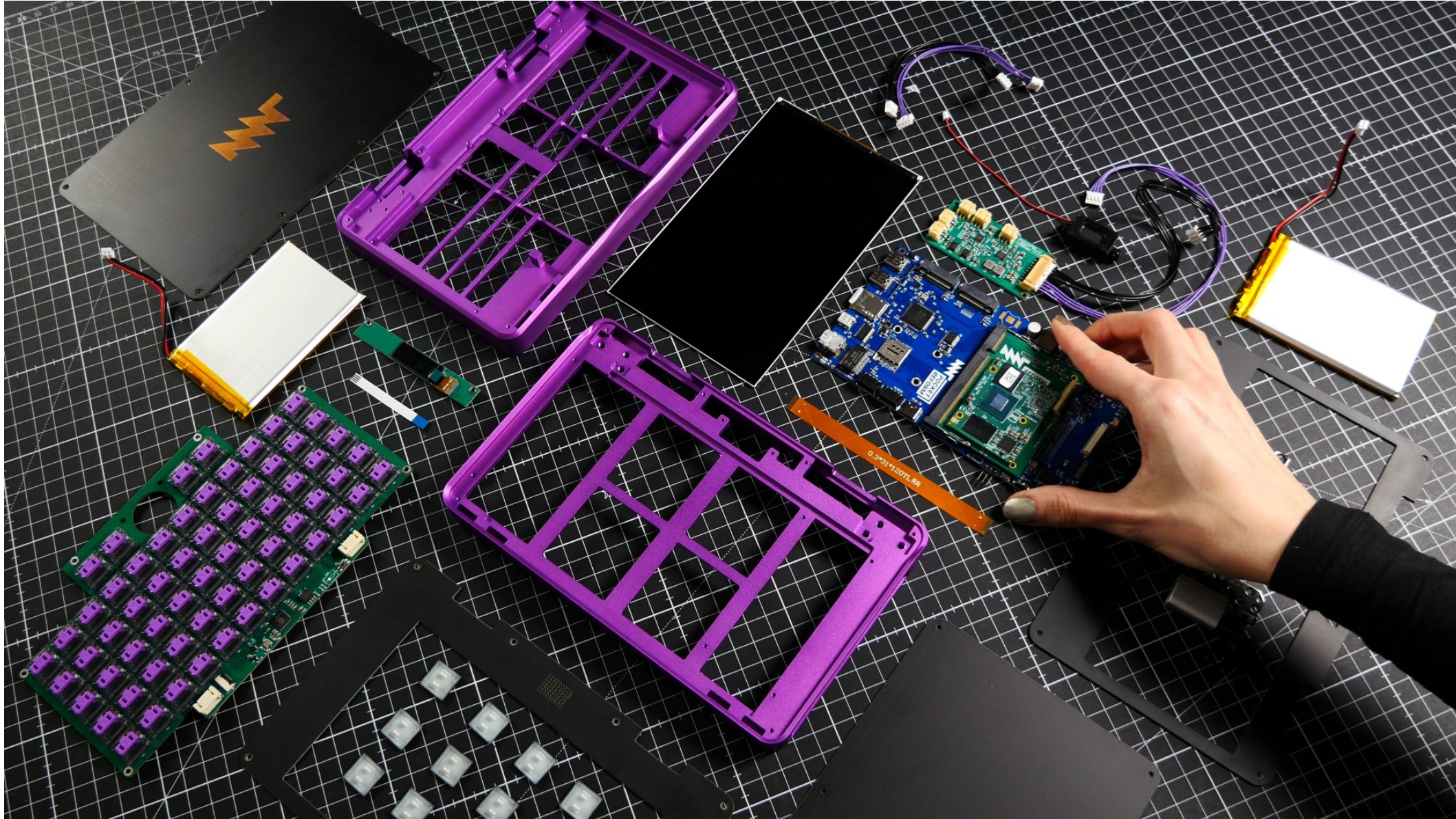
Mobile industry's FIRST announced dual channel 1600 MHz LPDDR4 memory

Qualcomm Technologies' FIRST UFS 2.0 Support

Greatly improved power management for DSP/Sensor Engine, Low Power Snapdragon Voice Activation (SVA), 12-channel surround sound decode

Qualcomm Technologies' FIRST hardware implementation of 4K HEVC/ H.265 video encode. HEVC designed to deliver up to 50% better video compression

Qualcomm Technologies' FIRST 14-bit Dual ISP for highest quality, depth enabled photography. Up to 21MP for main camera with depth assist, phase detect, for sharper dual camera user experiences



Thank You!

Lukas F. Hartmann — lukas@mntre.com
Fediverse: @mntmn@mastodon.social

MNT Research GmbH — https://mntre.com
FSIC2023, Paris