Weaponization Of Cellular Based IoT Technology

Leveraging Smart Devices to Gain a Foothold

Deral Heiland & Carlota Bindner

Deral Heiland
Principal Security Research (IoT), Rapid7
deral_heiland@rapid7.com
@percent_x

Carlota Bindner
Lead Product Security Researcher
Thermo Fisher Scientific
@carlotabindner

Project Introduction

Observations

- Growing use of cellular in IoT
- Lack of effective knowledge
- Lack of security testing methods

Goal

- Understand technology
- Build testing methodologies
- Answer needed security question

NB-IoT

- Slow (26-127 kbits)
- Telemetry Data
- Half-duplex
- Latency (1.6-10s)

LTE-M

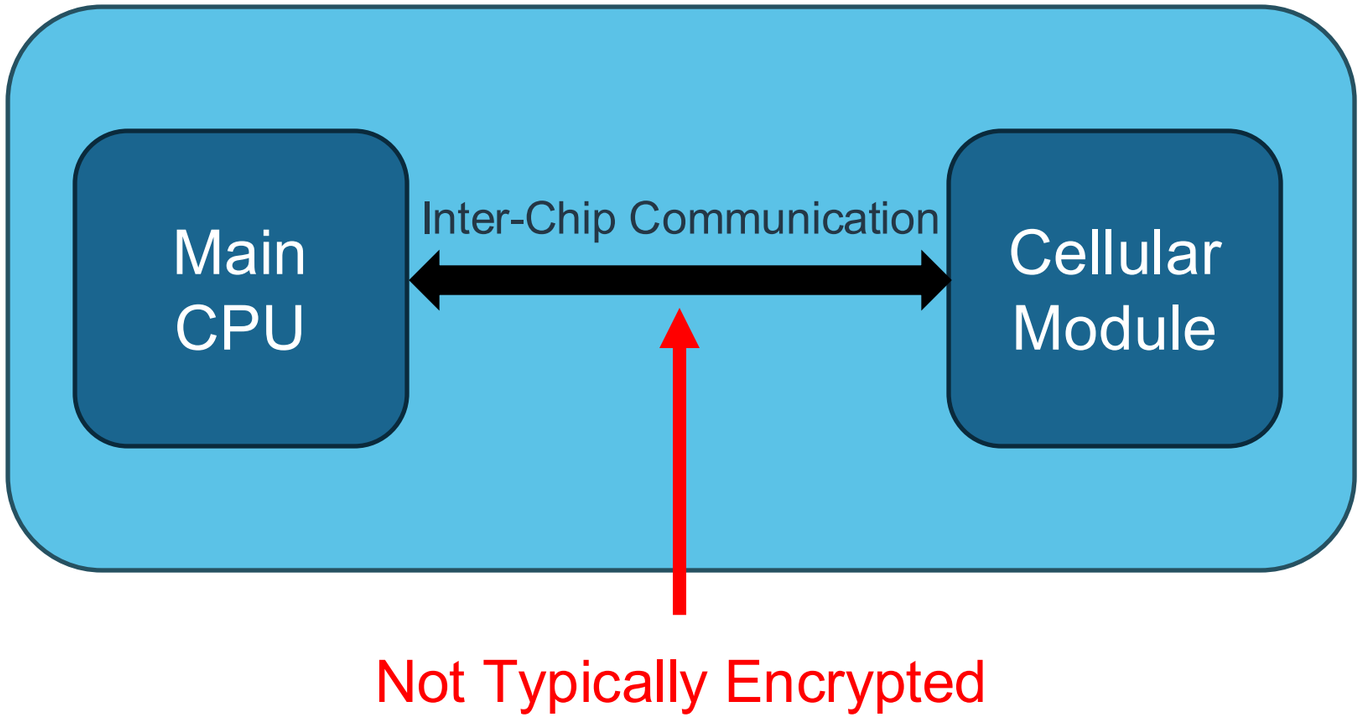
- Faster (1-4 mbits)
- Voice, Images, Video
- Full-duplex
- Latency (10-15ms)

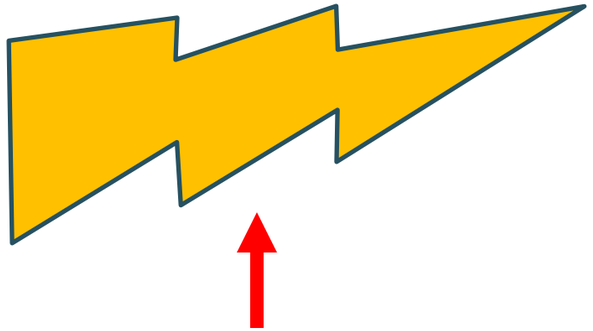
Inter-Chip Communication

- Encryption (Unlikely)
- Easy to sniff
- Easy to inject & control

Cellular Service

Internet of Things Hardware

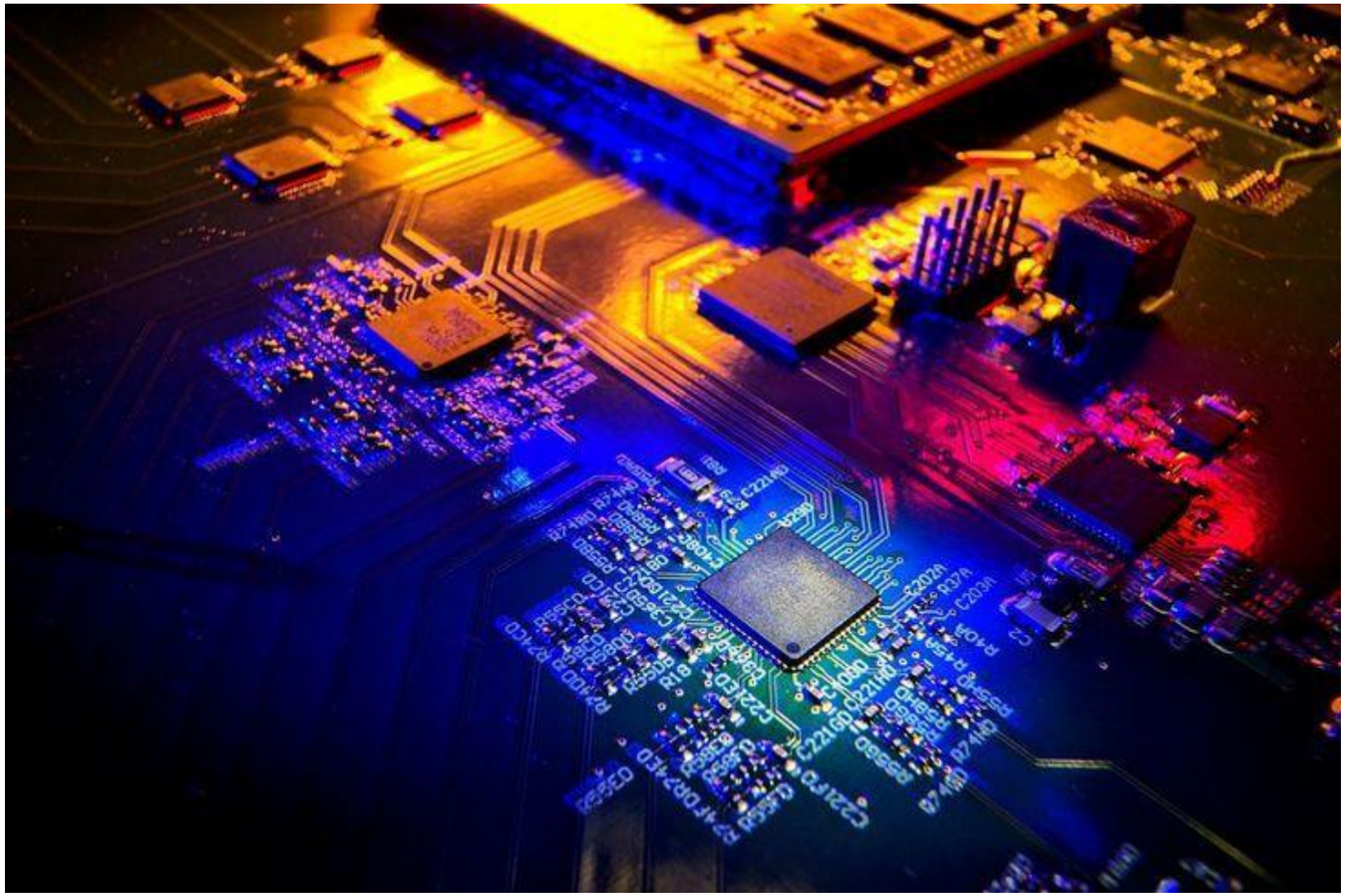


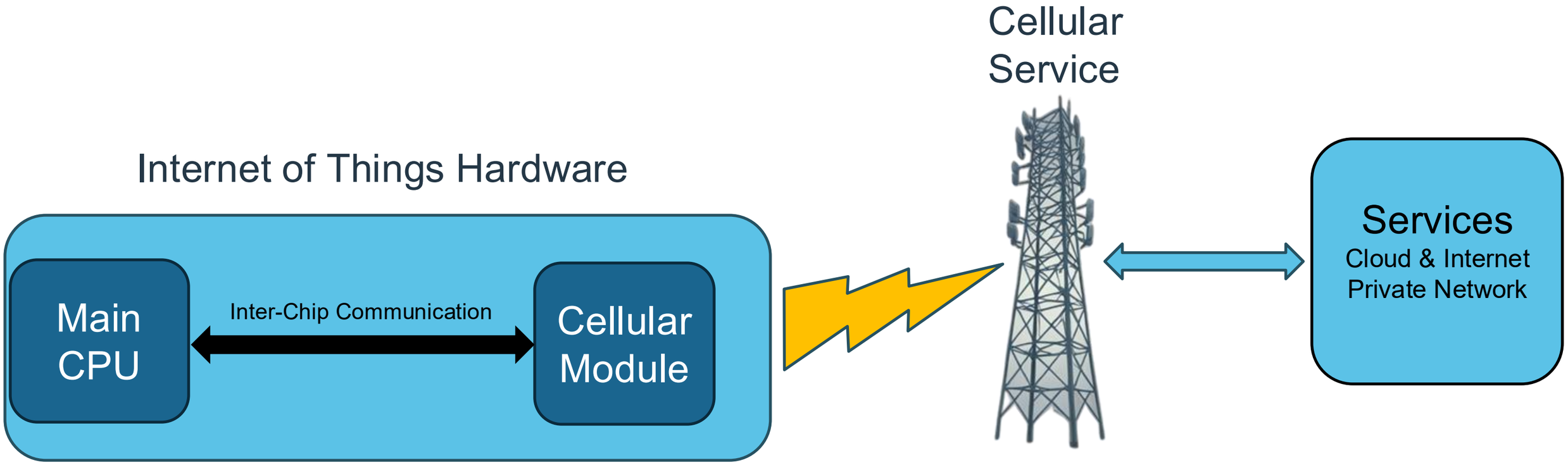


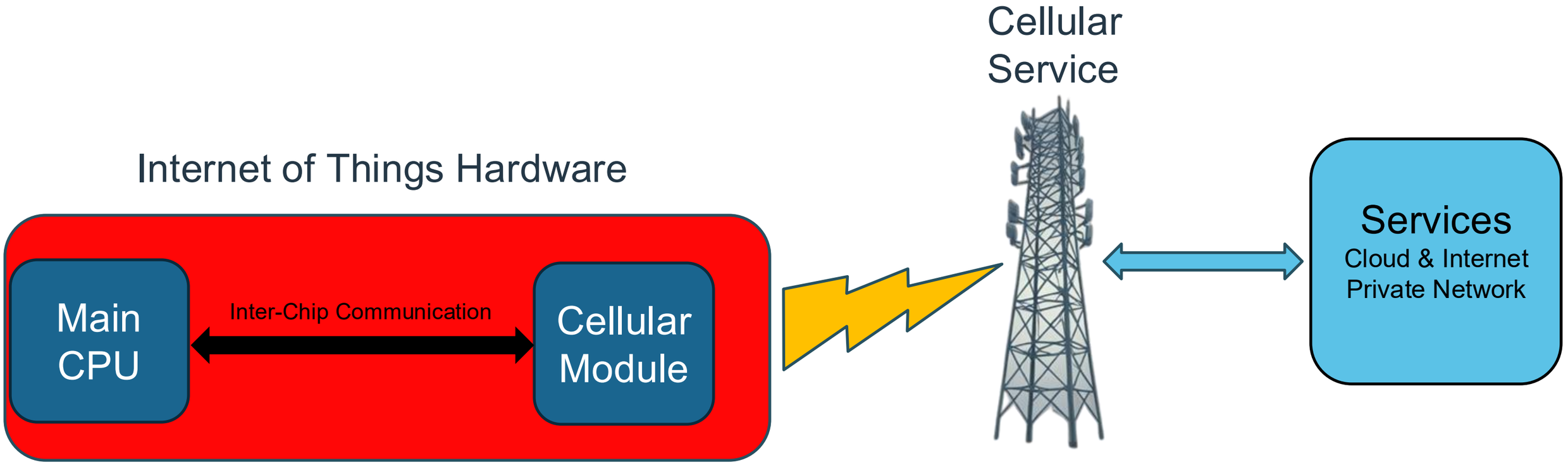
Typically Encrypted
&
FCC Regulated

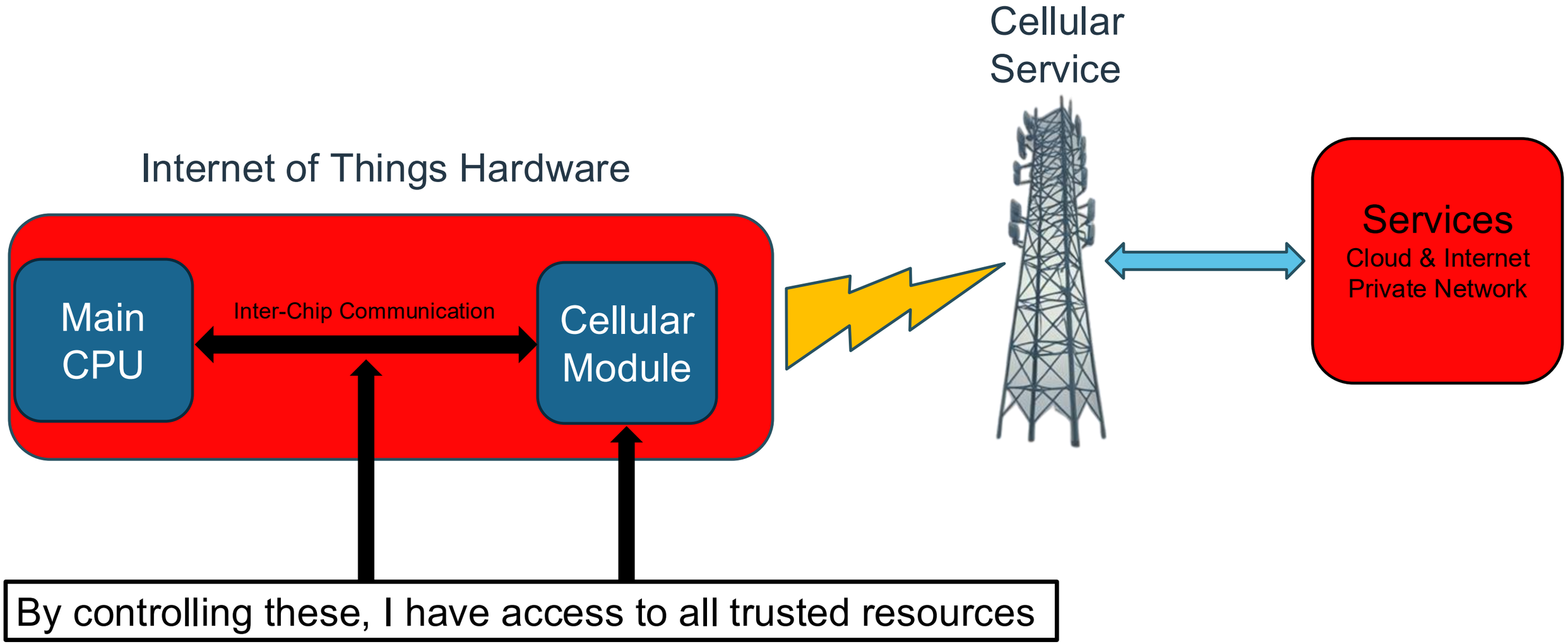
Trust

- Machine-to-Machine (overly trusted)
- Implicit Trust
- Automated Authentication & Validation
- Limited Containment & Segmentation




Cellular Service
Internet of Things Hardware
Main CPU
Inter-Chip Communication
Cellular Module
Services
Cloud & Internet
Private Network


Cellular Service
Internet of Things Hardware
Main CPU
Inter-Chip Communication
Cellular Module
Services
Cloud & Internet
Private Network


Cellular Service
Internet of Things Hardware
Main CPU
Inter-Chip Communication
Cellular Module
Services
Cloud & Internet
Private Network
By controlling these, I have access to all trusted resources

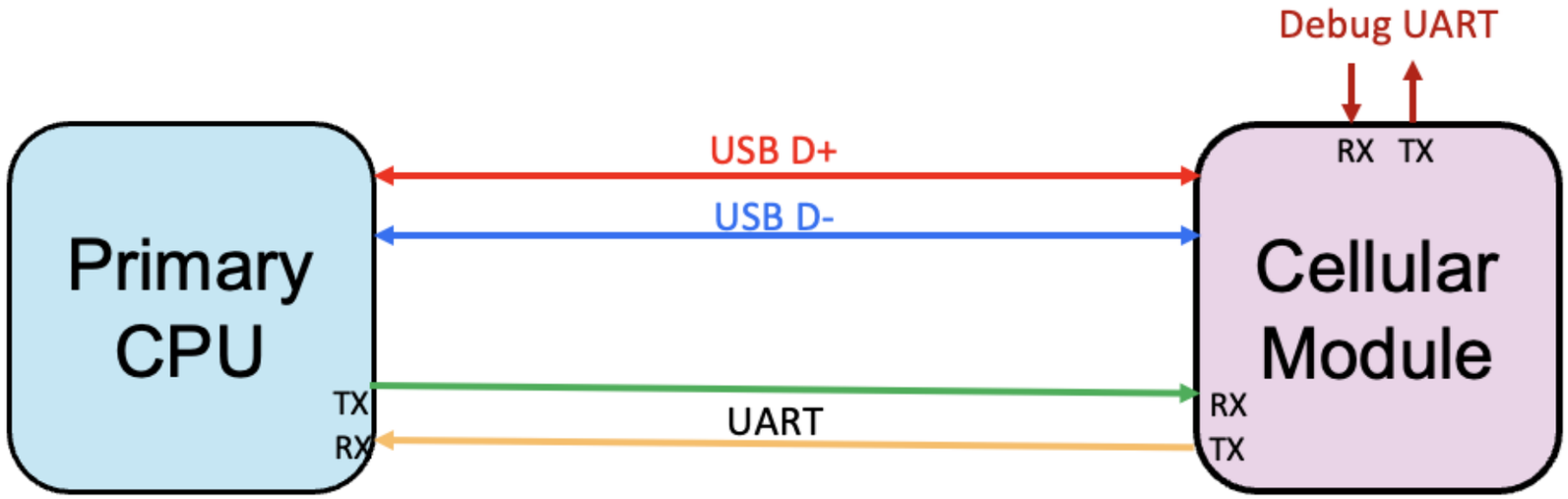
How To Interact With Cellular Modules

USB

- Standard 2.0 HS
- Implement basic functions

UART

- Debug UART (External)
- Main UART (Inter-Chip)



Talking to a Cellular Module

AT Commands

- AT=Attention
- Used to control modems

Allow communication and control

- Configuration and management
- Diagnostics
- Updates

Type	Syntax	Function
Test	AT+<COMMAND>=?	Returns parameters and value ranges.
Read	AT+<COMMAND>?	Returns the current parameter values.
Write/Set	AT+<COMMAND>=<INPUT>	Sets command parameters to user-defined values.
Execute	AT+<COMMAND>	Executes the command.

Types of AT Commands

3GPP Standardized
- Required
- Implement basic functions

Manufacturer Specific
- Specific to features
- Enhance functionality

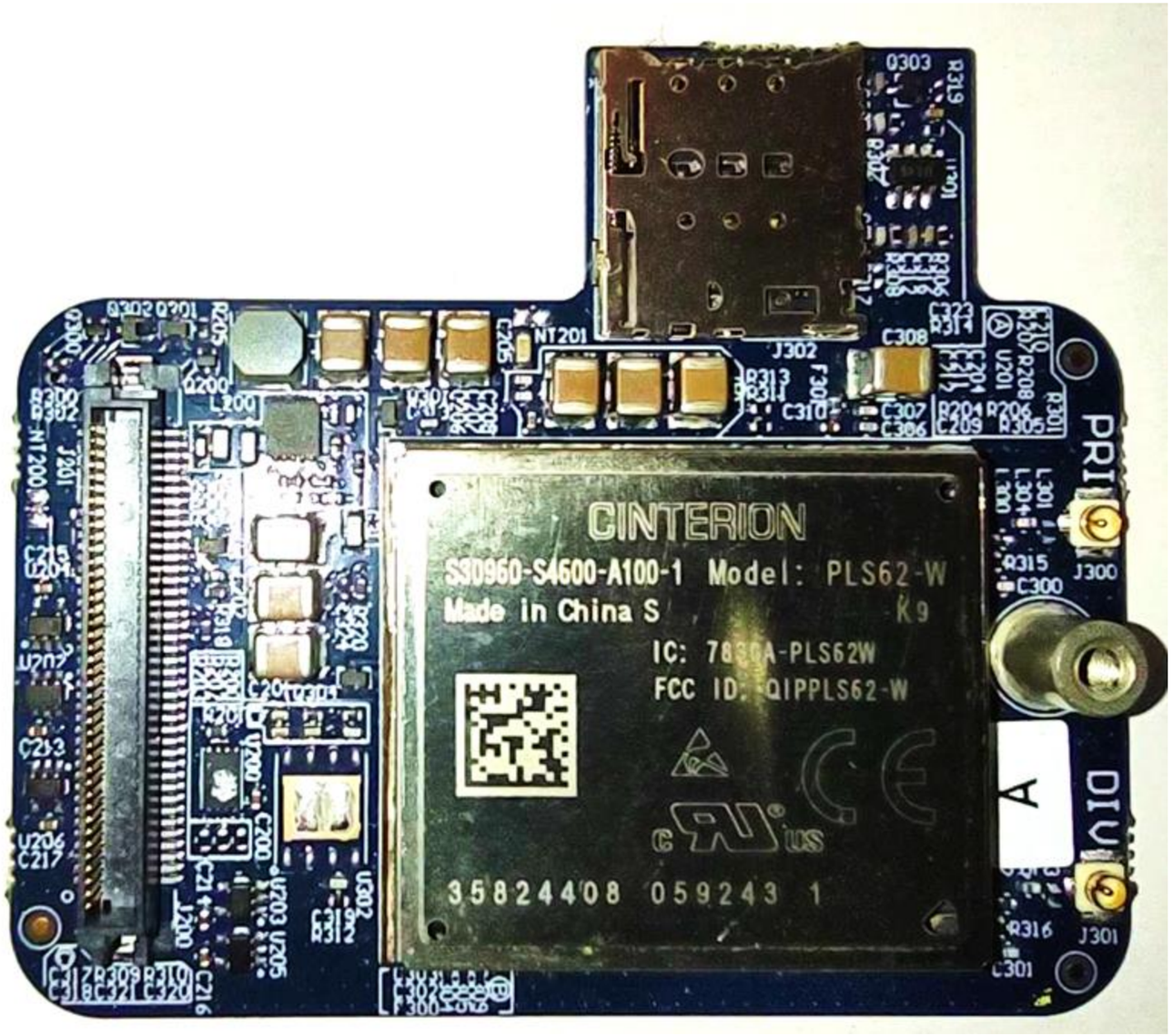
Manufacturer	Custom Syntax
Quectel	AT+Q
U-Blox	AT+U
Telit	AT@, AT#, AT$, AT*
Nordic	AT%
Murata	AT%
Huawei	AT^

Hardware Hacking

Physical Interaction with Hardware

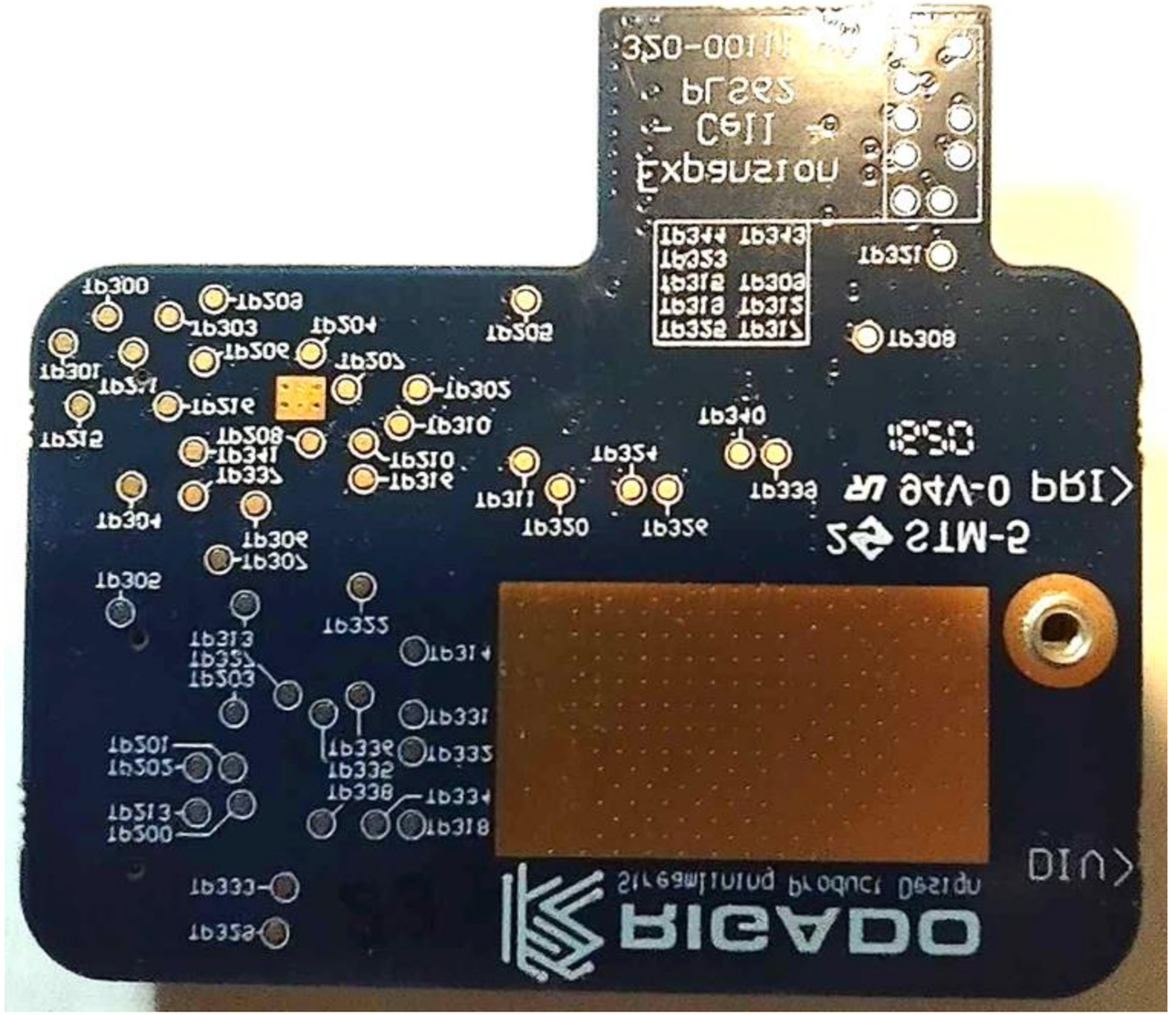
Mapping Access

Obverse



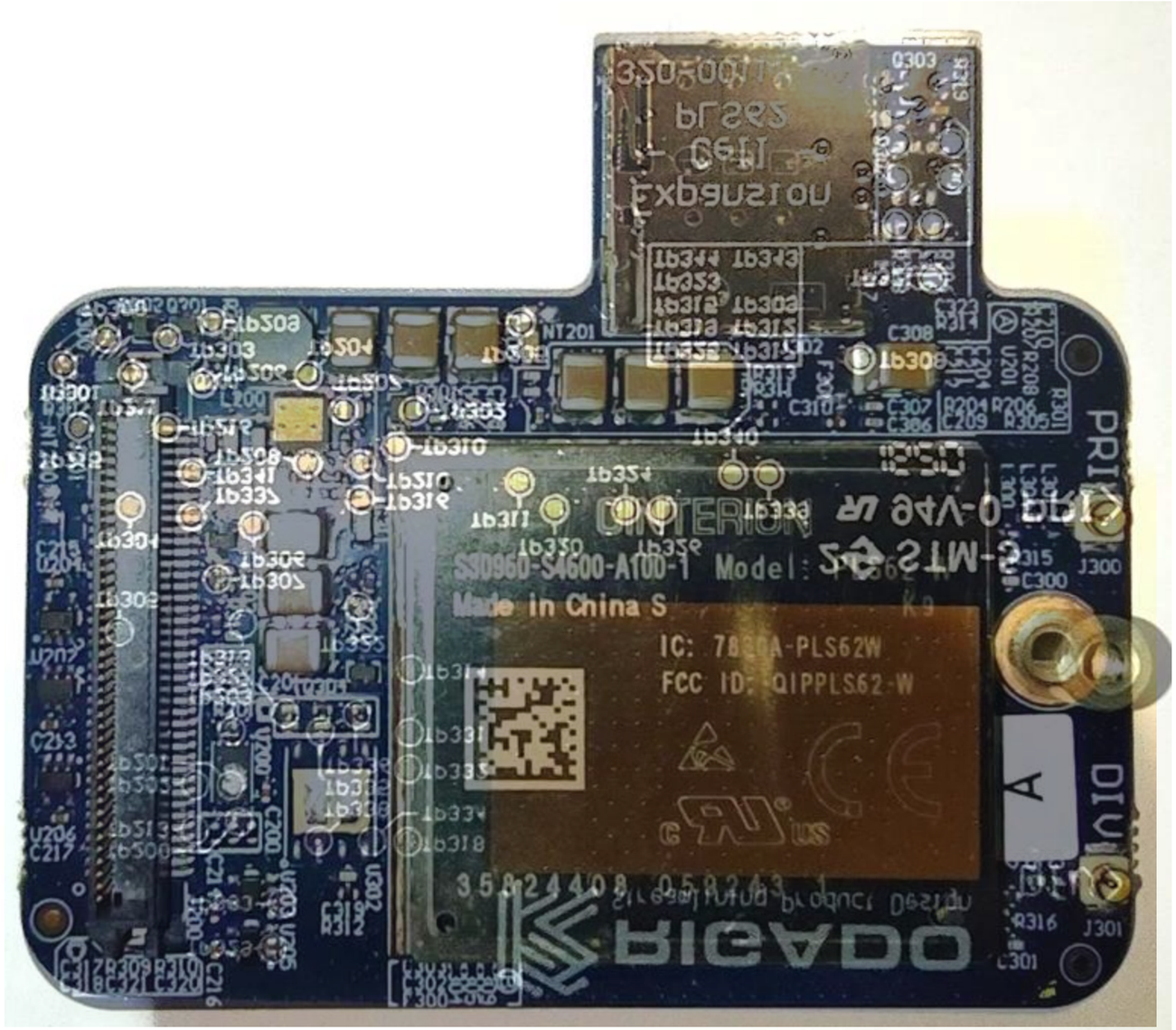
Mapping Access

Reverse (flipped)



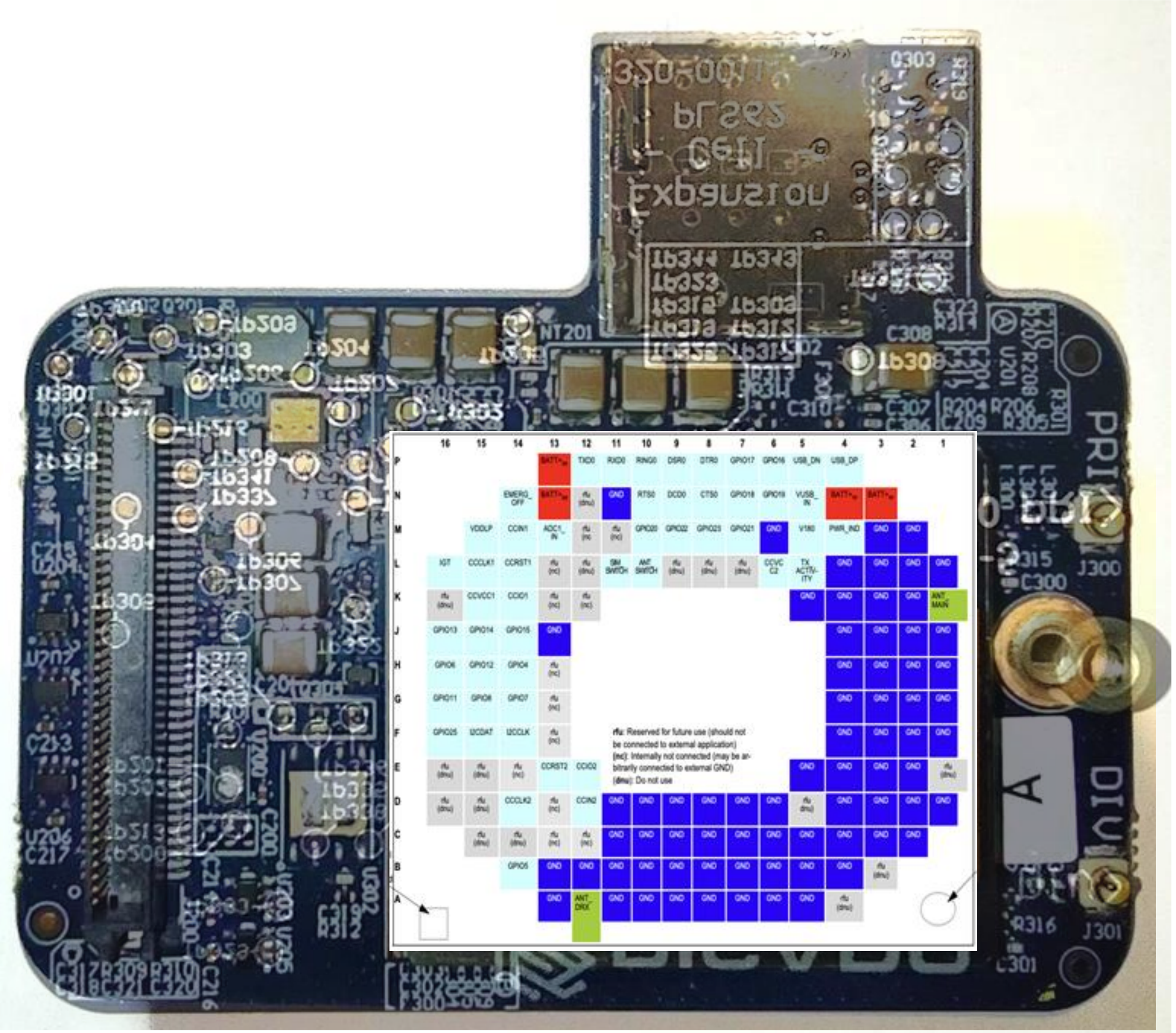
Mapping Access

Transparency (Obverse overlay)



Mapping Access

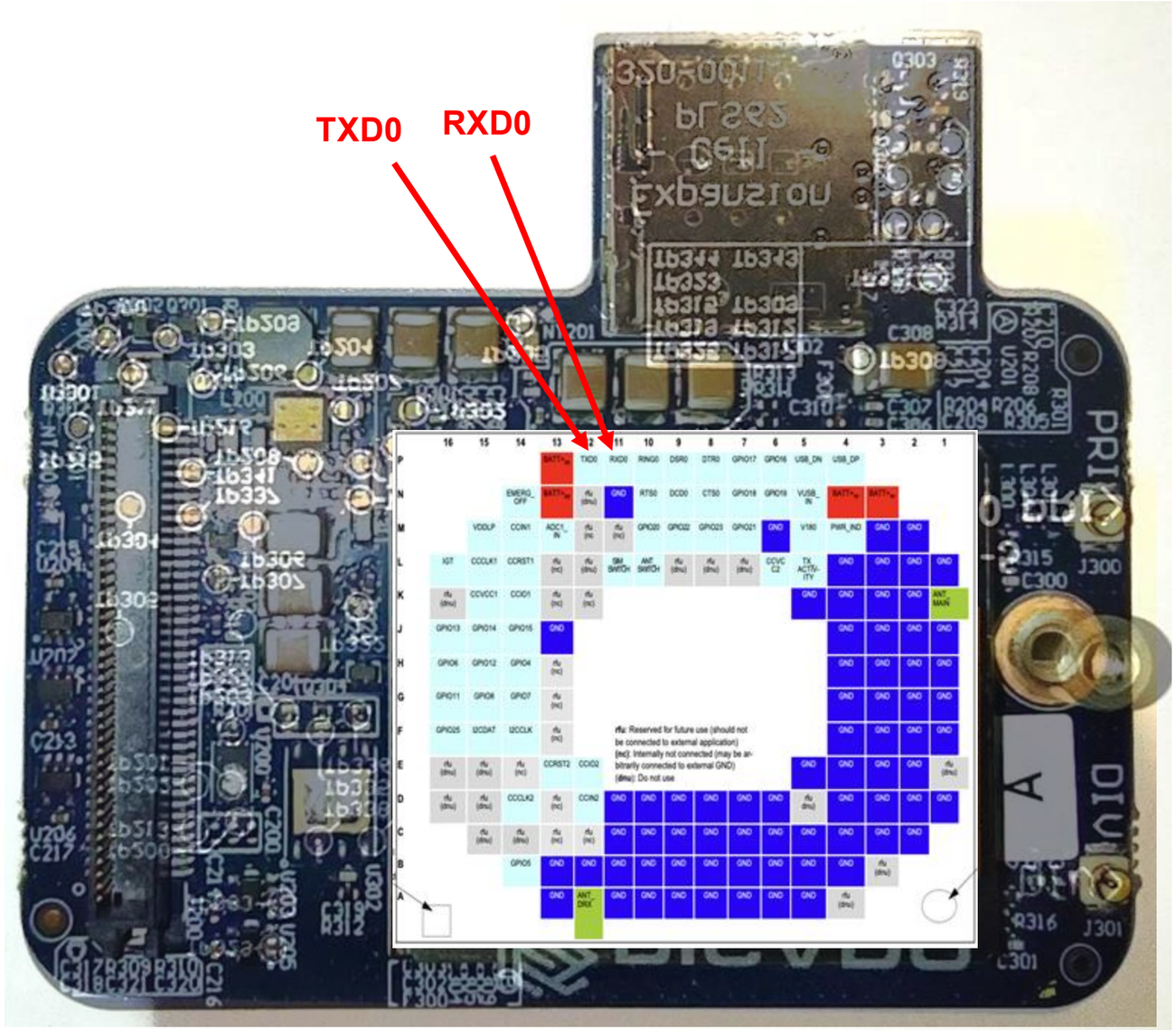
Data sheet LGA overlayed



Mapping Access

Data sheet LGA overlayed

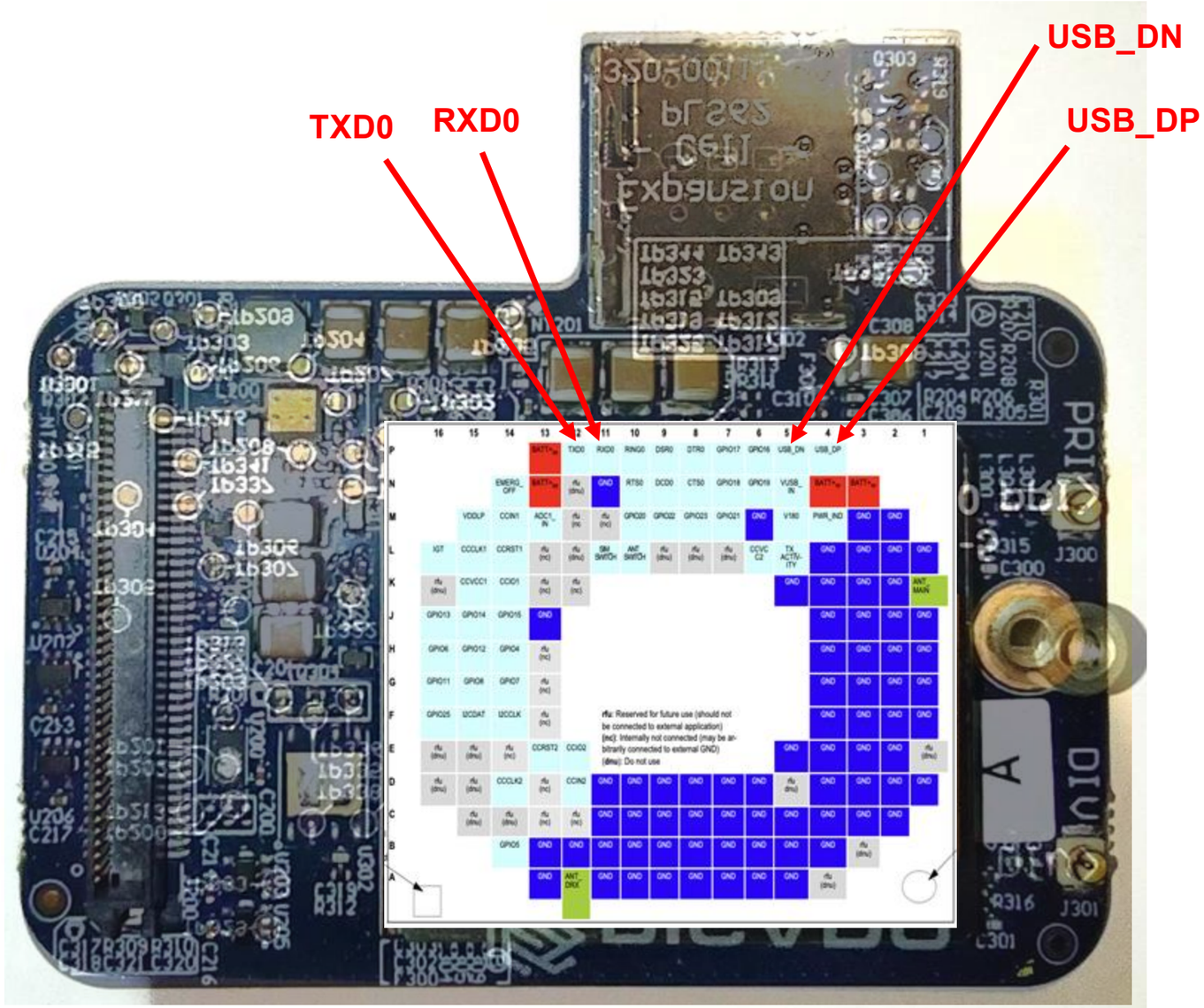
- UART



Mapping Access

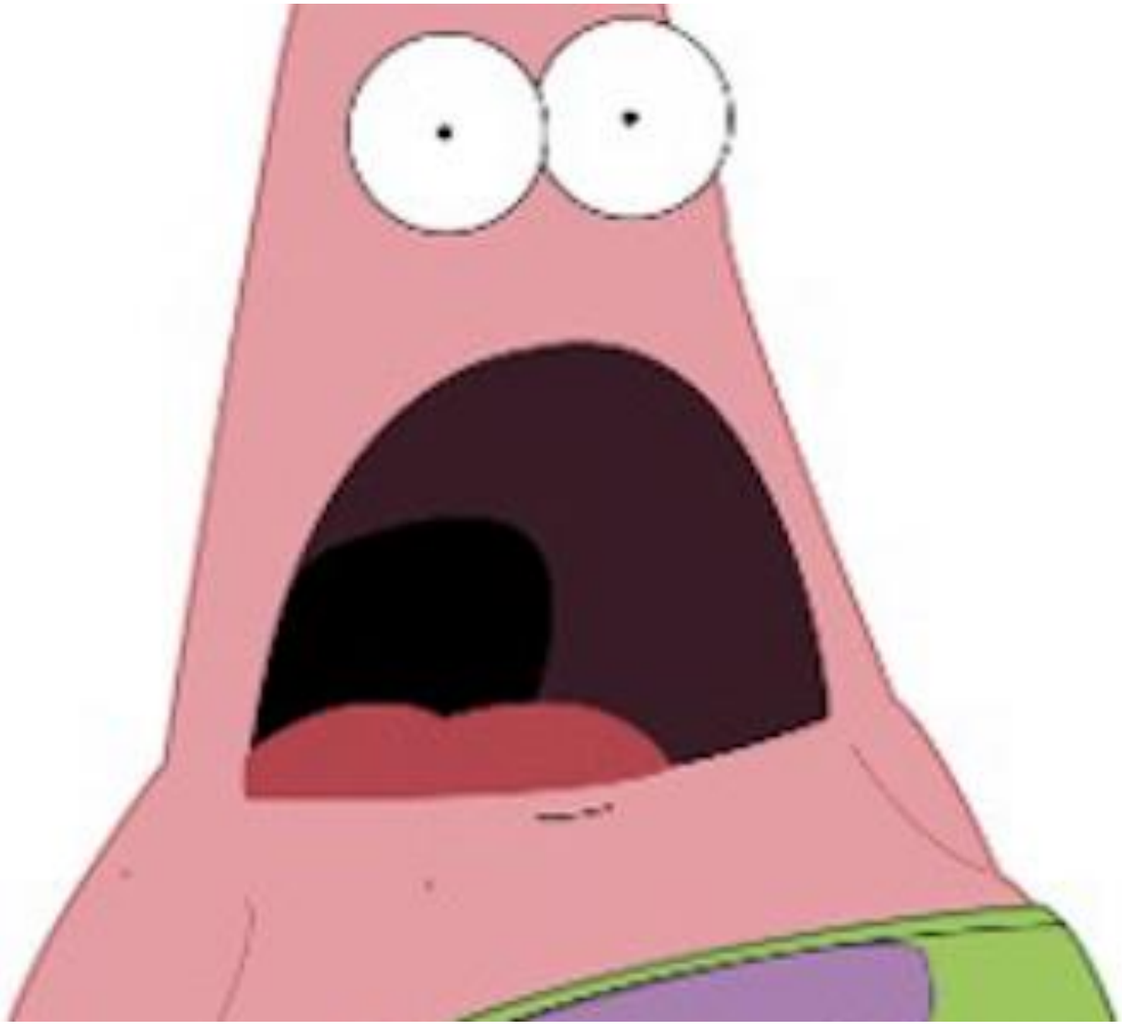
Data sheet LGA overlayed

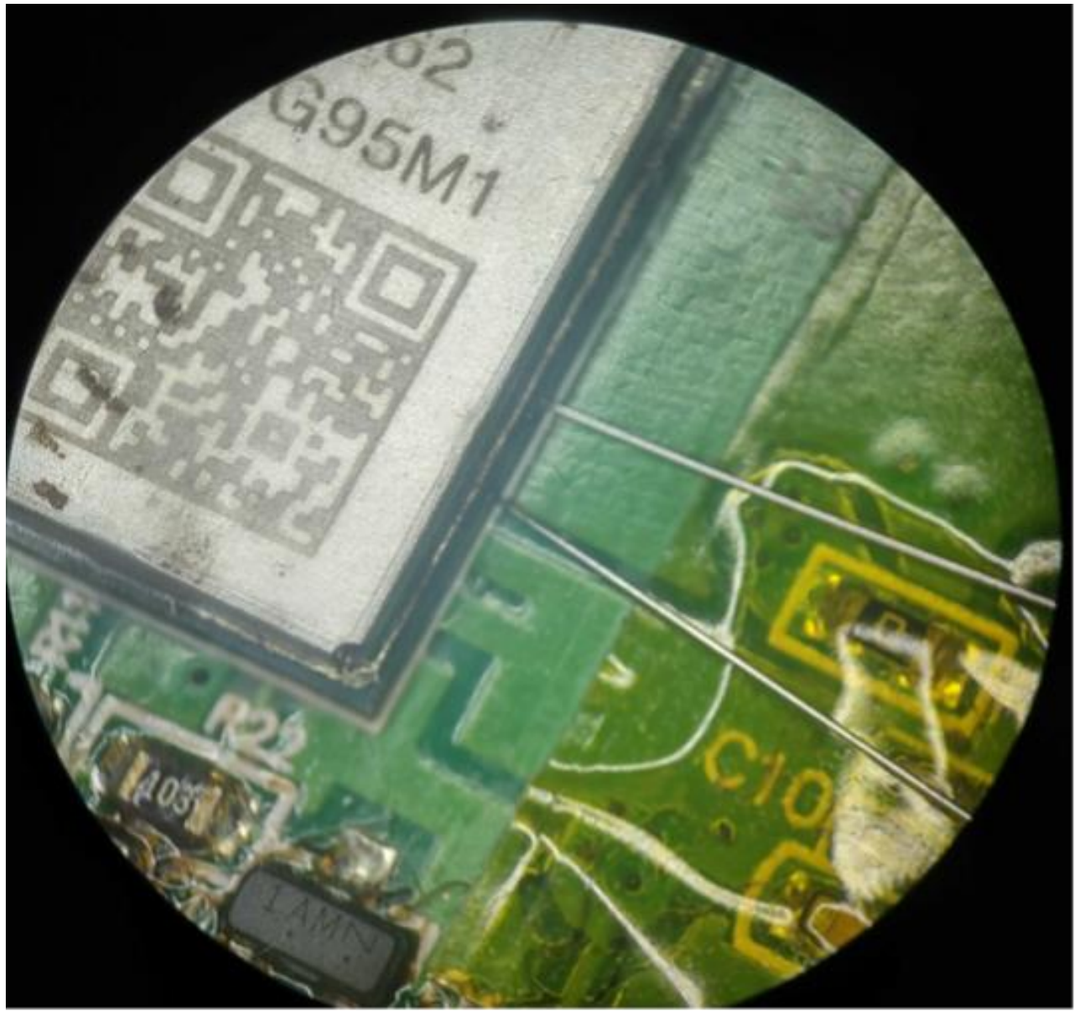
- UART
- USB

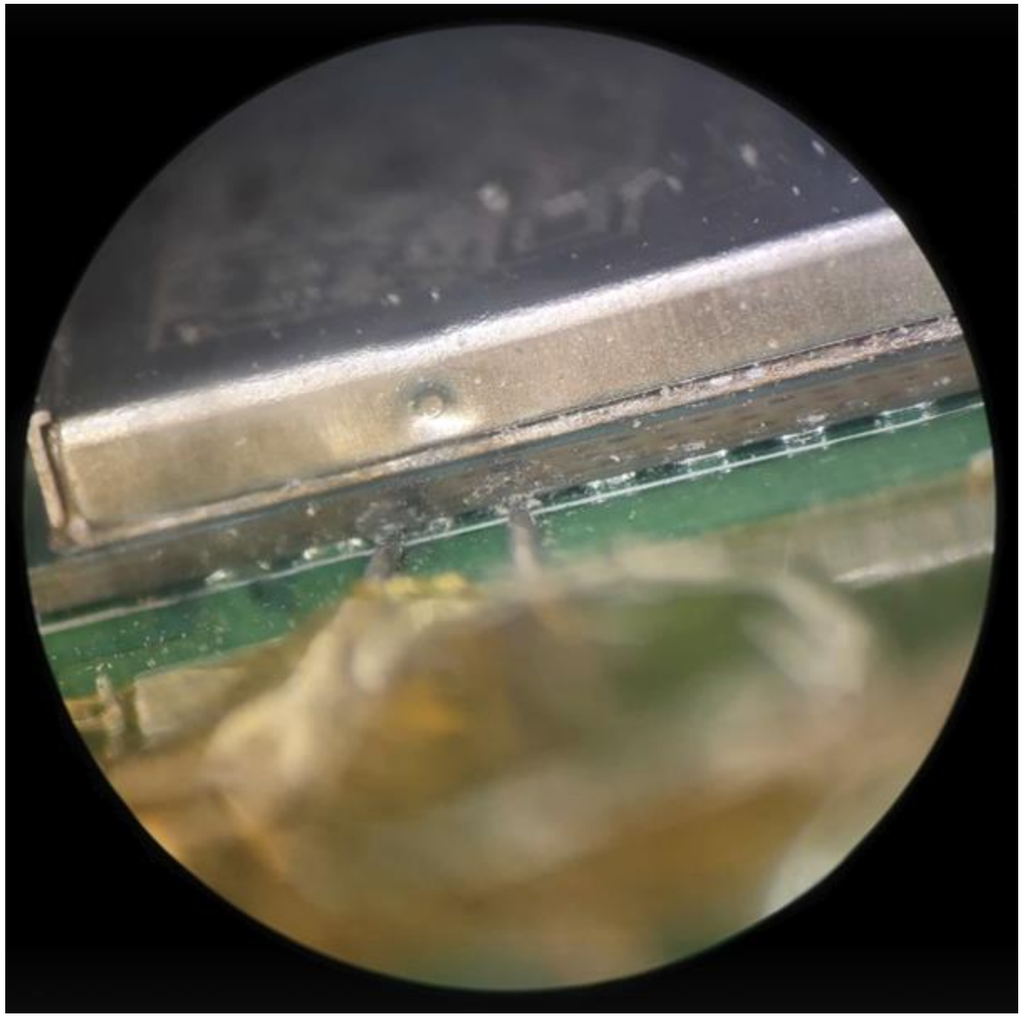


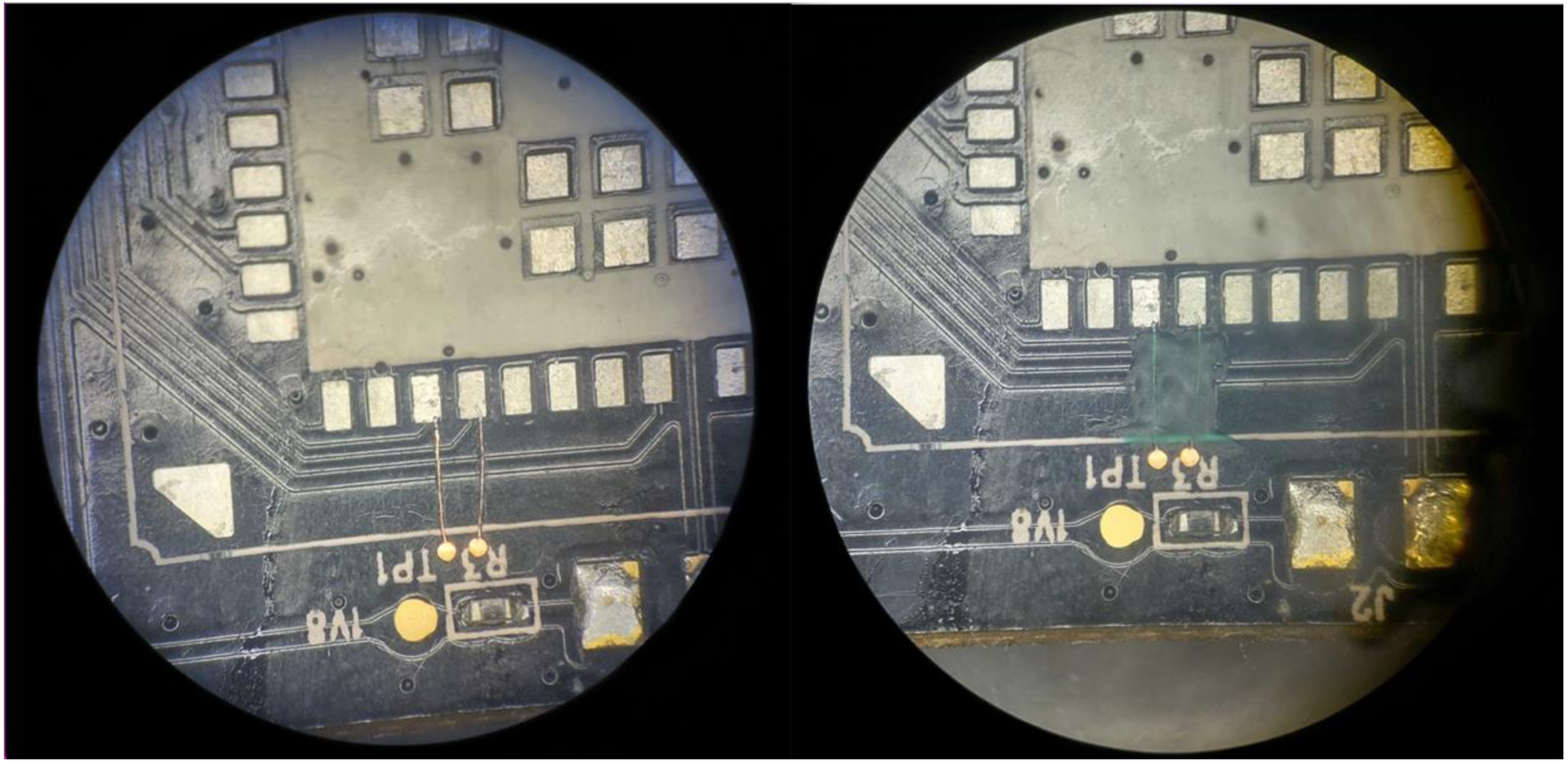
What if USB & UART Are Not Bot Accessible?

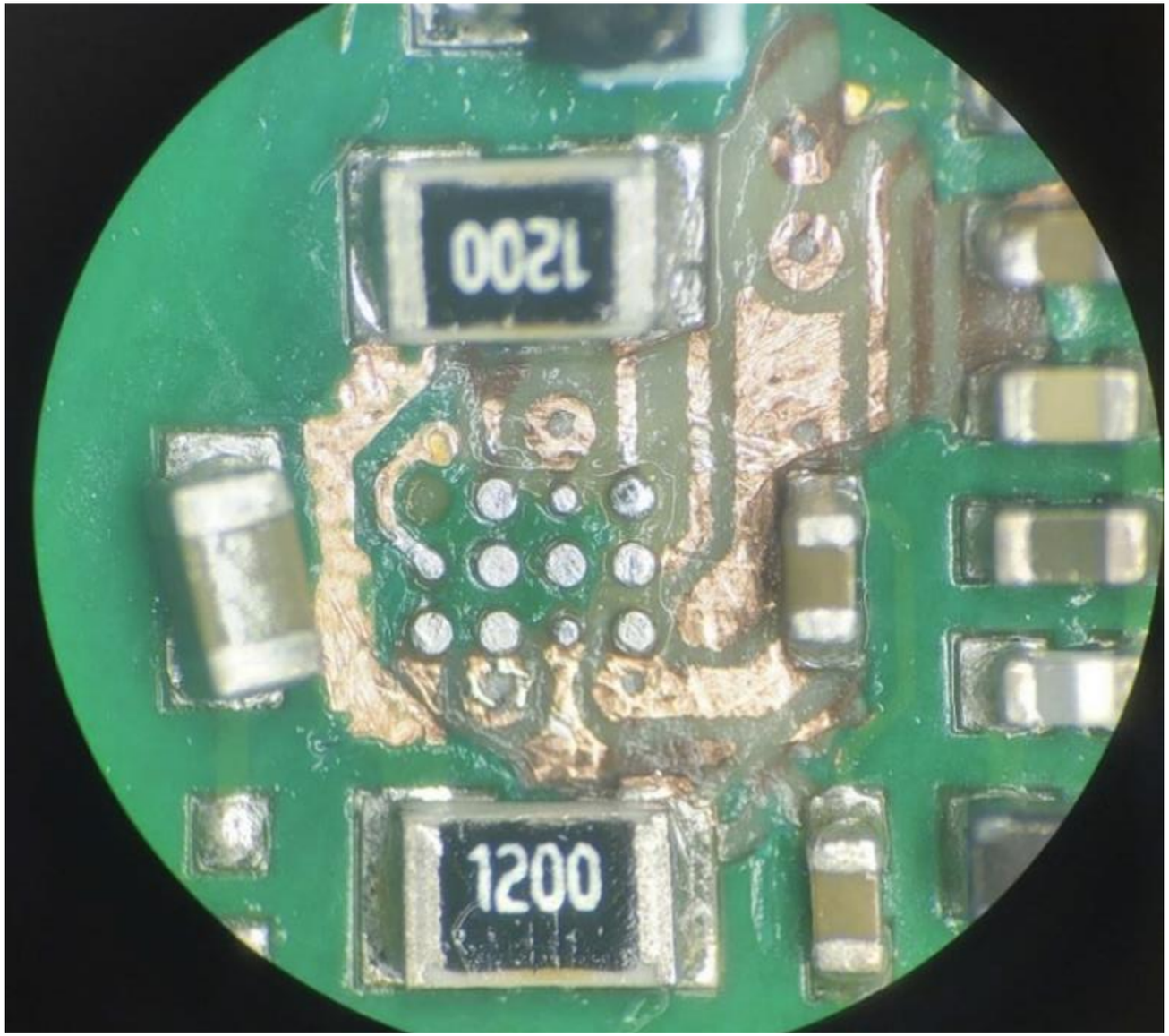
- Acupuncture needles
- Circuit run modifications
- Cut through sublayers




G95M1
C10

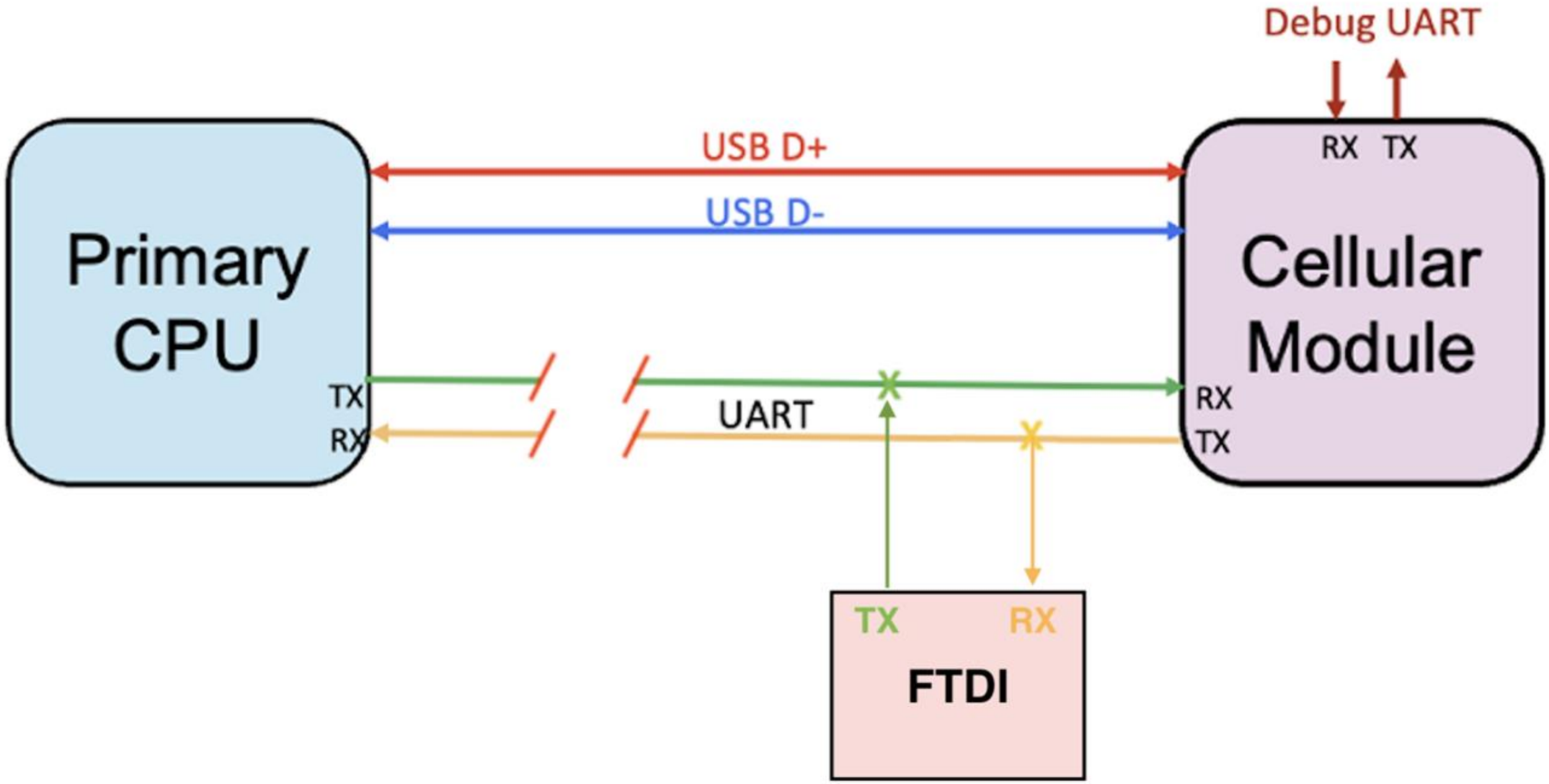


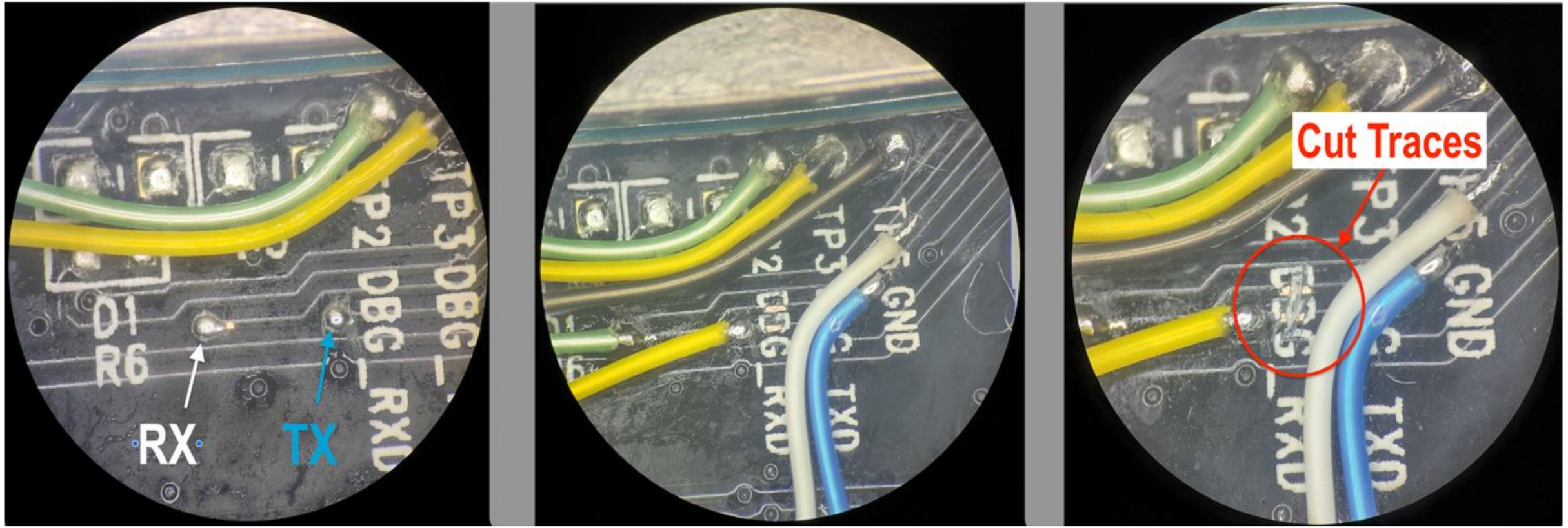

R3
TP1
1V8
R3
TP1
1V8
J2

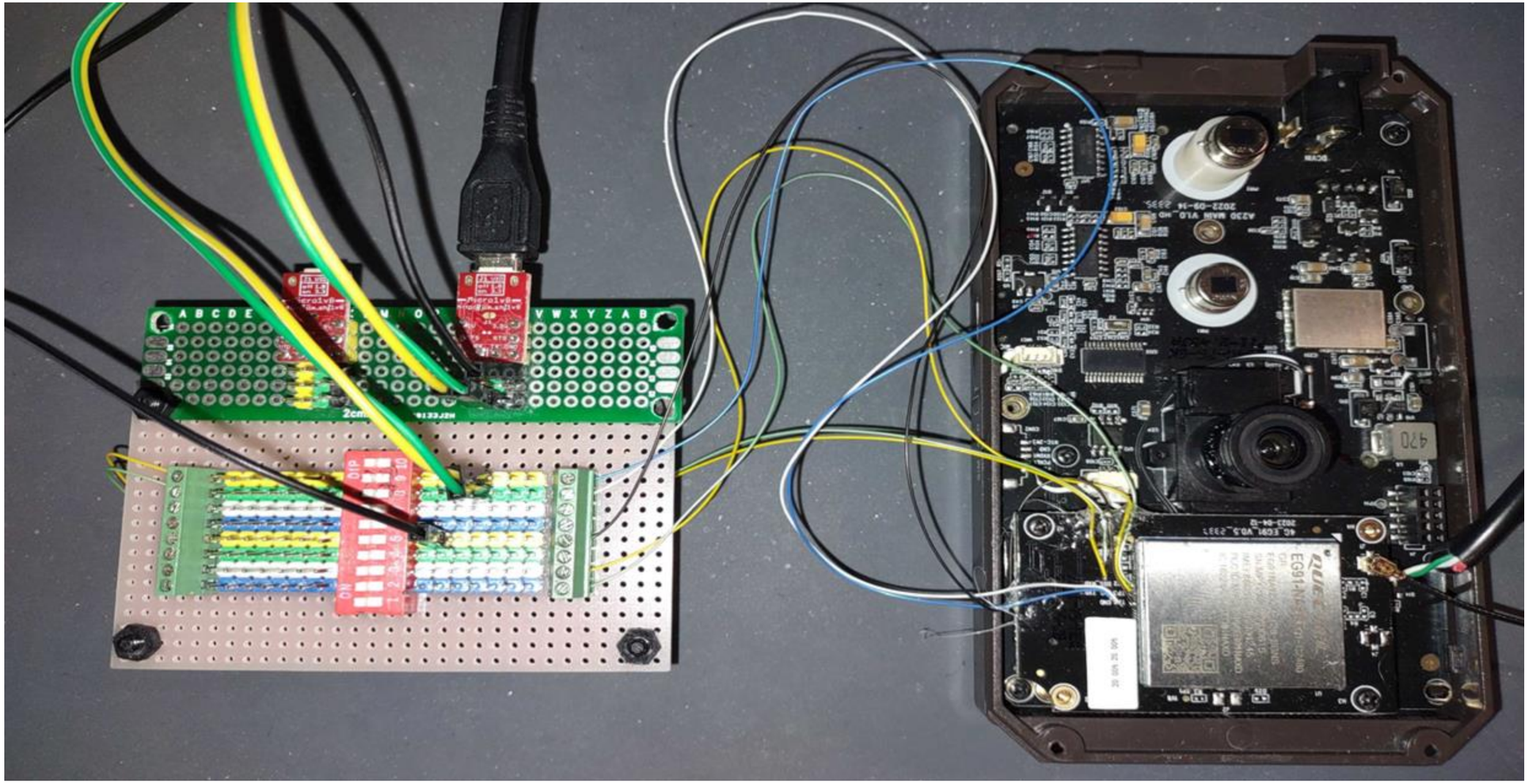

1200
1200

Weaponization

The Mechanics of UART


Debug UART
RX
TX
USB D+
USB D-
Primary CPU
TX
RX
UART
Cellular Module
RX
TX
TX
RX
FTDI


R6
RX
TX
Cut Traces



HTTP and Sockets

- Vendor-specific AT commands for HTTP and sockets
- Allows communications to cloud and internet-facing resources
- HTTPS support varies across modules and may be limited or inconsistent

```
AT+QIOPEN=1,0,"TCP","44.213.105.7",80,0,0

OK

+QIOPEN: 0,0
AT+QISEND=0

> GET / HTTP/1.1
Host: 44.213.105.7
User-Agent: EG91
Connection: close
```

```
+QIRD: 319
HTTP/1.1 403 Forbidden
Date: Fri, 25 Jul 2025 00:25:15 GMT
Server: Apache/2.4.62 (Amazon Linux)
Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
ETag: "2d-432a5e4a73a80"
Accept-Ranges: bytes
Content-Length: 45
Connection: close
Content-Type: text/html; charset=UTF-8

<html><body><h1>It works!</h1></body></html>


OK
```

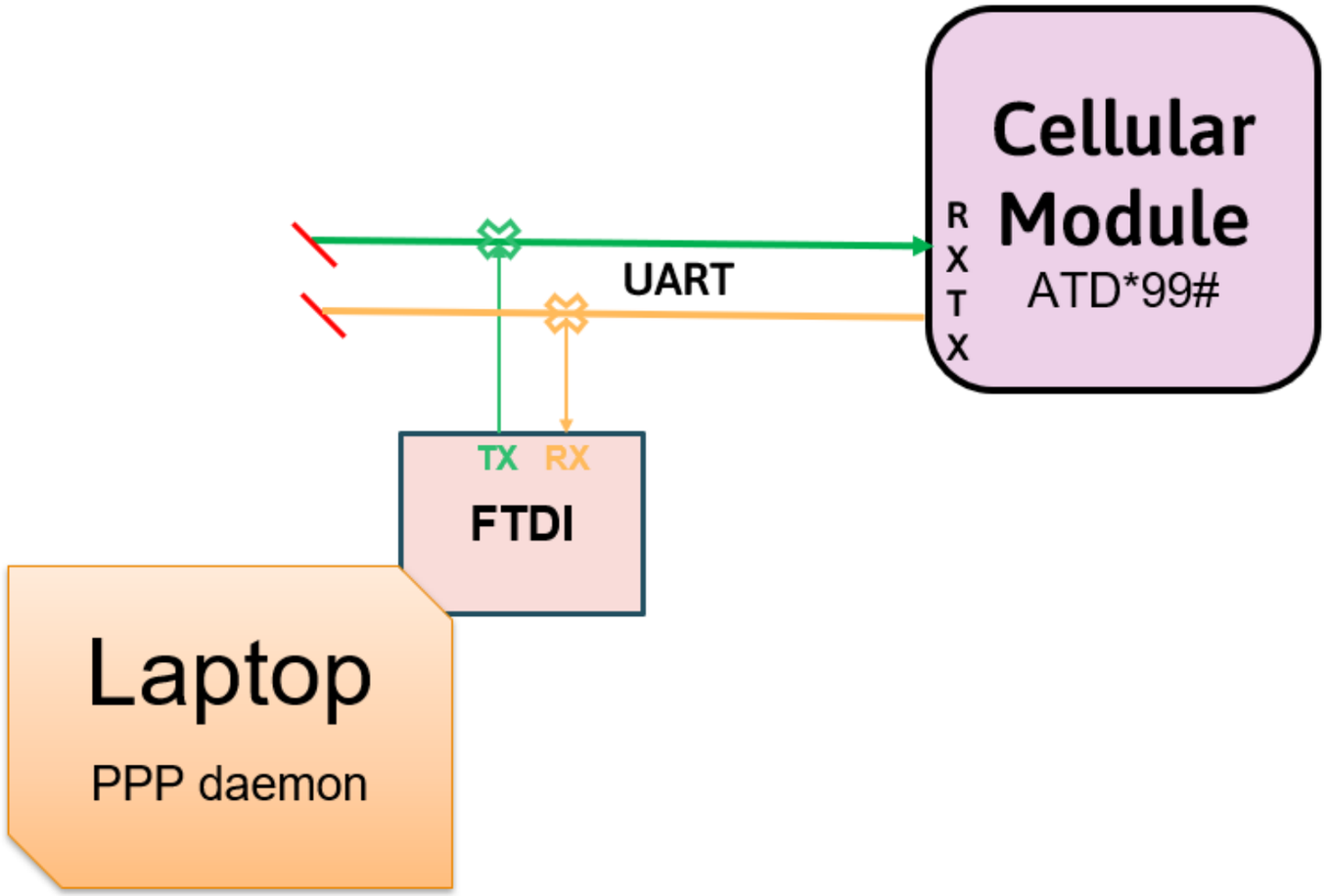
```
[MODEM] HTTPS GET: https://research-cellbucket1.s3.us-east-1.amazonaws.com/flag2.txt
[MODEM] >> AT+QHTTPURL=65,30
[MODEM] << AT+QHTTPURL=65,30
[MODEM] << CONNECT
[MODEM] >> AT+QHTTPGET=60
[MODEM] <<
[MODEM] << OK
[MODEM] << AT+QHTTPGET=60
[MODEM] << OK
[MODEM] <<
[MODEM] << +QHTTPGET: 0,404
[MODEM] >> AT+QHTTPREAD=30
[MODEM] << AT+QHTTPREAD=30
[MODEM] << CONNECT
[MODEM] << <?xml version="1.0" encoding="UTF-8"?>
[MODEM] << <Error><Code>NoSuchKey</Code><Message>The
RequestId><HostId>yI0pI89BBMb6ObDZTYlc3E4WdPgC0qxiWB
[MODEM] << OK
[MODEM] Response Body (truncated):
AT+QHTTPREAD=30
CONNECT
<?xml version="1.0" encoding="UTF-8"?>
<Error><Code>NoSuchKey</Code><Message>The specified key does not exist.</Message><Key>flag2.txt</Key><RequestId>9X2ADHEAXME049ZH</RequestId><
HostId>yI0pI89BBMb6ObDZTYlc3E4WdPgC0qxiWBzVj1JuK9o2dXXr6n0MHorUIXzyLeNmhpWa5B7Mnuk=</HostId></Error>
OK
NOT FOUND https://research-cellbucket1.s3.us-east-1.amazonaws.com/flag2.txt → HTTP 404
[MODEM] HTTPS GET: https://research-cellbucket1.s3.us-east-1.amazonaws.com/Flag1.txt
[MODEM] >> AT+QHTTPURL=65,30
[MODEM] <<
[MODEM] << +QHTTPREAD: 0
[MODEM] << AT+QHTTPURL=65,30
[MODEM] << CONNECT
[MODEM] >> AT+QHTTPGET=60
[MODEM] <<
```

DEMO

PPP over UART

Provides network access via serial:

- Establishes IP network interface
- Compatible with standard TCP/IP stacks
- Modem handles cellular network layer
- After initial setup, no AT commands



Downloads — sudo ◂ Python CellPPP.py --device /dev/tty.usbserial-A5069RR4 --baud 115200 --apn flolive.net — 141×38

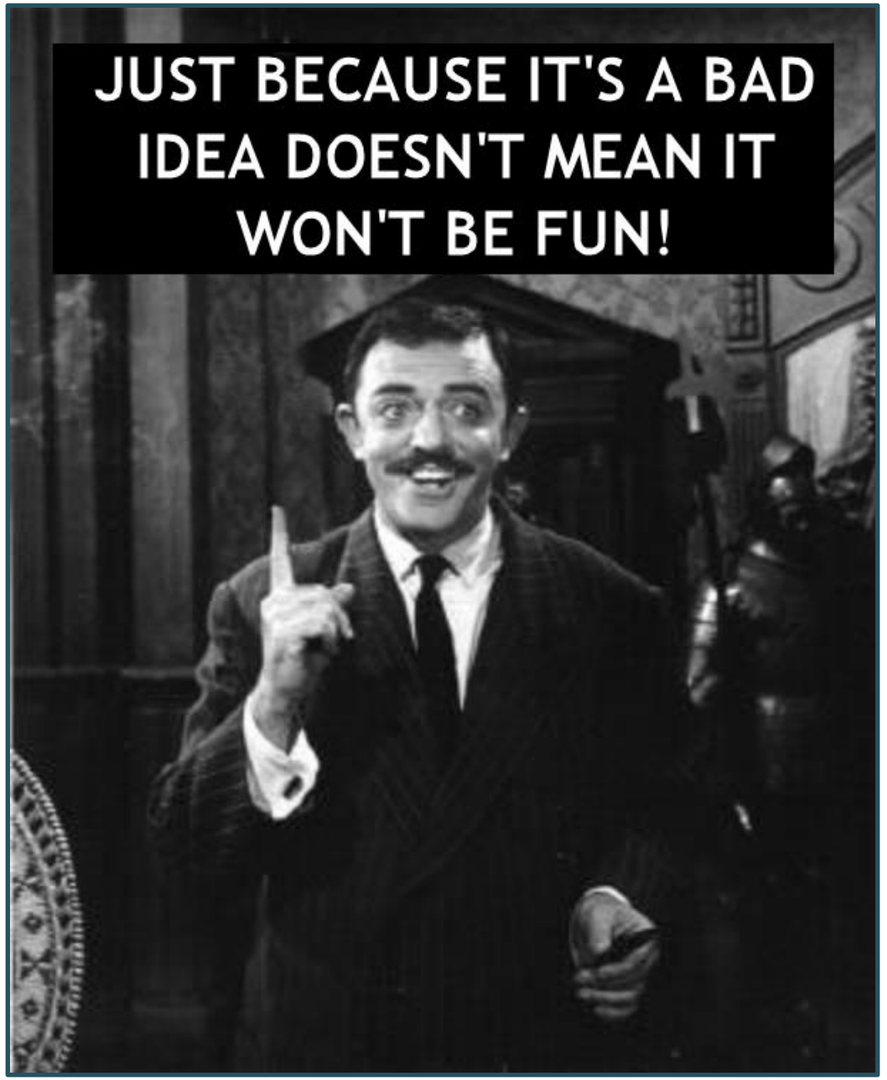
```
Wed Jul 23 18:55:44 2025 : rcvd [LCP ConfReq id=0x0 <asyncmap 0x0> <auth chap MD5> <magic 0x7a2cc10a> <pcomp> <accomp>]
Wed Jul 23 18:55:44 2025 : lcp_reqci: returning CONFREJ.
Wed Jul 23 18:55:44 2025 : sent [LCP ConfRej id=0x0 <pcomp> <accomp>]
Wed Jul 23 18:55:44 2025 : rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x623e01f5>]
Wed Jul 23 18:55:44 2025 : rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <auth chap MD5> <magic 0x7a2cc10a>]
Wed Jul 23 18:55:44 2025 : lcp_reqci: returning CONFACK.
Wed Jul 23 18:55:44 2025 : sent [LCP ConfAck id=0x1 <asyncmap 0x0> <auth chap MD5> <magic 0x7a2cc10a>]
Wed Jul 23 18:55:44 2025 : rcvd [LCP DiscReq id=0x2 magic=0x7a2cc10a]
Wed Jul 23 18:55:44 2025 : rcvd [CHAP Challenge id=0x1 <c7b6dbeb97d117e73ad88d31d945aec7>, name = "UMTS_CHAP_SRVR"]
Wed Jul 23 18:55:44 2025 : sent [CHAP Response id=0x1 <c731bca8afb0cb7e771043ce163c4ad0>, name = "admin"]
Wed Jul 23 18:55:44 2025 : rcvd [CHAP Success id=0x1 ""]
Wed Jul 23 18:55:44 2025 : CHAP authentication succeeded
Wed Jul 23 18:55:44 2025 : sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns3 0.0.0.0>]
Wed Jul 23 18:55:44 2025 : sent [ACSCP ConfReq id=0x1 <route vers 16777216> <domain vers 16777216>]
Wed Jul 23 18:55:44 2025 : rcvd [LCP ProtRej id=0x3
Wed Jul 23 18:55:44 2025 : rcvd [IPCP ConfReq id=0x0
Wed Jul 23 18:55:44 2025 : ipcp: returning Configure
Wed Jul 23 18:55:44 2025 : sent [IPCP ConfNak id=0x0
Wed Jul 23 18:55:44 2025 : rcvd [IPCP ConfNak id=0x1 <addr 100.64.139.49> <ms-dns1 1.1.1.1> <ms-dns3 8.8.8.8>]
Wed Jul 23 18:55:44 2025 : sent [IPCP ConfReq id=0x2 <addr 100.64.139.49> <ms-dns1 1.1.1.1> <ms-dns3 8.8.8.8>]
Wed Jul 23 18:55:44 2025 : rcvd [IPCP ConfReq id=0x1]
Wed Jul 23 18:55:44 2025 : ipcp: returning Configure-ACK
Wed Jul 23 18:55:44 2025 : sent [IPCP ConfAck id=0x1]
Wed Jul 23 18:55:44 2025 : rcvd [IPCP ConfAck id=0x2 <addr 100.64.139.49> <ms-dns1 1.1.1.1> <ms-dns3 8.8.8.8>]
Wed Jul 23 18:55:44 2025 : ipcp: up
Wed Jul 23 18:55:44 2025 : Could not determine remote IP address: defaulting to 10.64.64.64
Wed Jul 23 18:55:44 2025 : local  IP address 100.64.139.49
Wed Jul 23 18:55:44 2025 : remote IP address 10.64.64.64
Wed Jul 23 18:55:44 2025 : primary   DNS address 1.1.1.1
Wed Jul 23 18:55:44 2025 : secondary DNS address 8.8.8.8
Wed Jul 23 18:55:44 2025 : Received protocol dictionaries
Wed Jul 23 18:55:44 2025 : Received acsp/dhcp dictionaries
Wed Jul 23 18:55:44 2025 : Committed PPP store
Wed Jul 23 18:55:44 2025 : Received acsp/dhcp dictionaries
Wed Jul 23 18:55:44 2025 : Committed PPP store
✅ Default route is now through ppp0:
default            link#19            UCSg                ppp0
```

DEMO

UART Pros and Cons

- Low level of effort
- PPP over UART

- Slower speeds and limited data throughput
- APN may not support PPP



Weaponization

The Mechanics of USB

USB Interfacing

- Can I gain access to and control the USB?
- What technical issues will I need to deal with?
- Where do I even start?

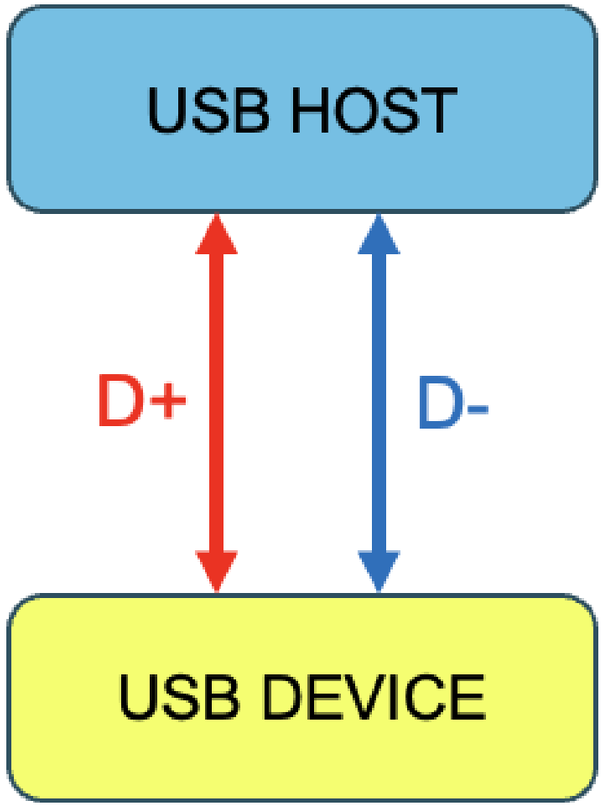
USB Interfacing

Termination & impedance matching resistors

Trace length limitation

Trace spacing

- Prevent crosstalk
- Signal reflections
- Impedance mismatch



USB Interfacing

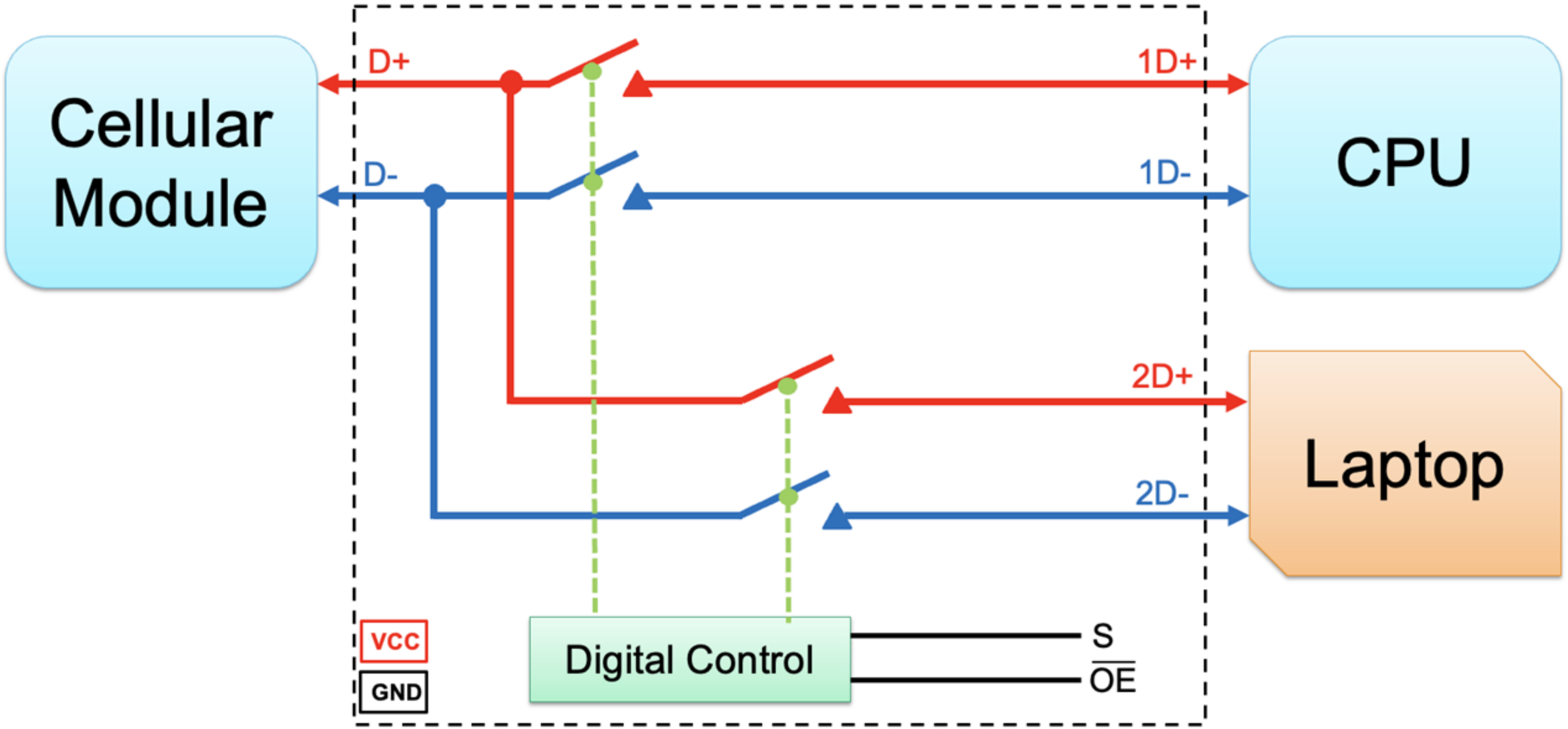
Texas Instrument

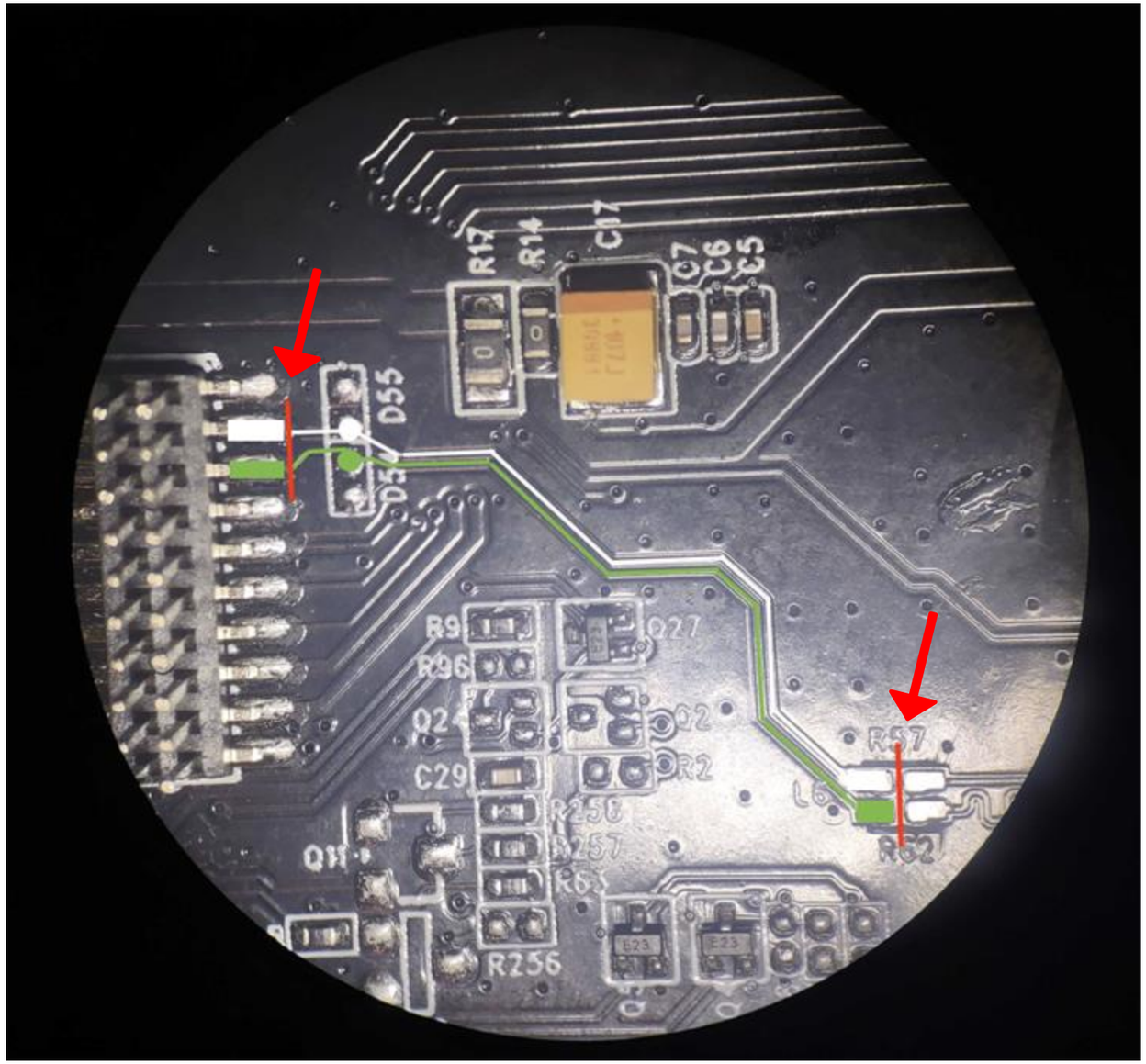
- TS3USB221E High-Speed USB 2.0 (480Mbps) 1:2 Multiplexer

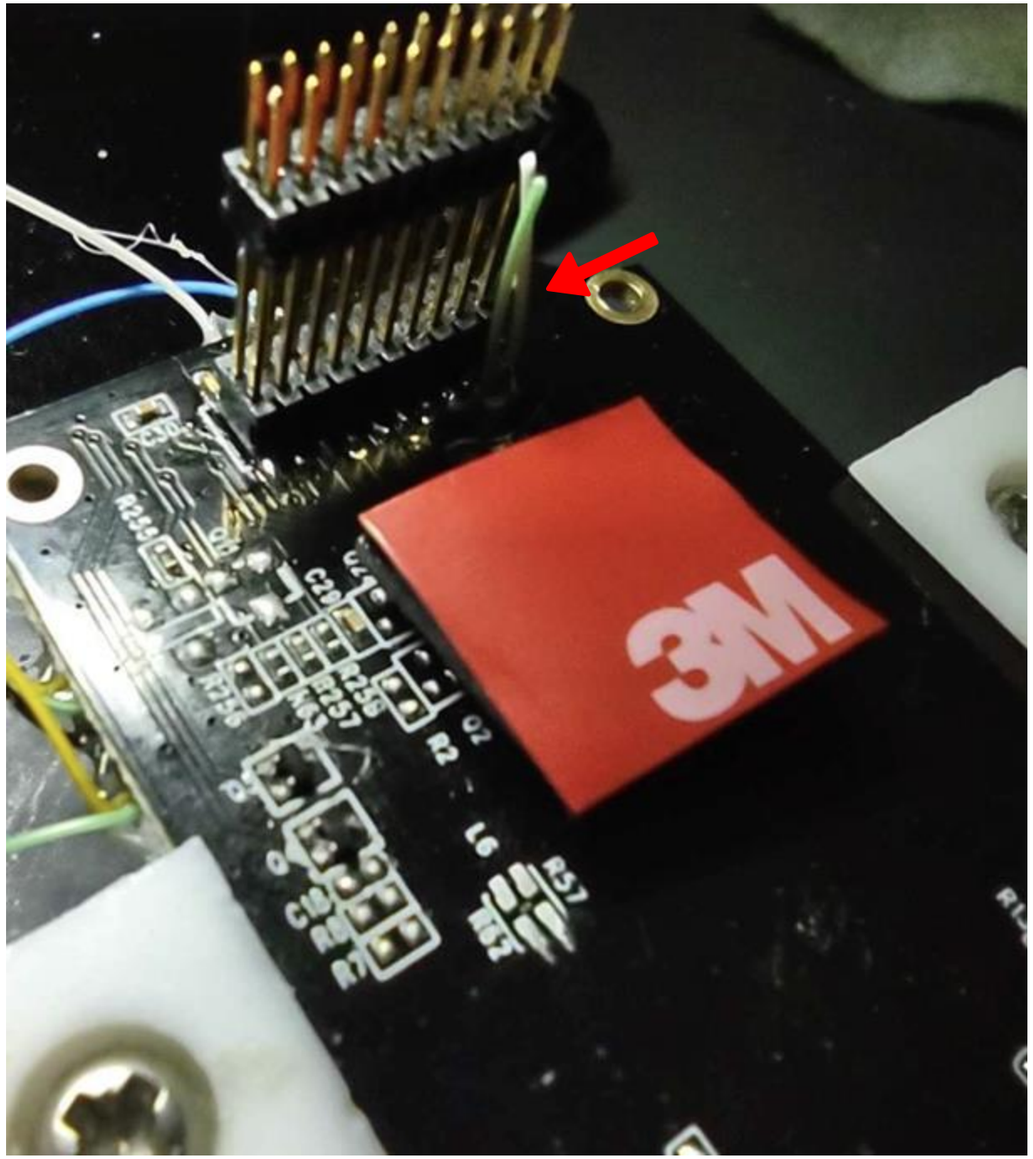
Pre-assembled Board (China)

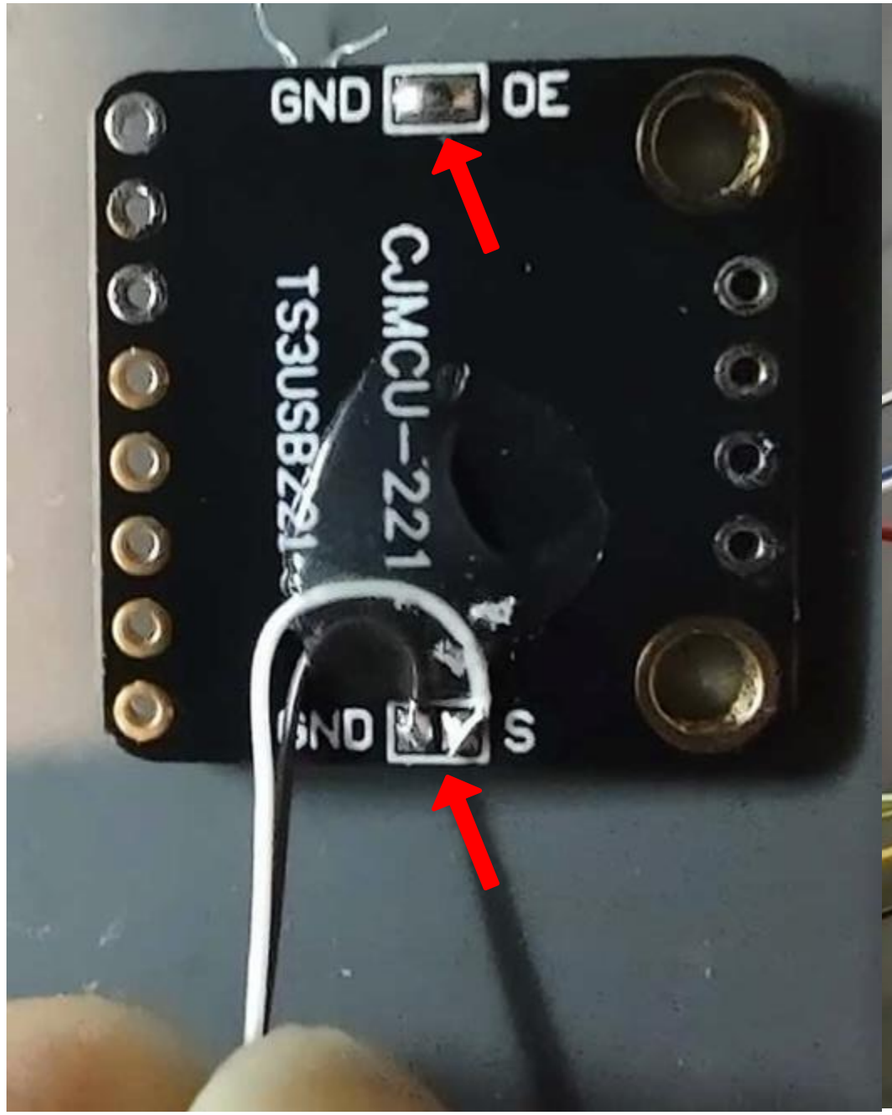
- Solved electronic requirement
- Now, how do I splice this in?

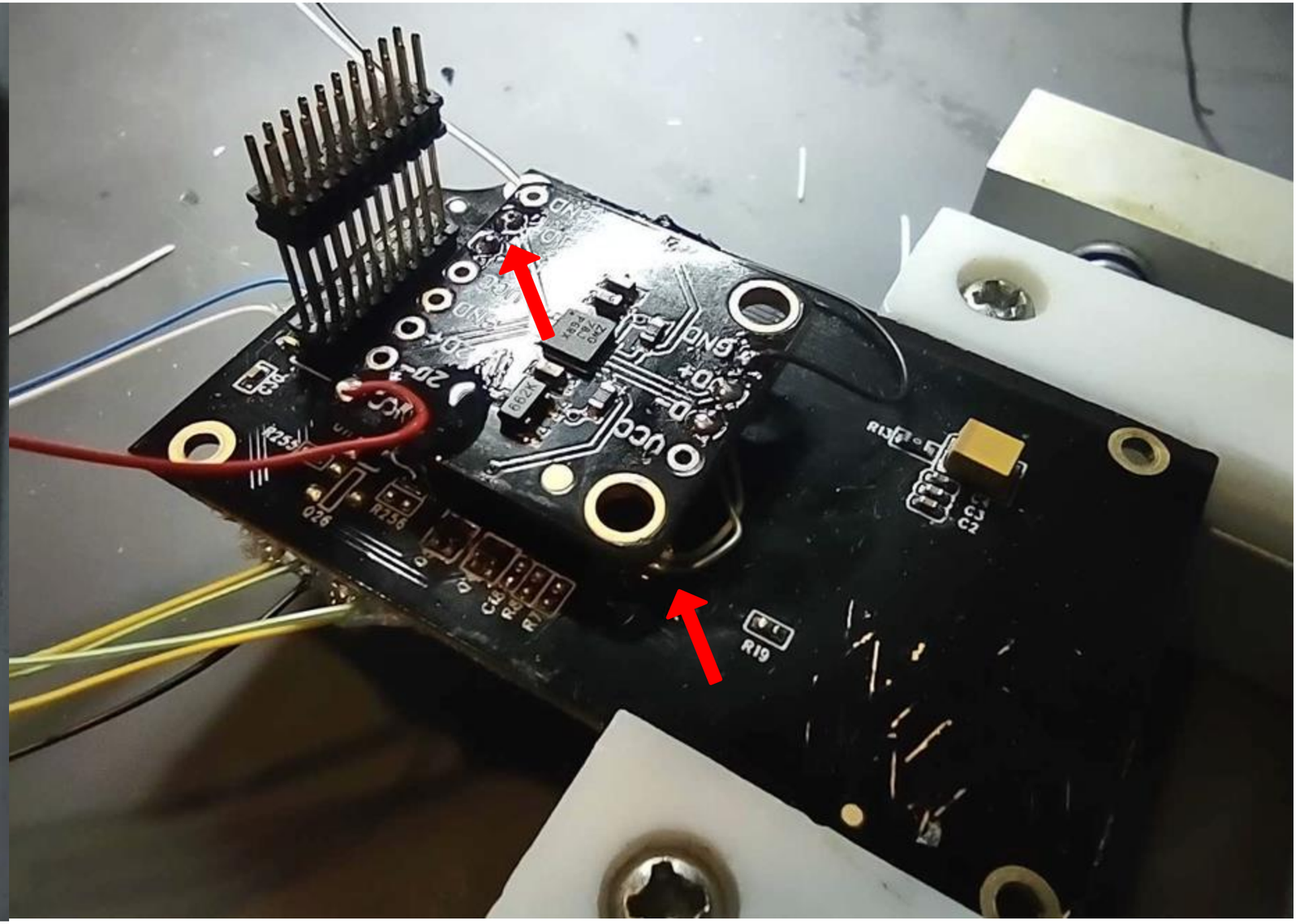
USB Multiplexer

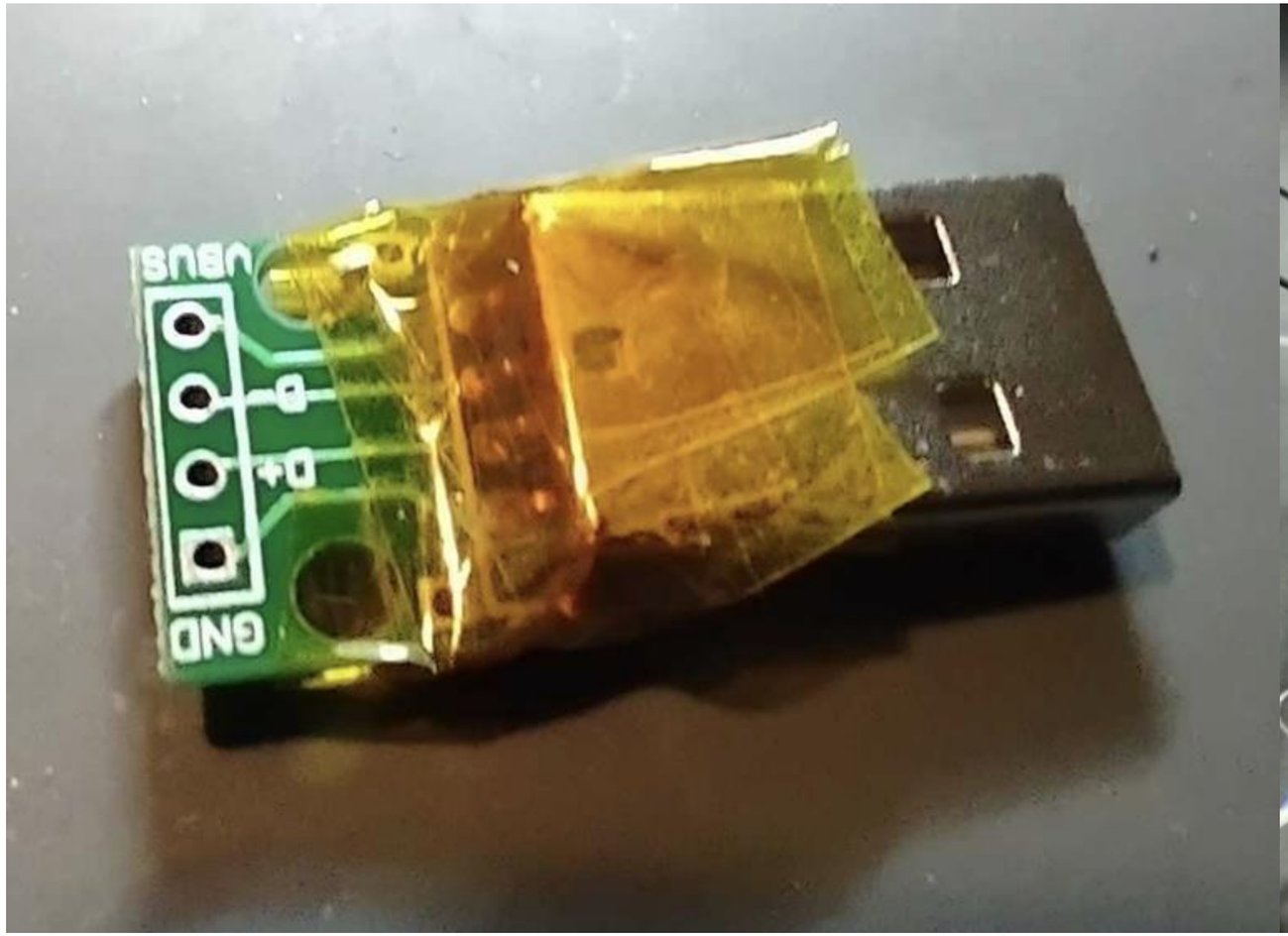


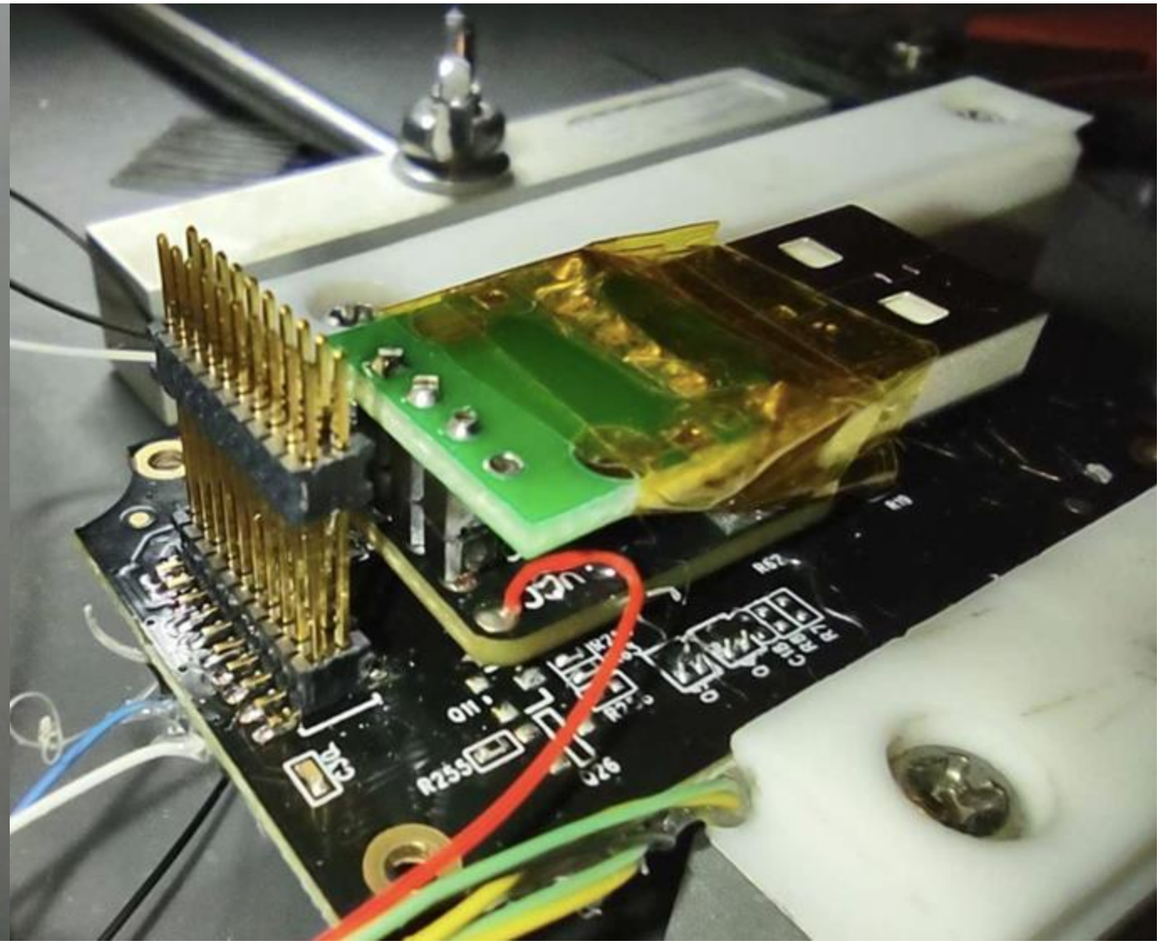

R17
R14
C17
C7
C6
C5
D55
D5
R9
R96
Q27
Q24
Q2
C29
R2
R57
R52
R256
Q11

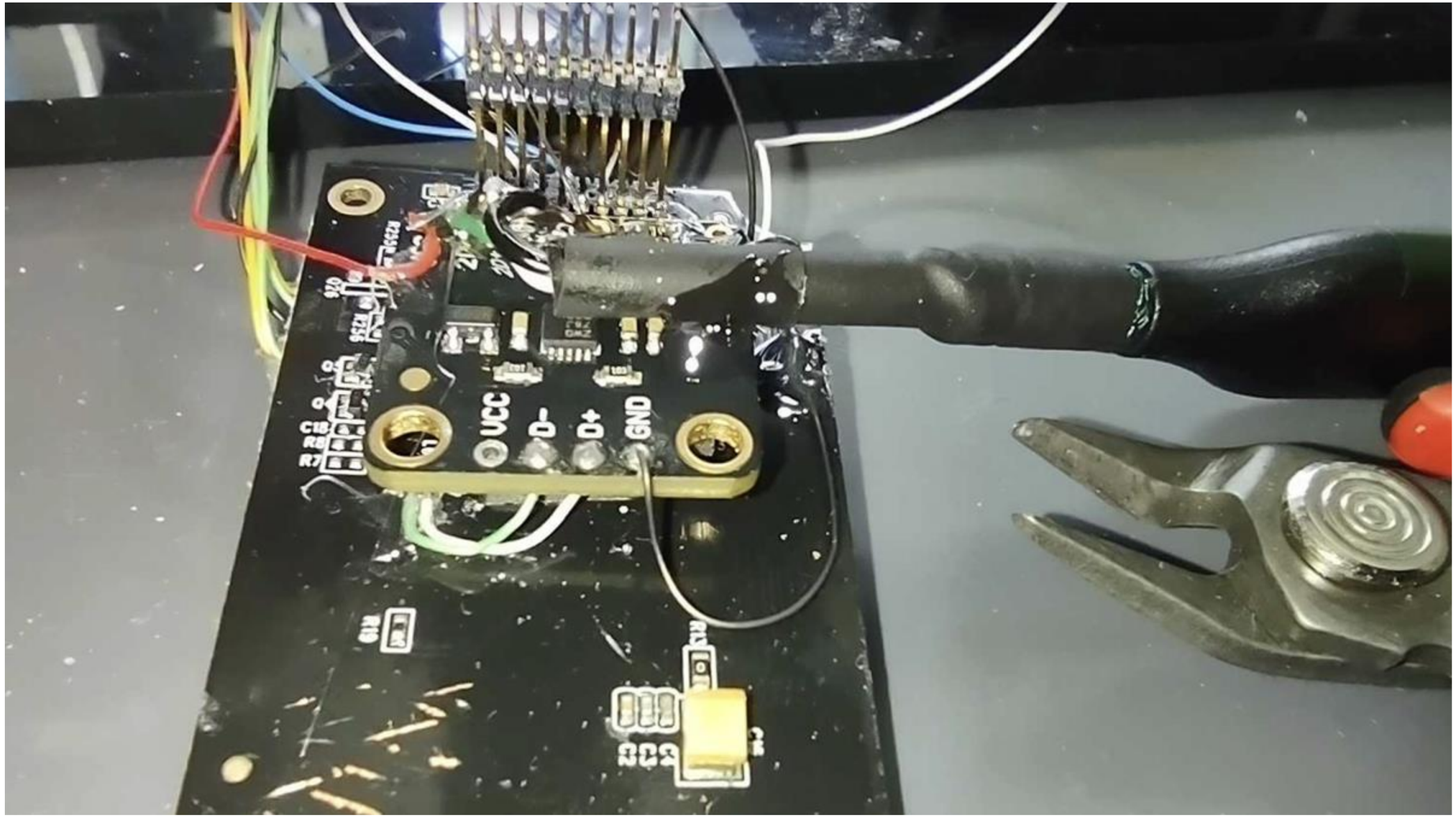

3M

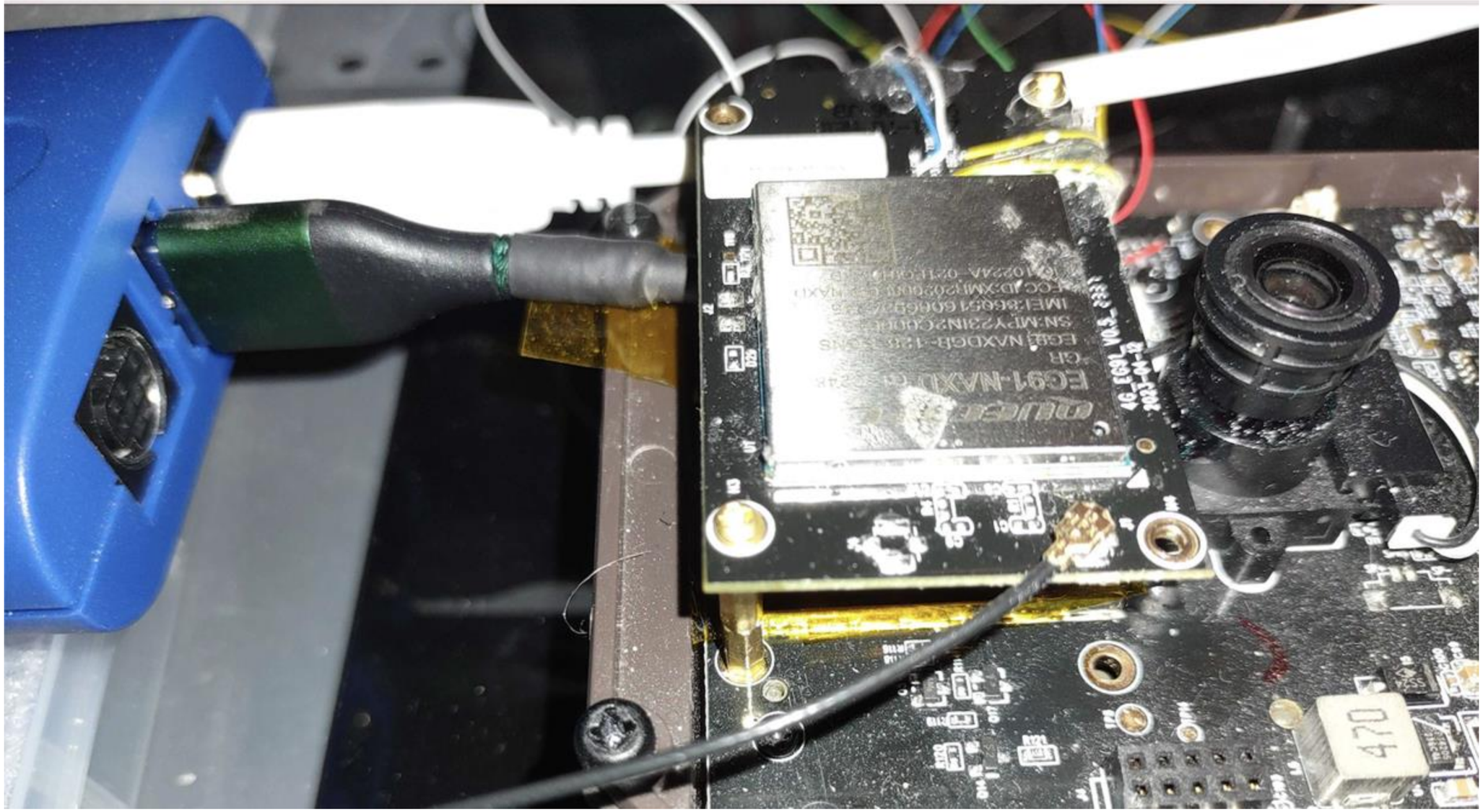

GND
OE
CJMCU-221
GND
S

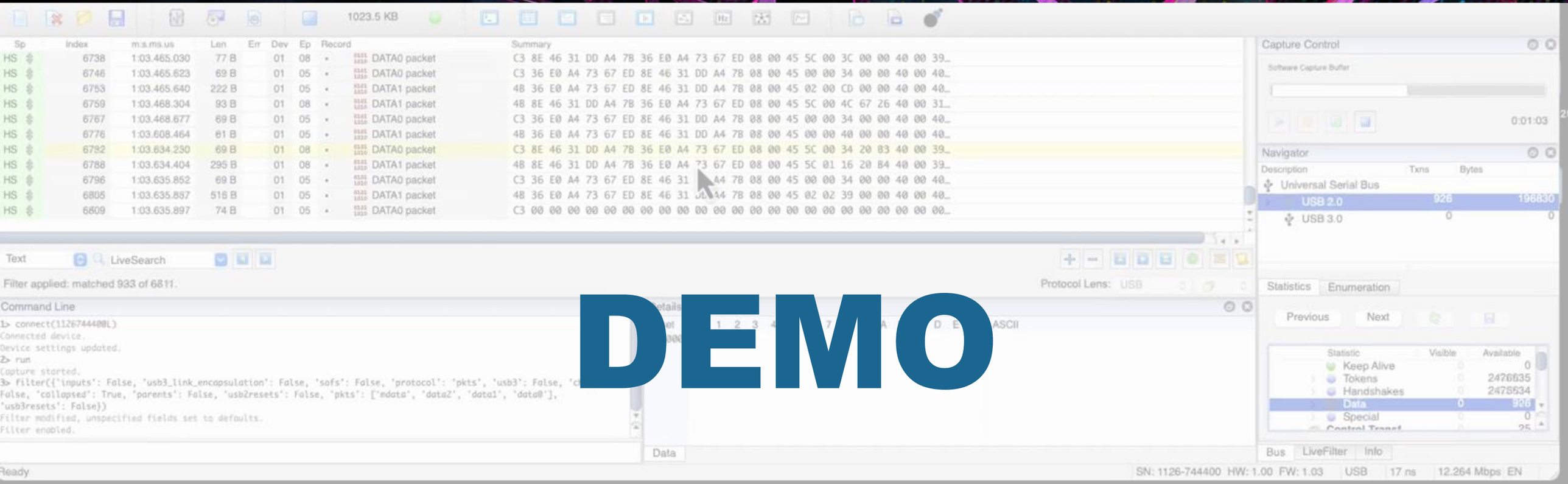



VBUS
D+
GND




VCC
D-
D+
GND


EC91-NAXD
420


1023.5 KB
Sp Index m:s.ms.us Len Err Dev Ep Record Summary
HS 6738 1:03.465.030 77 B 01 08 DATA0 packet C3 8E 46 31 DD A4 7B 36 E0 A4 73 67 ED 08 00 45 5C 00 3C 00 00 40 00 39…
HS 6746 1:03.465.623 69 B 01 05 DATA0 packet C3 36 E0 A4 73 67 ED 8E 46 31 DD A4 7B 08 00 45 00 00 34 00 00 40 00 40…
HS 6753 1:03.465.640 222 B 01 05 DATA1 packet 4B 36 E0 A4 73 67 ED 8E 46 31 DD A4 7B 08 00 45 02 00 CD 00 00 40 00 40…
HS 6759 1:03.468.304 93 B 01 08 DATA1 packet 4B 8E 46 31 DD A4 7B 36 E0 A4 73 67 ED 08 00 45 5C 00 4C 67 26 40 00 31…
HS 6767 1:03.468.677 69 B 01 05 DATA0 packet C3 36 E0 A4 73 67 ED 8E 46 31 DD A4 7B 08 00 45 00 00 34 00 00 40 00 40…
HS 6776 1:03.608.464 61 B 01 05 DATA1 packet 4B 36 E0 A4 73 67 ED 8E 46 31 DD A4 7B 08 00 45 00 00 40 00 00 40 00 40…
HS 6792 1:03.634.230 69 B 01 08 DATA0 packet C3 8E 46 31 DD A4 7B 36 E0 A4 73 67 ED 08 00 45 5C 00 34 20 83 40 00 39…
HS 6788 1:03.634.404 295 B 01 08 DATA1 packet 4B 8E 46 31 DD A4 7B 36 E0 A4 73 67 ED 08 00 45 5C 01 16 20 B4 40 00 39…
HS 6796 1:03.635.852 69 B 01 05 DATA0 packet C3 36 E0 A4 73 67 ED 8E 46 31 A4 7B 08 00 45 00 00 34 00 00 40 00 40…
HS 6805 1:03.635.857 516 B 01 05 DATA1 packet 4B 36 E0 A4 73 67 ED 8E 46 31 A4 7B 08 00 45 02 02 39 00 00 40 00 40…
HS 6809 1:03.635.897 74 B 01 05 DATA0 packet C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00…
Capture Control
Software Capture Buffer
0:01:03
Navigator
Description Txns Bytes
Universal Serial Bus
USB 2.0 926 196830
USB 3.0 0 0
Text LiveSearch
Filter applied: matched 933 of 6811.
Protocol Lens: USB
Command Line
1> connect(1126744400L)
Connected device.
Device settings updated.
2> run
Capture started.
3> filter({'inputs': False, 'usb3_link_encapsulation': False, 'sofs': False, 'protocol': 'pkts', 'usb3': False,
False, 'collapsed': True, 'parents': False, 'usb2resets': False, 'pkts': ['mdata', 'data2', 'data1', 'data0'],
'usb3resets': False})
Filter modified, unspecified fields set to defaults.
Filter enabled.
Statistics Enumeration
Previous Next
Statistic Visible Available
Keep Alive 0 0
Tokens 0 2476635
Handshakes 0 2476534
Data 0 926
Special 0 0
Bus LiveFilter Info
Data
Ready
SN: 1126-744400 HW: 1.00 FW: 1.03 USB 17 ns 12.264 Mbps EN

DEMO


Untitled_0
RDY
AT
OK
usbserial-140 / 115200 8-N-1
Connected 00:00:47, 38,584 / 4 bytes
TX RTS DTR DCD
RX CTS DSR RI

USB Pros & Cons

USB ECM (Ethernet Control Model)

- Supported drivers on most host OS's
- All standard tools at your disposal

Complex Hardware Hacking

- Limited bandwidth (NB-IoT)
- Latency issues (NB-IoT)

Security Mitigation Strategies

Mitigations

Tamper Protection

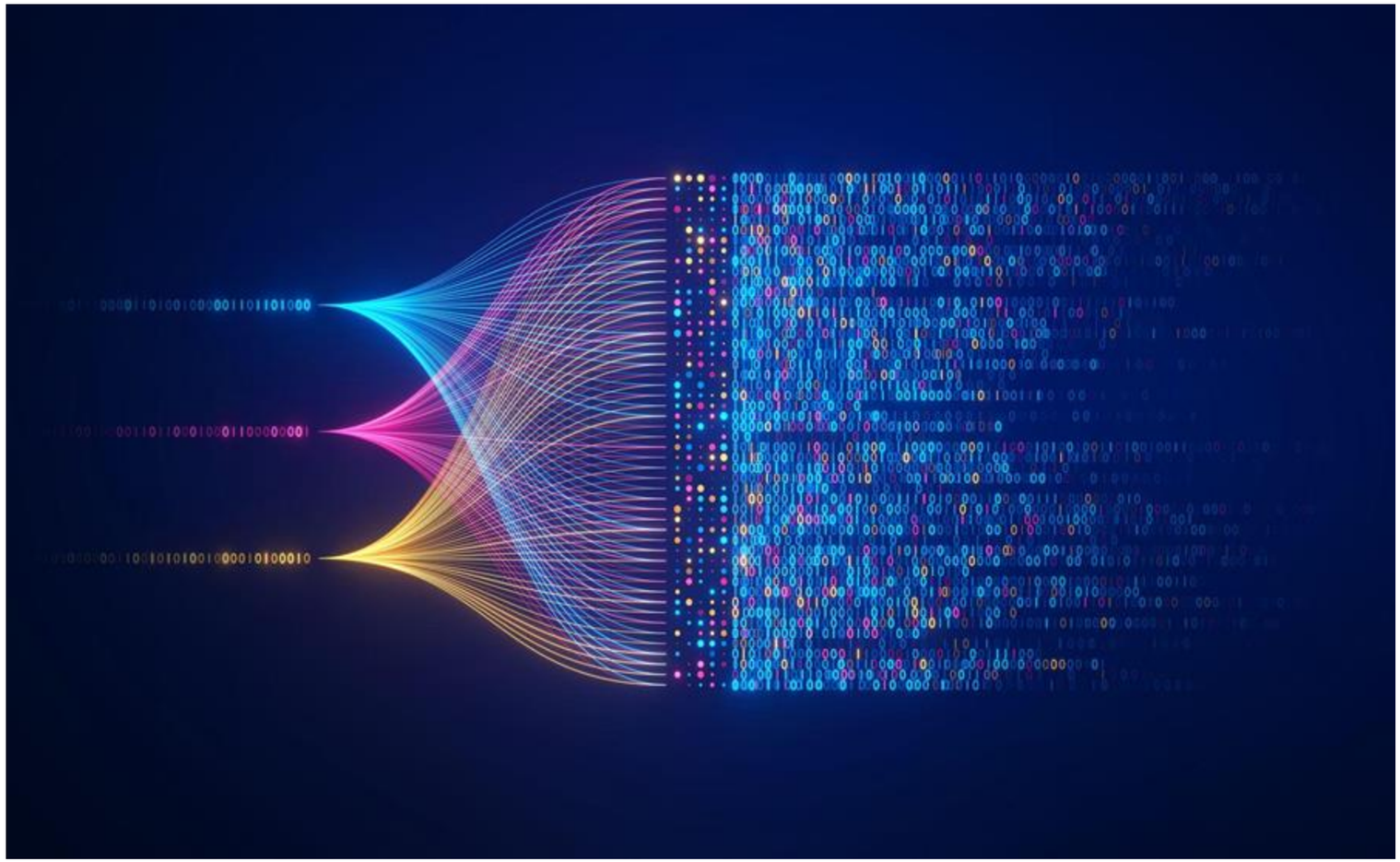
- Case triggers
- Epoxy potting

Disable USB/UART

- Physically
- Software
- AT commands

Using a SIM Card PIN or Password

Communication Encrypted



Mitigations (cont.)

APN monitoring

- Cellular bandwidth usage
- Behavior

Internal network security monitoring

Segmentation

Re-evaluate current security

- Models & Methodologies
- Threat modeling

Product Security testing

One Last Comment

Two communication channels (USB/UART) also allows a cellular-enabled IoT device to be modified so it can phone home and be used for any number of nefarious activities

- C2
- Surveillance
- Remote function triggers
- No impact on devices' normal functionality
  - Vendor may not know
  - Vendor never sees the traffic
  - End user not aware

"Black Hat Sound Bytes"

- Cellular module AT language allow easy construction of tool to weaponizing cellular modules in IoT devices.
- Cellular enabled IoT devices' trusted access allows for compromise and attacks against cloud & internet services and private network environments.
- Mitigation of these threats are not easy. How do you protect a device against its normal functions from being used against you – General good security practices such as, limit access to only what is needed, segmentation, and monitoring.

Conclusion & Questions

Deral Heiland
Principal Security Research (IoT), Rapid7
deral_heiland@rapid7.com
@percent_x

RAPID7

Carlota Bindner
Lead Product Security Researcher
Thermo Fisher Scientific
@carlotabindner

- https://github.com/dheiland-r7/CellPOC
- https://github.com/dheiland-r7/CellMod

References

(1) Craig Peacock, (2010) , USB in a Nutshell, https://www.beyondlogic.org/usbnutshell/usb2.shtml

(2) Ken Munro, (2017). Hacking IoT vendors & smart cars via private APNs : https://www.pentestpartners.com/security-blog/hacking-iot-vendors-smart-cars-via-private-apns/

(3) Deral Heiland, Matthew Kienow, and Pearce Barry (2021), Leveraging Inter-chip Communication Analysis for Examining End-to-End Security within IoT Technology, https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-leveraging-inter-chip-communication-analysis.pdf

(4) Kaspersky ICS CERT researchers (2021), Kaspersky identifies significant security risks in widely-used Cinterion modems: https://usa.kaspersky.com/about/press-releases/kaspersky-identifies-significant-security-risks-in-widely-used-cinterion-modems

(5) Reza Vahidnia and F. John Dian (2021), Cellular Internet of Things for Practitioners, https://pressbooks.bccampus.ca/cellulariot/

(6) Renesas (2022), Data Over UART with PPP, https://www.mouser.com/pdfDocs/REN_r19an0071eu0150-lte-modules-data-over-uart-ppp_APN_20221012.pdf?srsltid=AfmBOor_Ti0_2v7S6bi-_ZisDiqg0pGebXr3glSYftYWGLWqbEaZwix6

(7) Deral Heiland and Carlota Bindner (2024), ANALYSIS OF CELLULAR BASED INTERNET OF THINGS (IOT) TECHNOLOGY, https://www.rapid7.com/globalassets/_pdfs/research/rapid7-2024-cellular-iot.pdf

(8) Jennifer C. Lin, Richard Y. Lin, and Salim S.I (2024), Cellular IoT Vulnerabilities: Another Door to Cellular Networks, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/cellular-iot-vulnerabilities-another-door-to-cellular-networks

(9)Texas Instruments (2024),TS3USB221E USB Multiplexer Datasheet , https://www.ti.com/lit/ds/symlink/ts3usb221e.pdf

(10) Jesal Shah (2025), How USB Works: Communication Protocol (Part 2), https://www.circuitbread.com/tutorials/how-usb-works-communication-protocol-part-2