Exploration of Cellular Based IoT Technology

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

Carlota Bindner
Lead Product Security Research
Thermo Fisher Scientific
@carlotabindner





Shout Out:

Damien Cauquil - HackInParis 2018

From printed circuit boards to exploits: pwning IoT devices like a boss

Intro to IoT Cellular

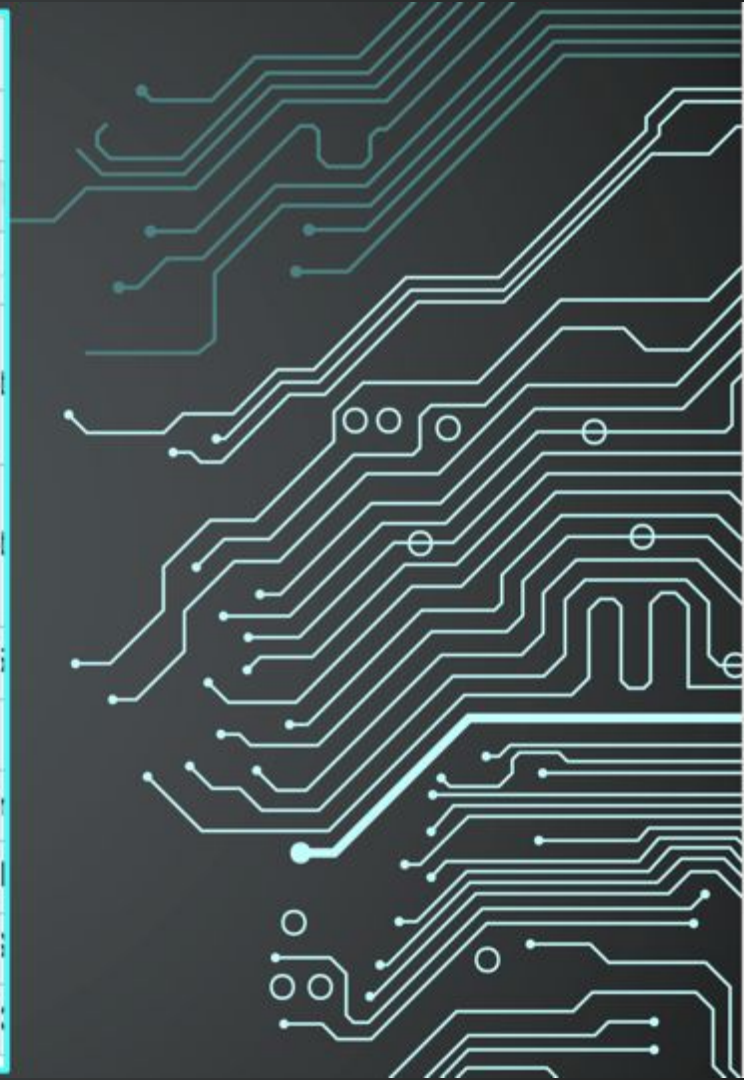


NB-IOT

	LTE Cat NB1	LTE Cat NB2
3GPP Release	Release 13	Release 14
Downlink Peak Rate	26 kbit/s	127 kbit/s
Uplink Peak Rate	66 kbit/s (multi-tone) 16.9 kbit/s (single-tone)	159 kbit/s
Latency	1.6–10 s	
Number of Antennas	1	1
Duplex Mode	Half Duplex	Half Duplex
Device Receive Bandwidth	180 kHz	180 kHz
Receiver Chains	1 (SISO)	1 (SISO)
Device Transmit Power	20 / 23 dBm	14 / 20 / 23 dBm

LTE-M

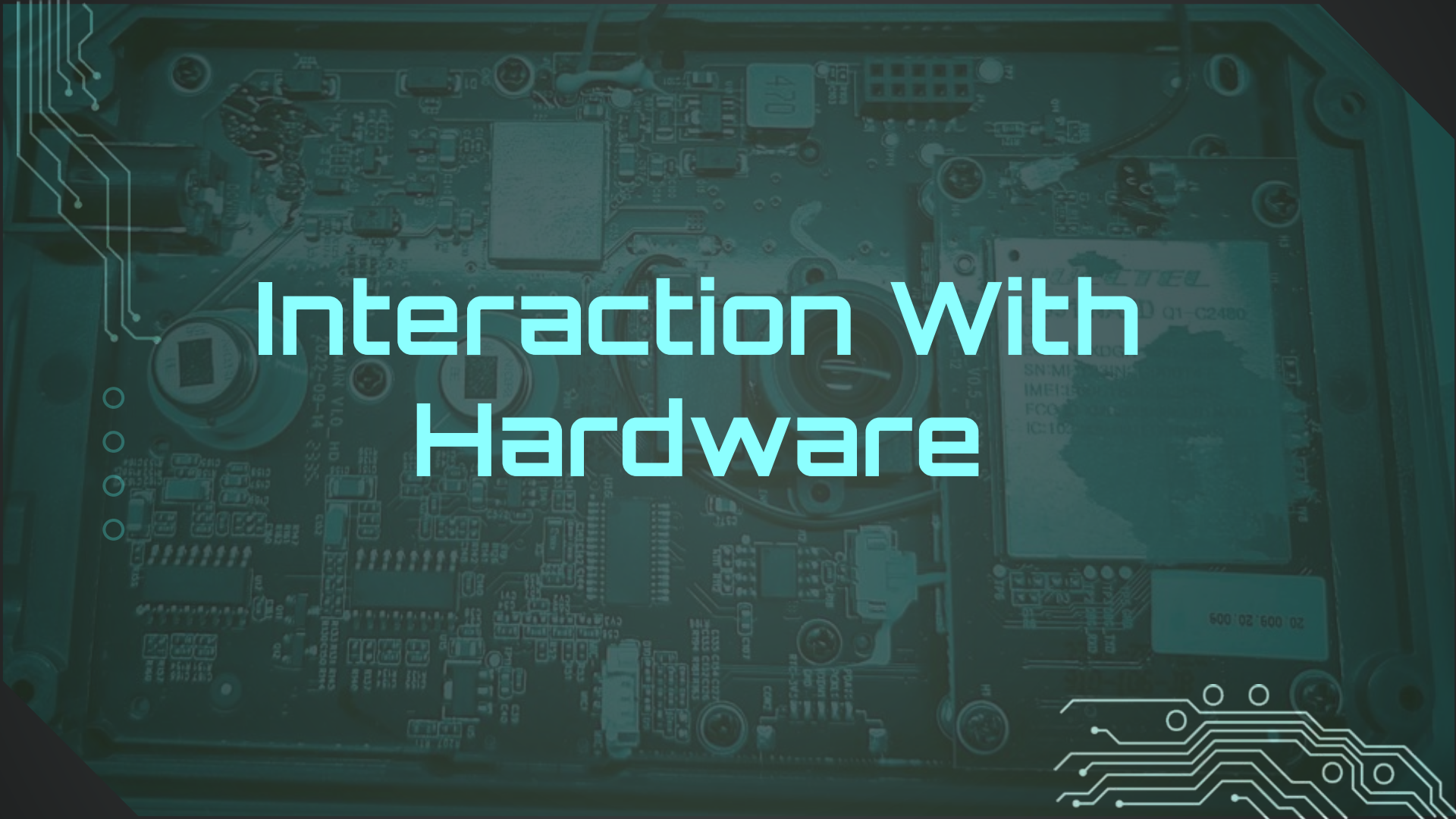
	eMTC	
	LTE Cat M1	LTE Cat M2
3GPP Release	Release 13	Release 14
Downlink Peak Rate	1 Mbit/s	~4 Mbit/s
Uplink Peak Rate	1 Mbit/s	~7 Mbit/s
Latency	10–15 ms	
Number of Antennas	1	1
Duplex Mode	Full or Half Duplex	Full or Half Duplex
Device Receive Bandwidth	1.4 MHz	5 MHz
Receiver Chains	1 (SISO)	1 (SISO)
Device Transmit Power	20 / 23 dBm	20 / 23 dBm



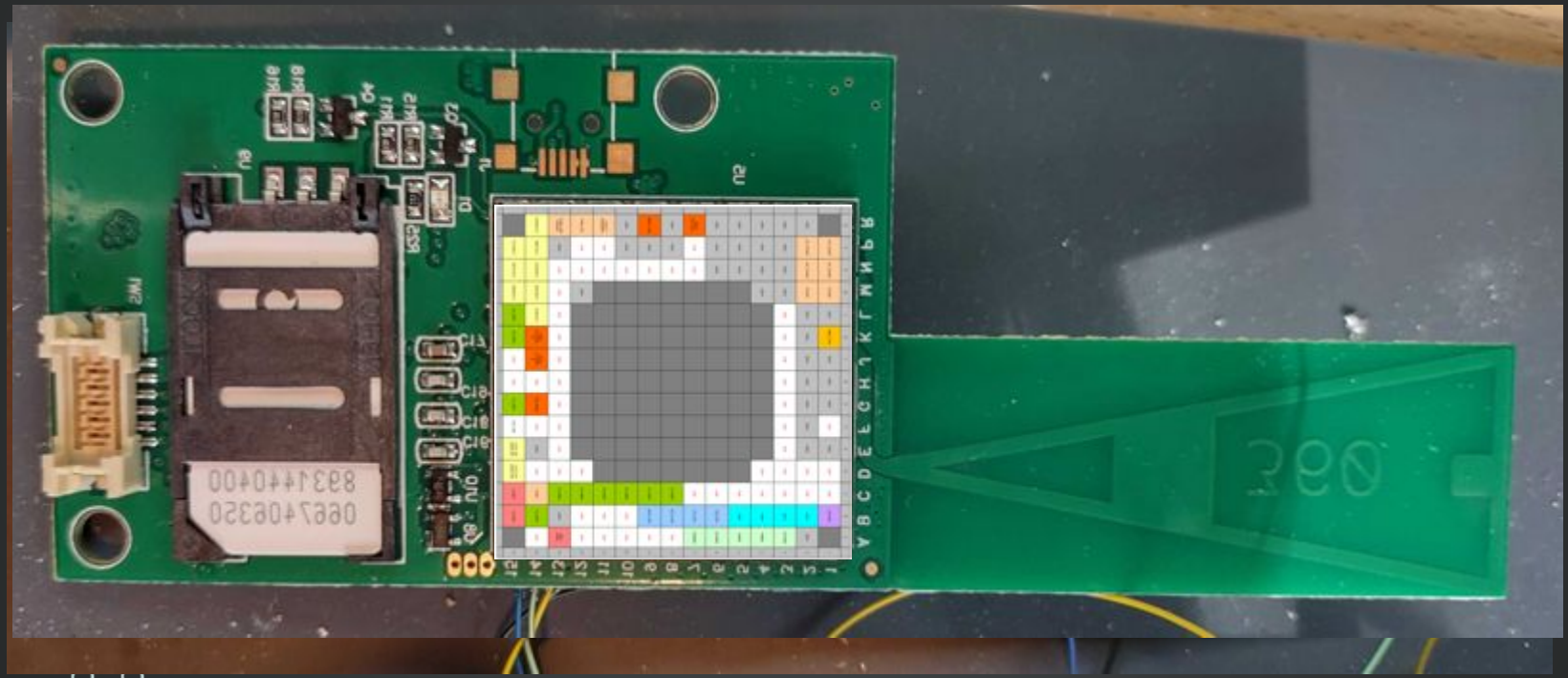
3GPP Release 15,16,17

- Network operation and efficiency improvements
- Improved access control
- Small-cell support
- Power management improvements
- Improved support of 5G services and features

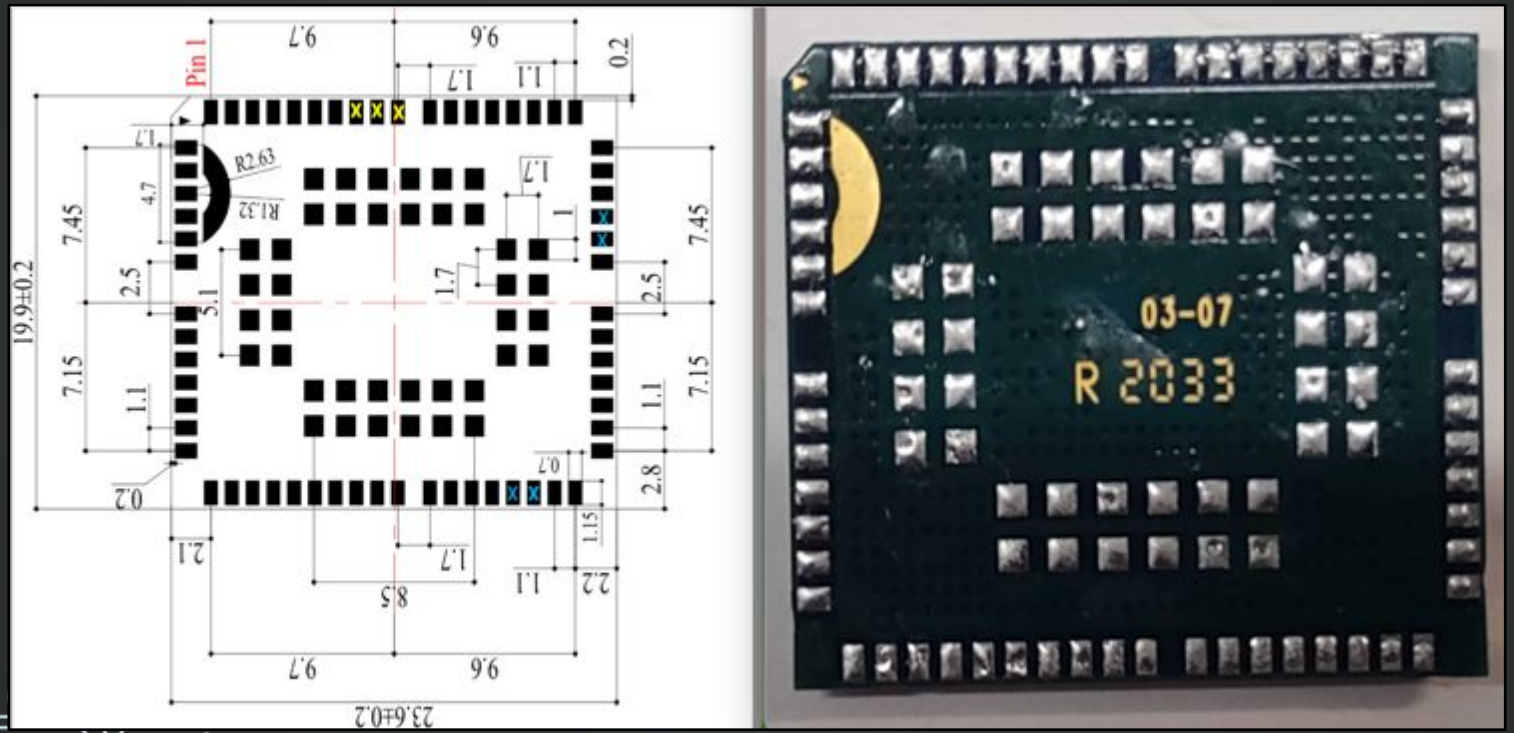



Interaction With
Hardware

Mapping Connection Point Paths

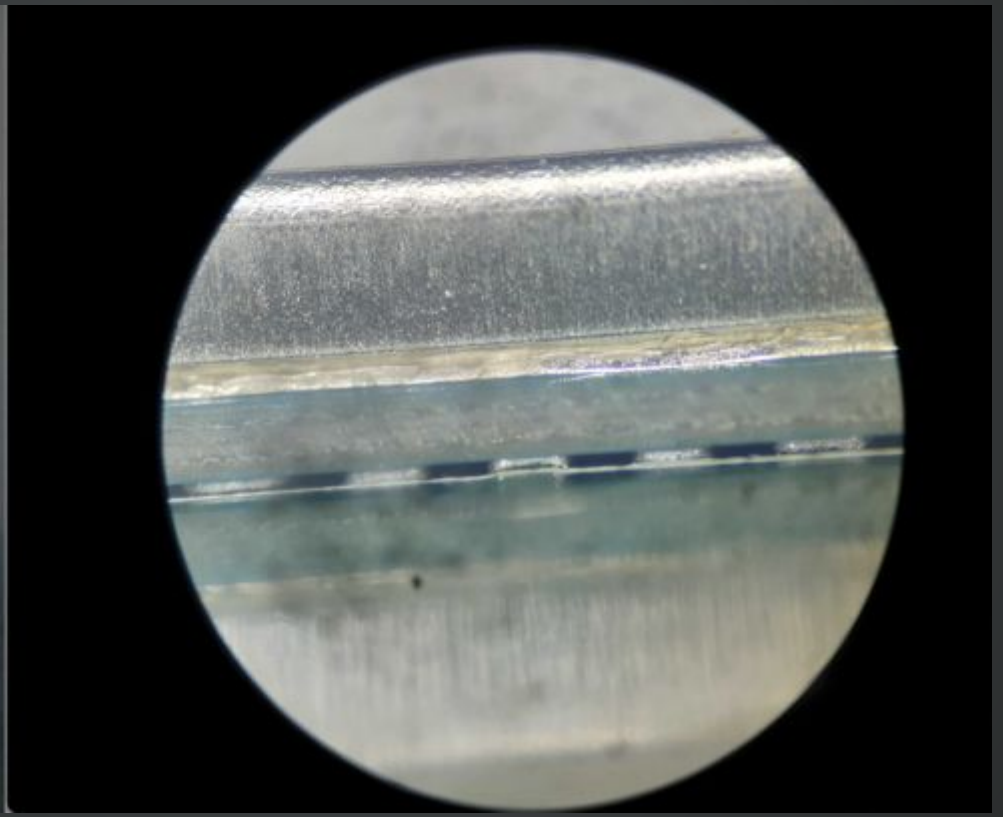


Sub-Module Access Method

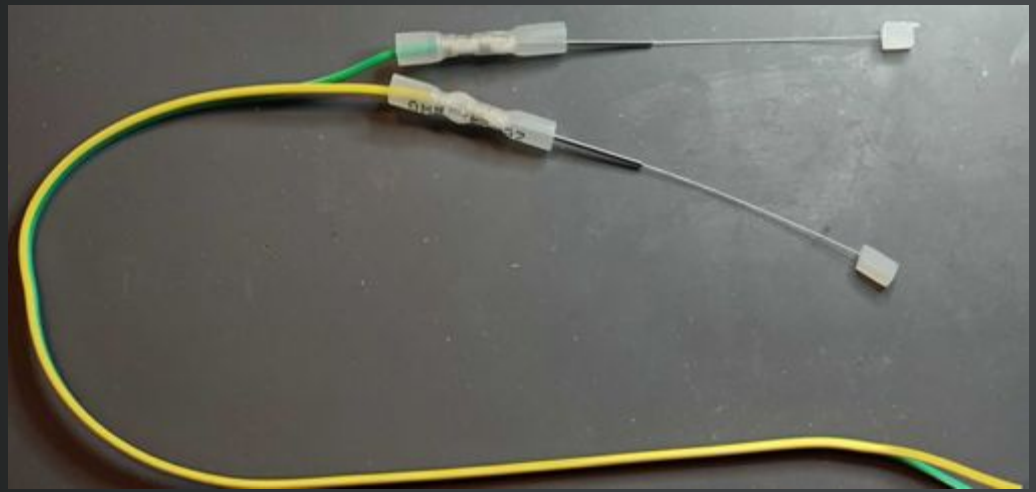


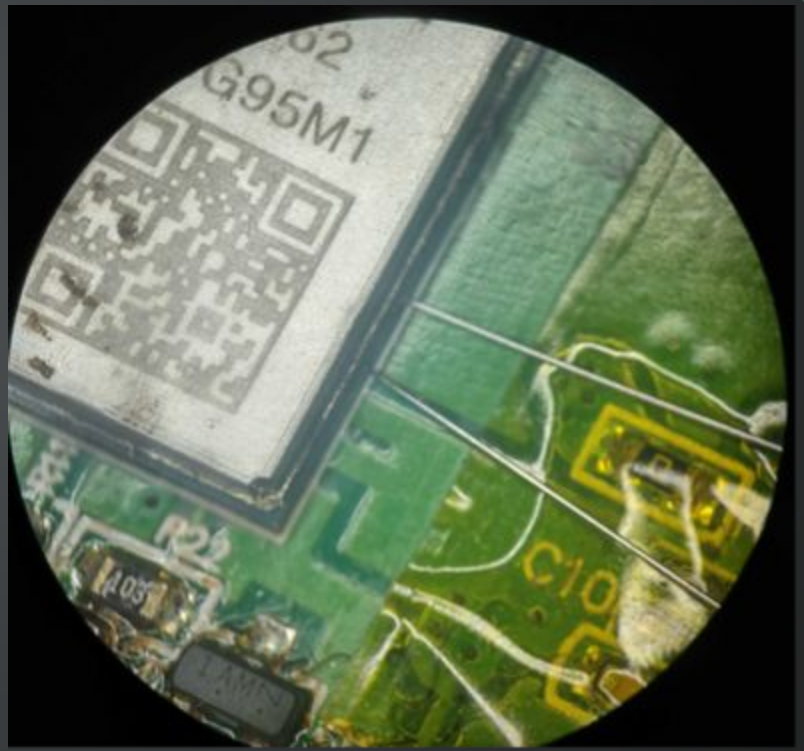
Sub-Module Access Method



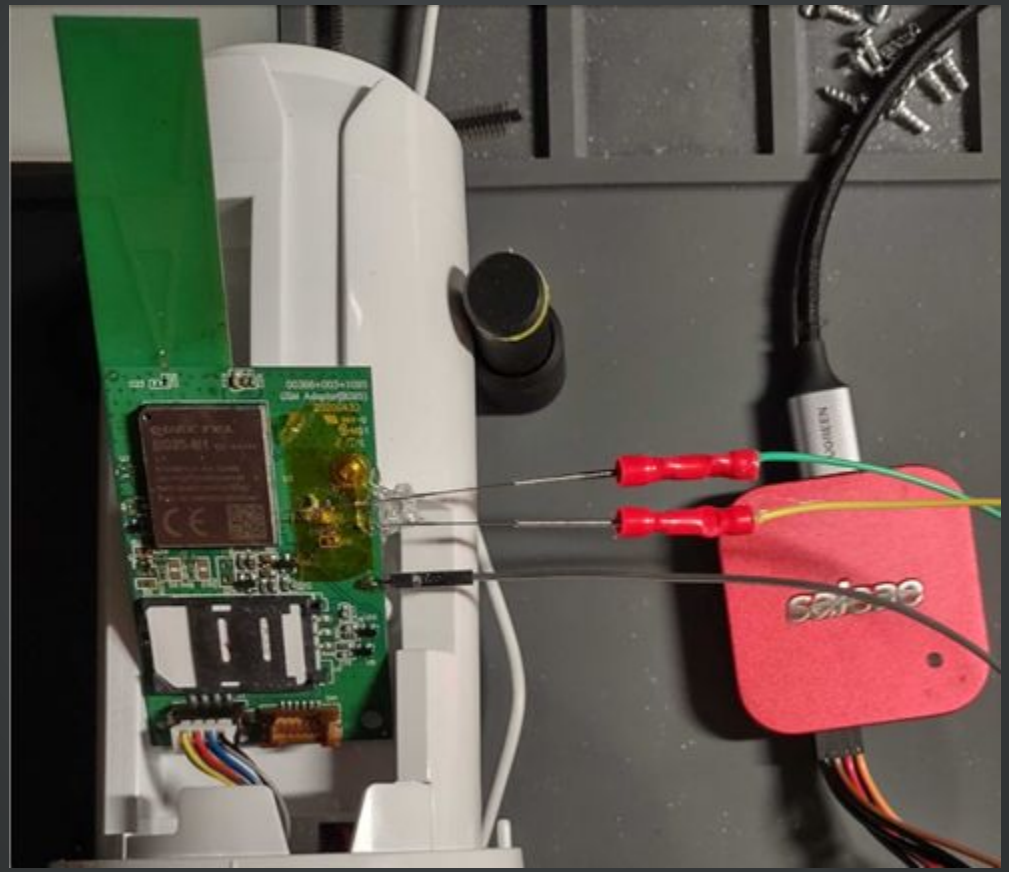


Sub-Module Access Method





Sub-Module Access Method



AT Commands

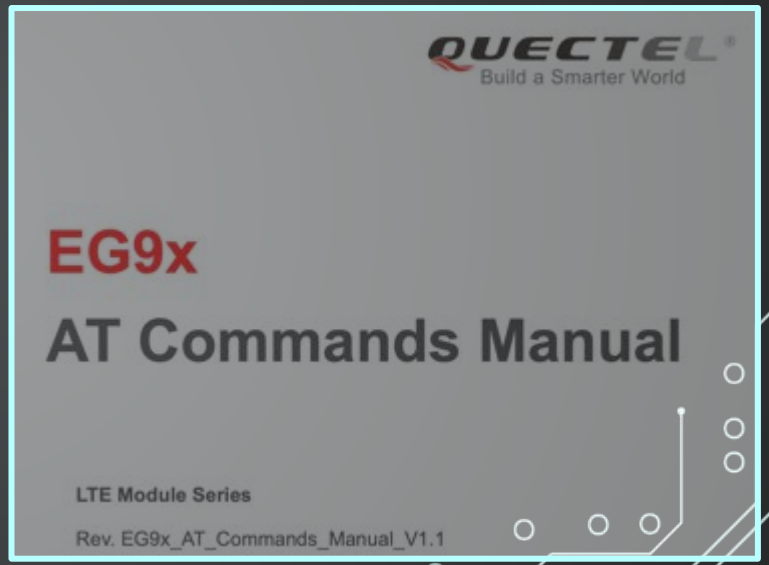
Controlling & Communicating Cellular Modules

Talking to a Cellular Module

AT Commands

AT = Attention

Allows communication with various RF controllers, including Cellular modules



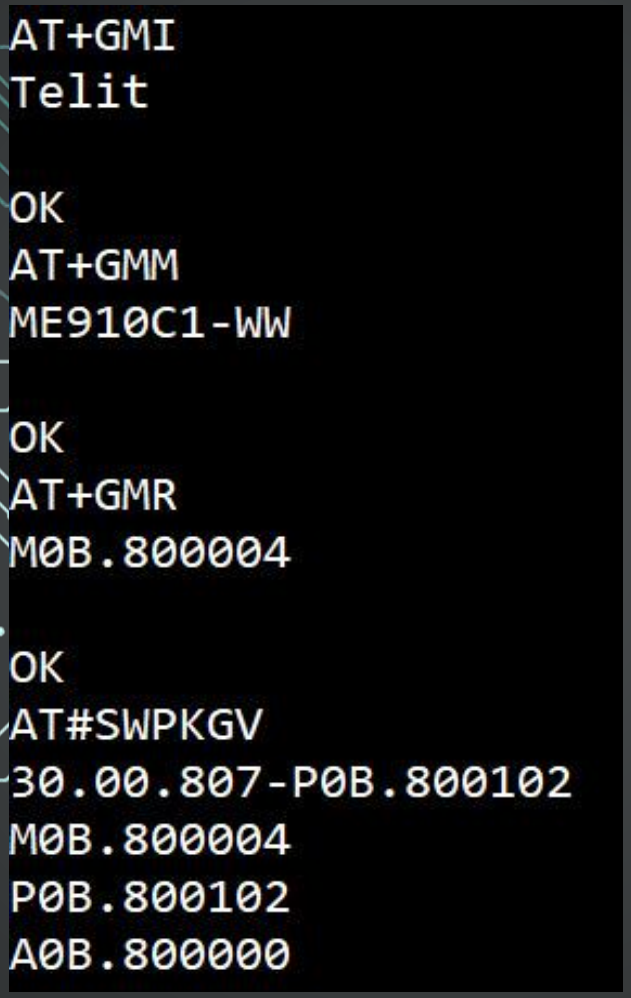
Types of AT Commands

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

Manufacturer Custom Commands

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





AT Commands for Enumeration

AT Commands for Sockets



AT#HTTPCFG=<prof_id>[,<server_address>[,<server_port>[,<auth_type>[,<username>[,<password>[,<ssl_enabled>[,<timeout>[,<cid>[,<pkt_size>[,<unused1>[,<unused2>]]]]]]]]]]]

```
#HTTPQRY: (0-2),(0-2),150,100

OK
AT#HTTPQRY?
ERROR
AT#HTTPCFG?
#HTTPCFG: 0,"www.google.com",80,0,"","******",0,120,1,
300,0,0
#HTTPCFG: 1,"",80,0,"","******",0,120,1,300,0,0
#HTTPCFG: 2,"m2mlocate.telit.com",9978,0,"","******",0
,120,1,300,0,0
```

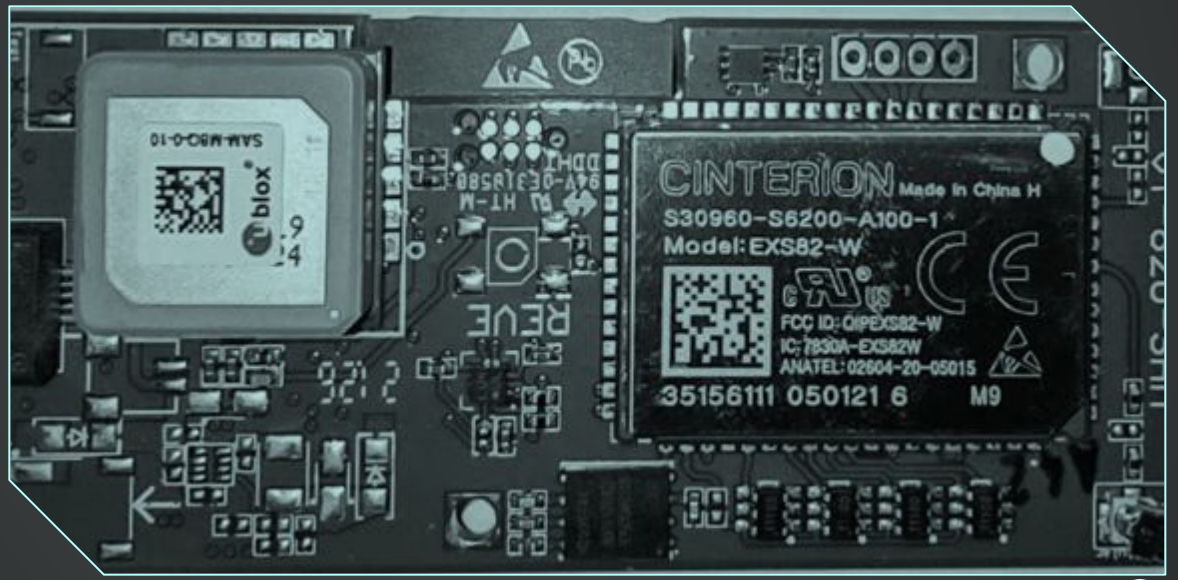
AT Command Scripts

```
[RMT-MBP-6330:CellMod ./ATquery.py QUECTEL TEST
 b'AT+CBC=?\r\r\n+CBC: (0-2),(0-100),(voltage)\r\n\r\nOK\r\n'
 b'AT+CCFC=?\r\r\n+CCFC: (0-5)\r\n\r\nOK\r\n'
 b'AT+CGDCONT=?\r\r\n+CGDCONT: (1-24,100-179),"IP",,,(0-2),(0-4),(0-1),(0-1)\r\n+CGDCONT:
 "IPV6",,,(0-2),(0-4),(0-1),(0-1)\r\n+CGDCONT: (1-24,100-179),"IPV4V6",,,(0-2),(0-4),(0-1)
 b'AT+CGEREP=?\r\r\n+CGEREP: (0-2),(0,1)\r\n\r\nOK\r\n'
 b'AT+CCLK=?\r\r\nOK\r\n'
 b'AT+CCWA=?\r\r\n+CCWA: (0,1)\r\n\r\nOK\r\n'
```

```
[RMT-MBP-6330:CellMod ./ATquery.py QUECTEL READ
 b'AT+CBC?\r\r\nERROR\r\n'
 b'AT+CCFC?\r\r\nERROR\r\n'
 b'AT+CGDCONT?\r\r\n+CGDCONT: 1,"IP","mcm.iot.us","0.0.0.0",0,0,0,0\r\n+CGDCONT: 2,"IPV4V6","ims"
 SOS","0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0",0,0,0,1\r\n\r\nOK\r\n'
 b'AT+CGEREP?\r\r\n+CGEREP: 0,0\r\n\r\nOK\r\n'
 b'AT+CCLK?\r\r\n+CCLK: "24/06/03,13:03:45+00"\r\n\r\nOK\r\n'
 b'AT+CCWA?\r\r\n+CCWA: 0\r\n\r\nOK\r\n'
 b'AT+CEDRXS?\r\r\nERROR\r\n'
 b'AT+CEREG?\r\r\n+CEREG: 0,5\r\n\r\nOK\r\n'
 b'AT+CFUN?\r\r\n+CFUN: 1\r\n\r\nOK\r\n'
```

Demo
AT Commands

Cellular Module Communications Types



Communication Types

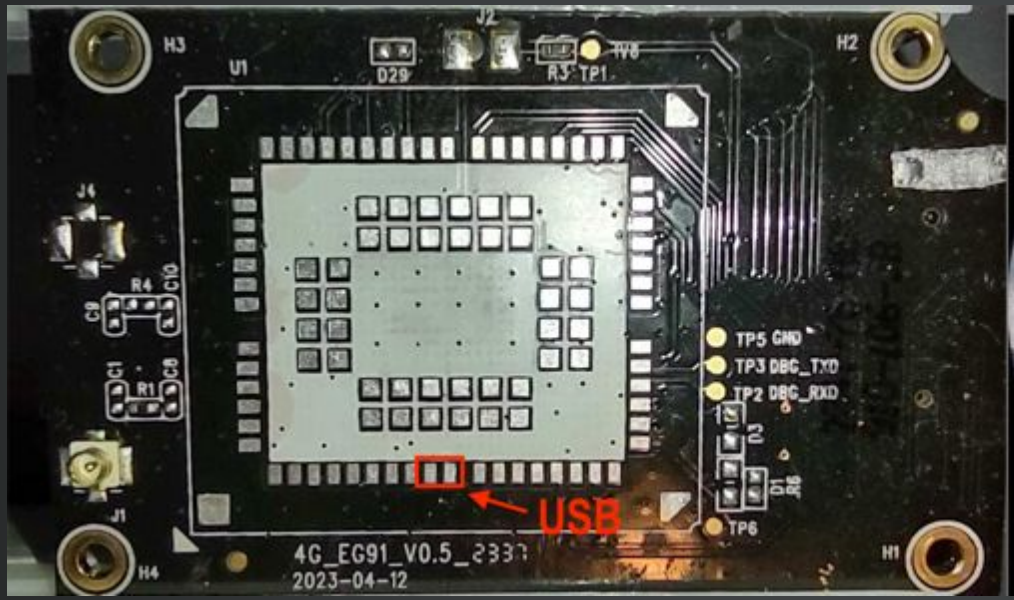
- USB
  - Inter-chip
    - HSIC (HS)
    - eUSB (HS)
    - Standard. (LS, FS, HS)
- UART
  - External (Debug UART)
  - Inter-chip (Main UART)

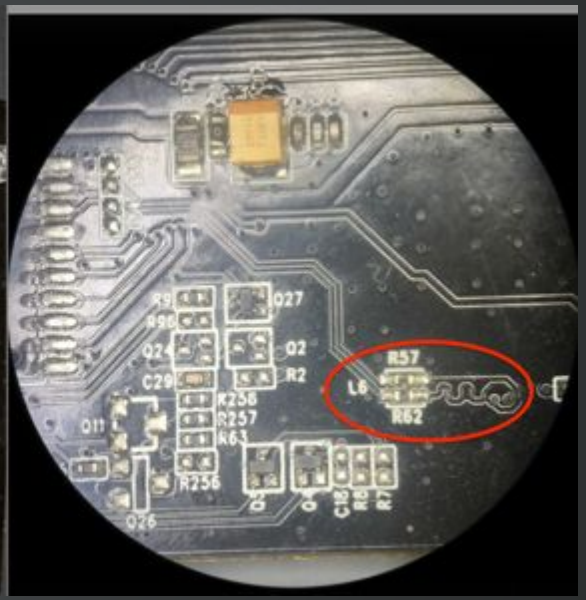
- **USB** 1.0/Low-**Speed**: 1.5 Mbps
- **USB** 1.1/Full-**Speed**: 12 Mbps
- **USB** 2.0/Hi-**Speed**: 480 Mbps
- **USB** 3.0/SuperSpeed: 5 Gbps
- **USB** 3.1/SuperSpeed: 10 Gbps

USB Capture & Decode

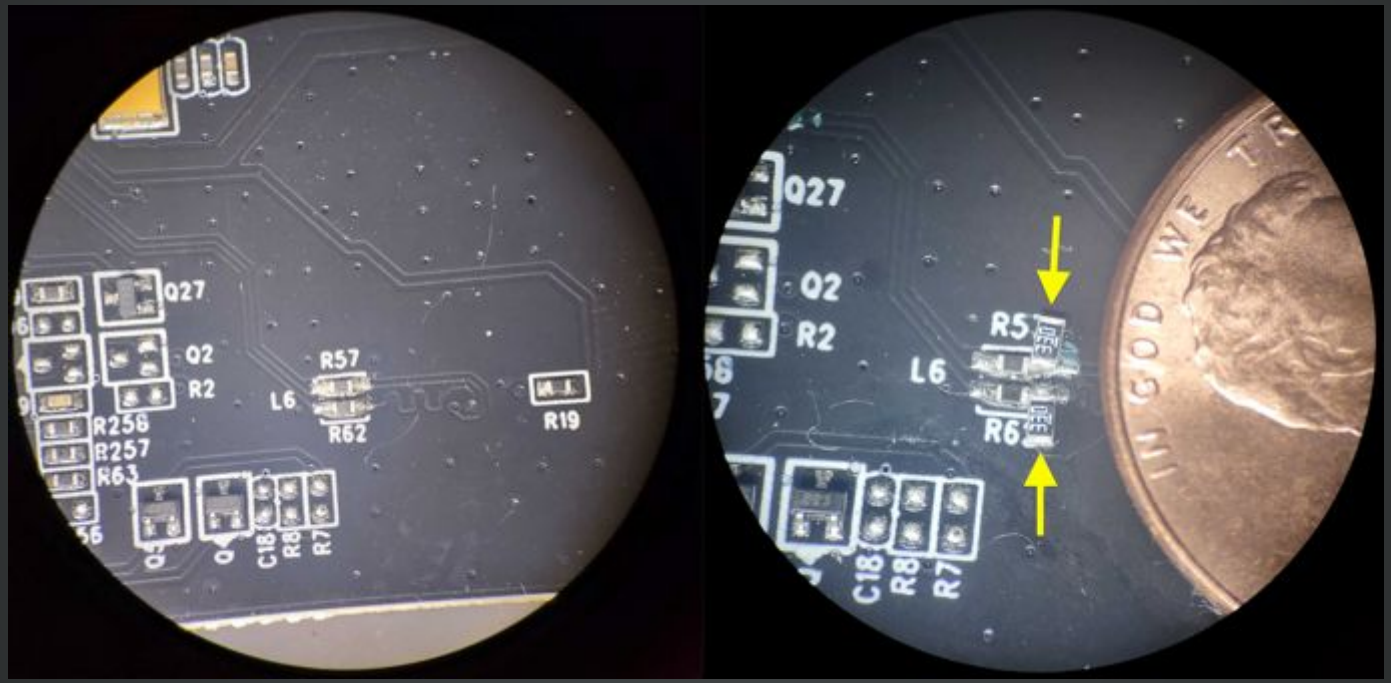


USB Inter-Chip Communication

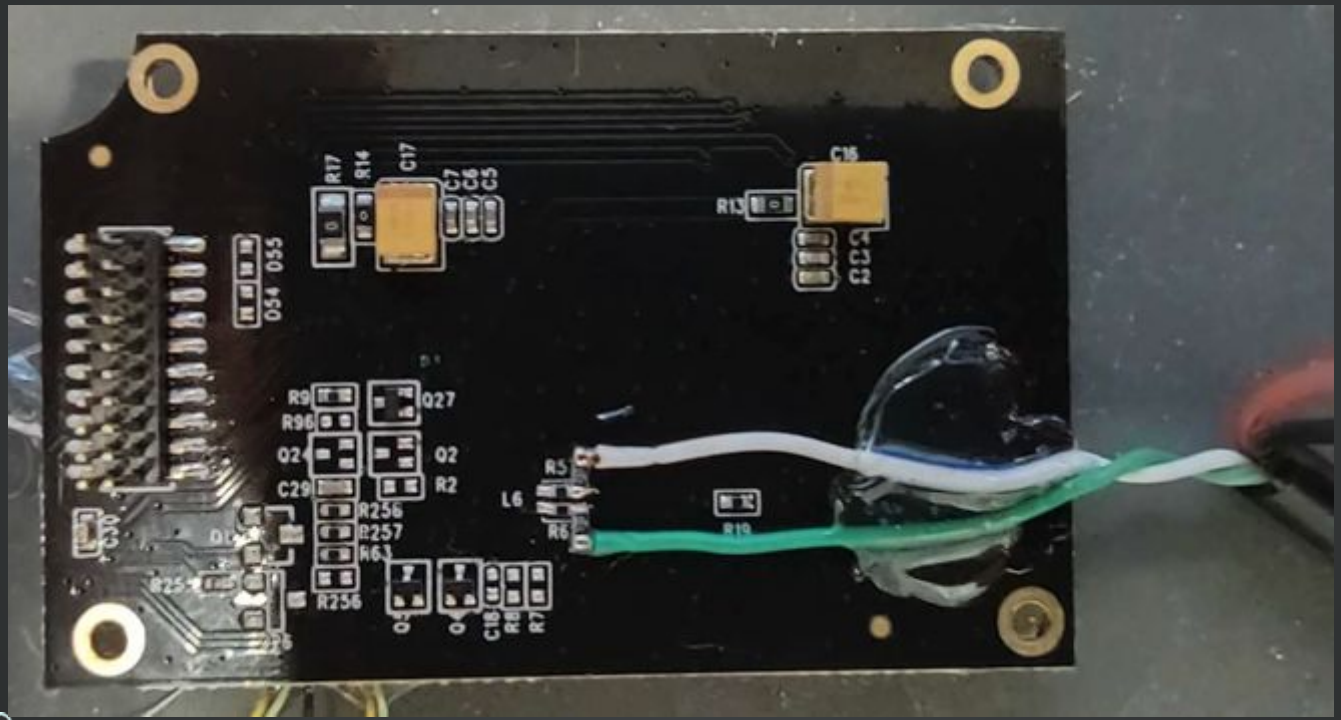




USB Inter-Chip Communication



USB Inter-Chip Communication



USB Inter-Chip Communication

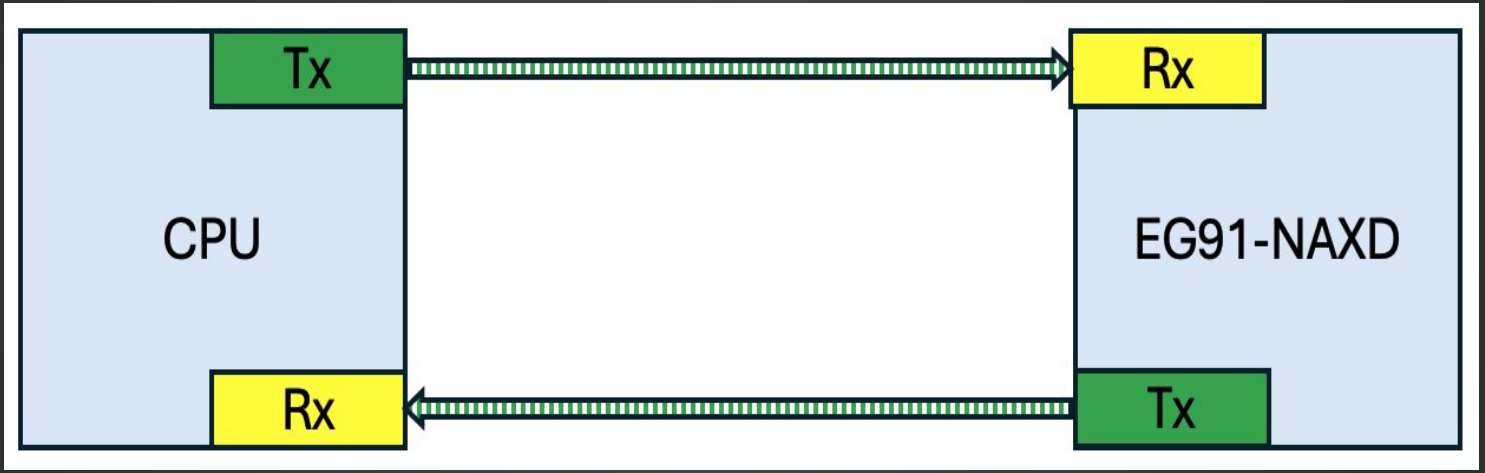


Demo
USB Capture

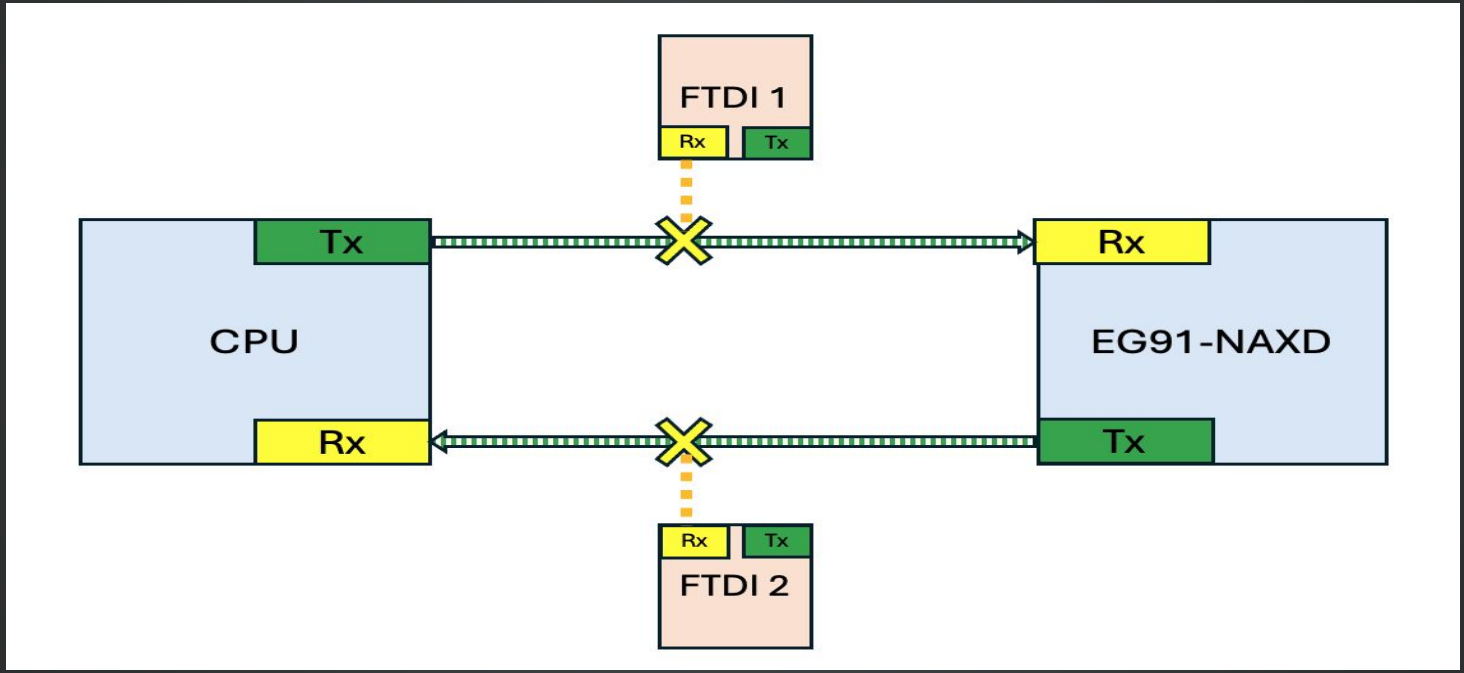
Serial Communication Capture & Interaction



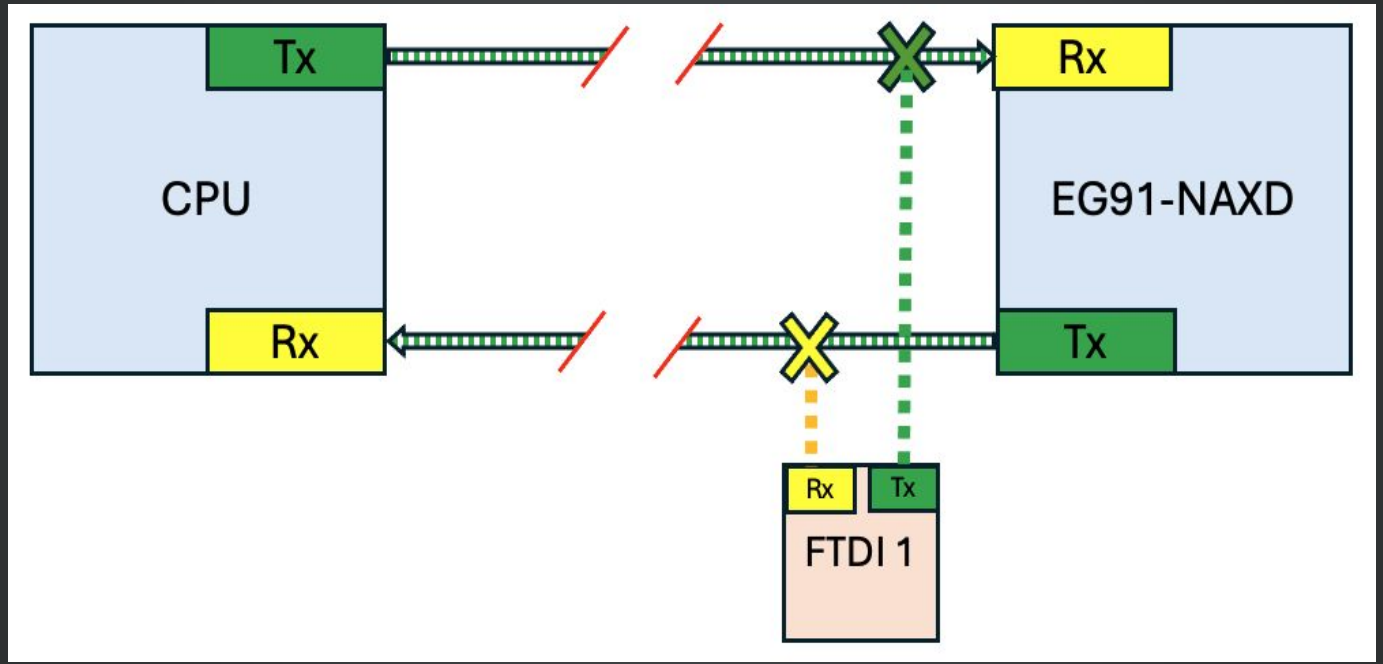
Inter-Chip Communication



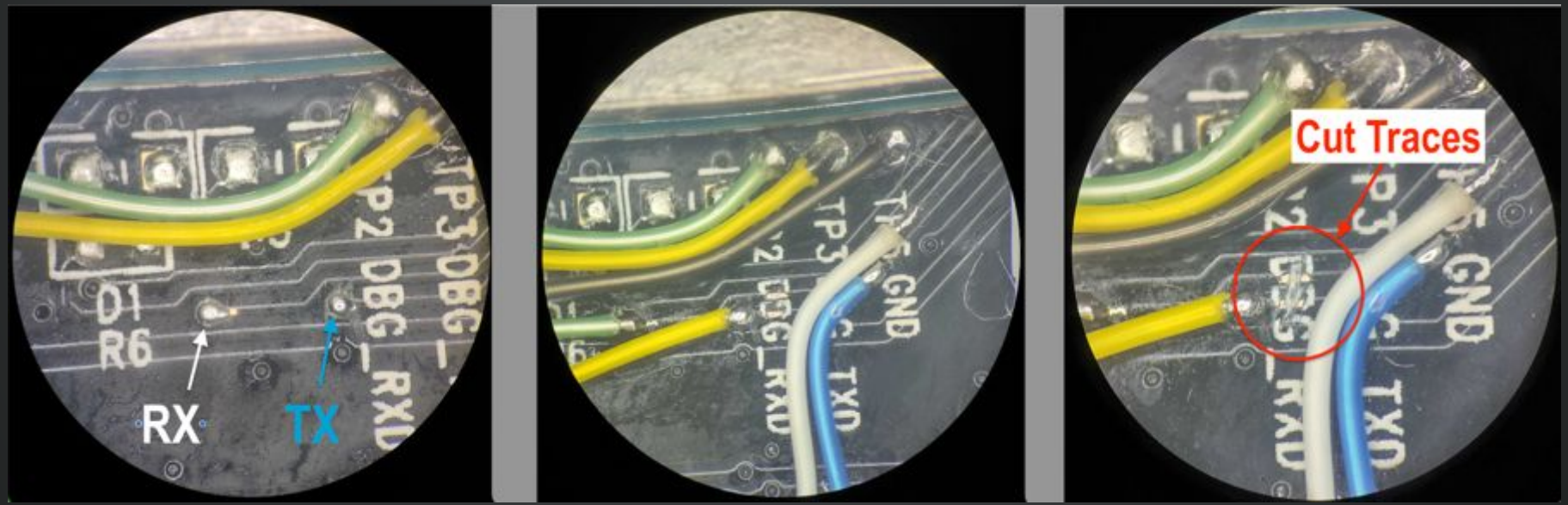
UART Inter-Chip Communication



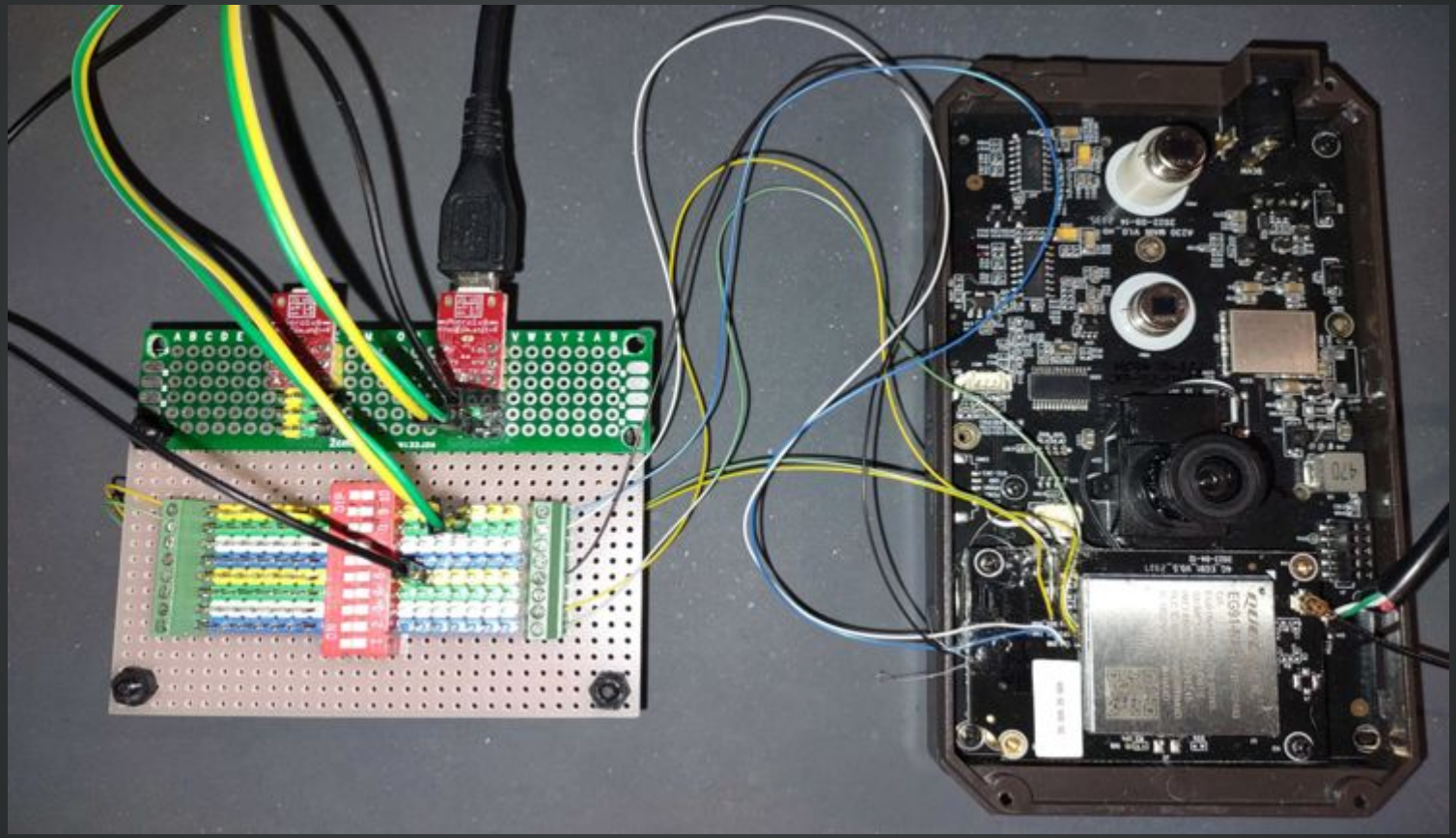
UART Inter-Chip Communication



UART Inter-Chip Communication



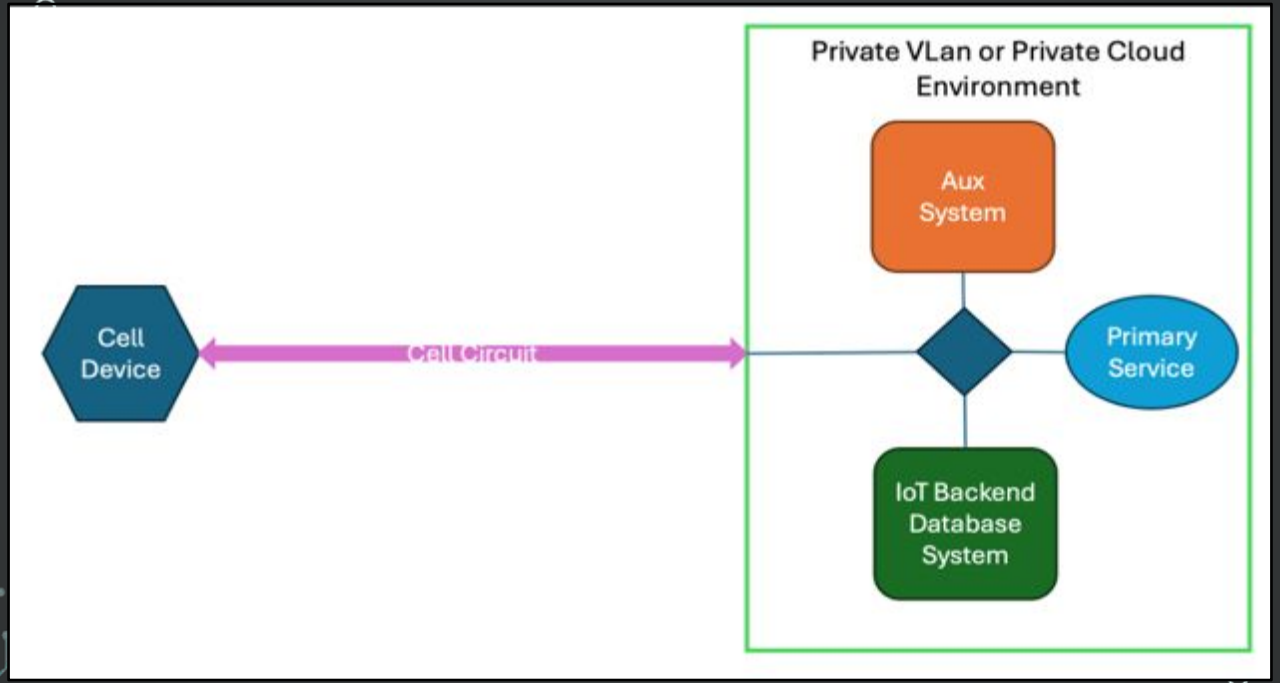
UART Inter-Chip Communication



AT Command



Injected Targeted Attacks


Private VLan or Private Cloud Environment
Aux System
Cell Device
Cell Circuit
Primary Service
IoT Backend Database System

Demo
AT Command
Port Scanning

Conclusion & Questions

Deral Heiland
Deral_heiland@rapid7.com
@percent_x

Carlota Bindner
@carlotabindner



Inter-Chip Communication:
https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-leveraging-inter-chip-communication-analysis.pdf
Dead Bugging BGA Memory Chips:
https://www.rapid7.com/blog/post/2022/04/07/lessons-in-iot-hacking-how-to-dead-bug-a-bga-flash-memory-chip/
General Blogs:
https://www.rapid7.com/blog/author/deral-heiland/