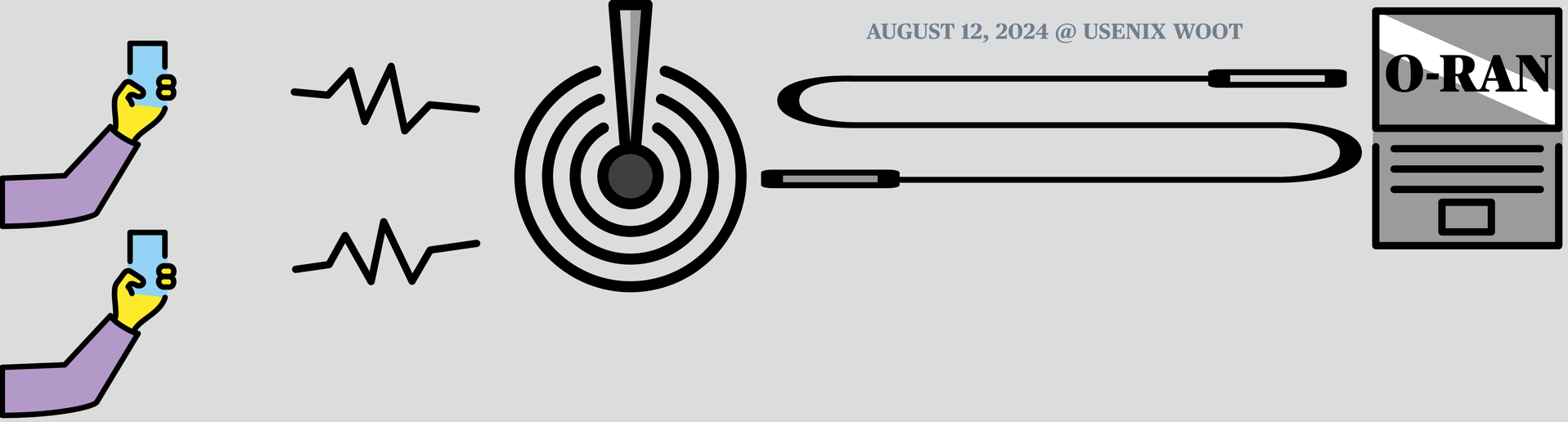


AUGUST 12, 2024 @ USENIX WOOT

Oh No My RAN! Breaking Into an O-RAN 5G Indoor Base Station

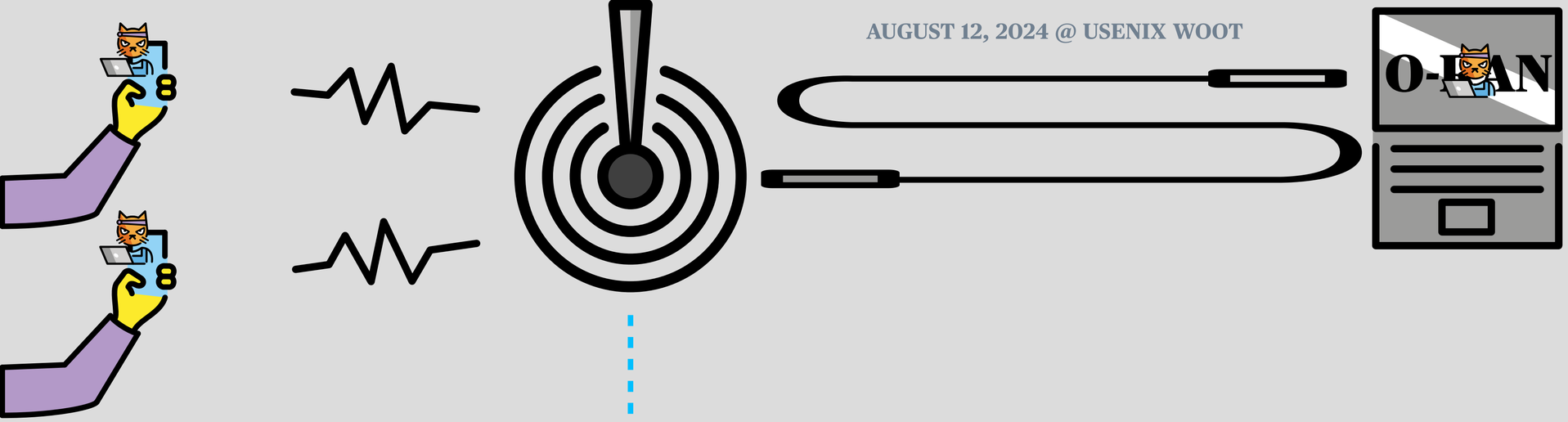
Leon Janzen, Lucas Becker, Colin Wiesenäcker, Matthias Hollick
{ljanzen,lbecker,cwiesenaecker,mhollick}@seemoo.de

SECURE MOBILE NETWORKING

Open6GHub

CRUST

TECHNISCHE UNIVERSITÄT DARMSTADT



AUGUST 12, 2024 @ USENIX WOOT

Oh No My RAN! Breaking Into an O-RAN 5G Indoor Base Station

Leon Janzen, Lucas Becker, Colin Wiesenäcker, Matthias Hollick
{ljanzen,lbecker,cwiesenaecker,mhollick}@seemoo.de

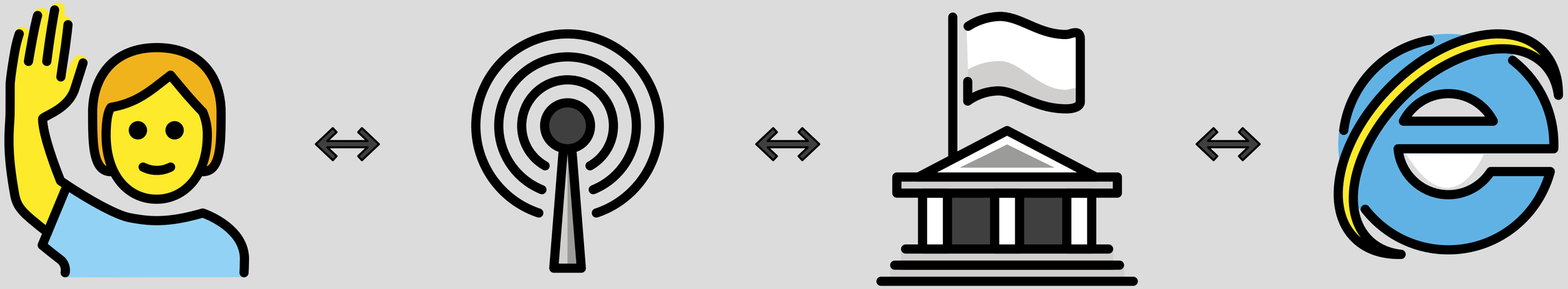
SECURE MOBILE NETWORKING

Open6GHub

CRUST

TECHNISCHE UNIVERSITÄT DARMSTADT

What are O-RAN 5G Indoor Base Stations?



user

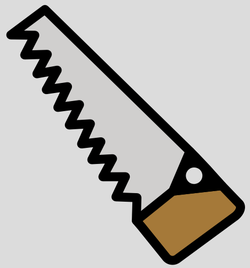
radio access network

core network

the Internet

What are O-RAN 5G Indoor Base Stations?

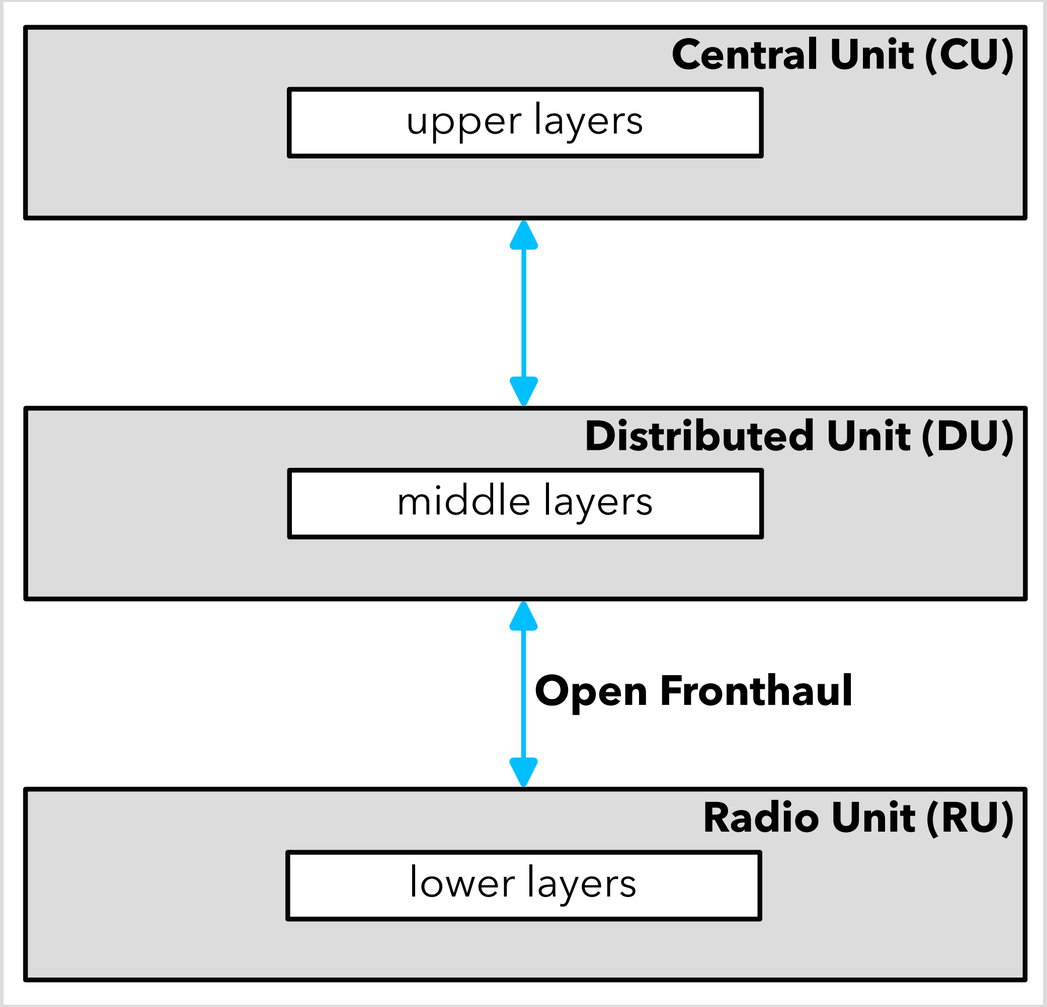
Open Radio Access Networks (O-RANs)



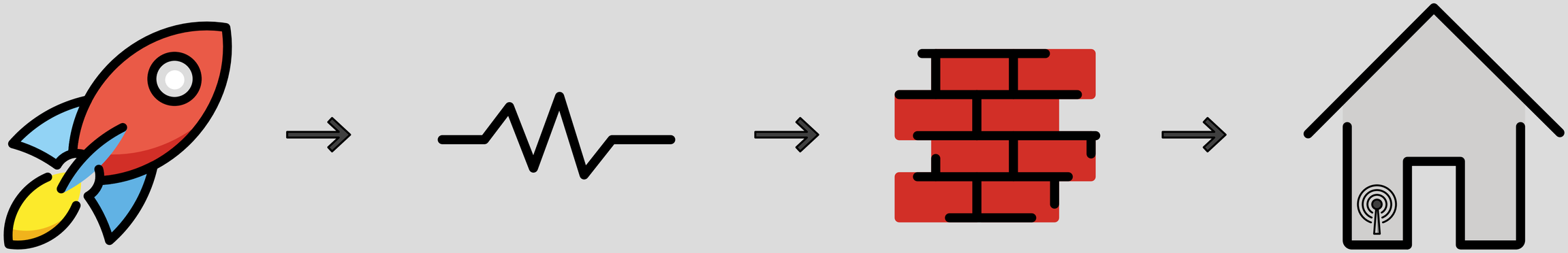
gNB = RU+DU+CU

only RU at cell-site

open interfaces,
no open source



What are O-RAN 5G Indoor Base Stations?



faster speeds

higher frequencies
(mmWave)

less penetration

indoor BSs
=
indoor RUs

16.05.24

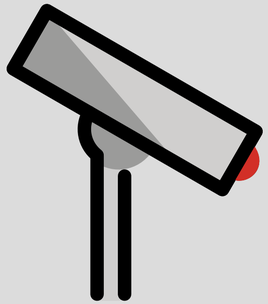
NEWS

1&1 completes roll-out of 5G technology at SIGNAL IDUNA PARK

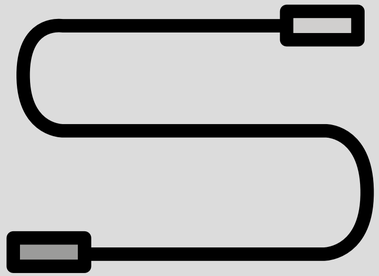
Borussia Dortmund's main sponsor 1&1 have successfully completed the roll-out of 5G technology at SIGNAL IDUNA PARK for the last Bundesliga match of the current season. 1&1 operates the first mobile network in Europe based on Open RAN technology and is now delivering high download and upload speeds for visitors just in time for the EURO tournament.

https://www.bvb.de/content/bvbweb/bvb_de/de/en/news/news-overview/news.html/content/dam/bvbweb/en/news/commercial-partnerships/2024/05/16/-2-0-7-1-5-2-/-2-0-7-1-5-2-.html

System Model

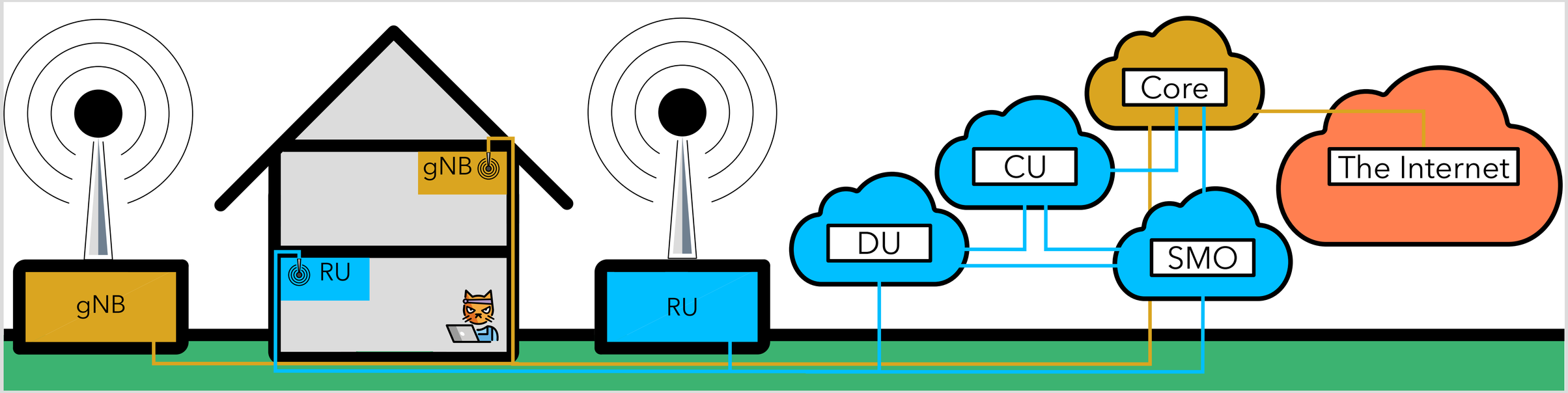


physical access control
hard for indoor BSs



RU highly connected
within O-RAN

high vendor diversity
for O-RAN RUs



SMO = Service Management & Orchestration Platform

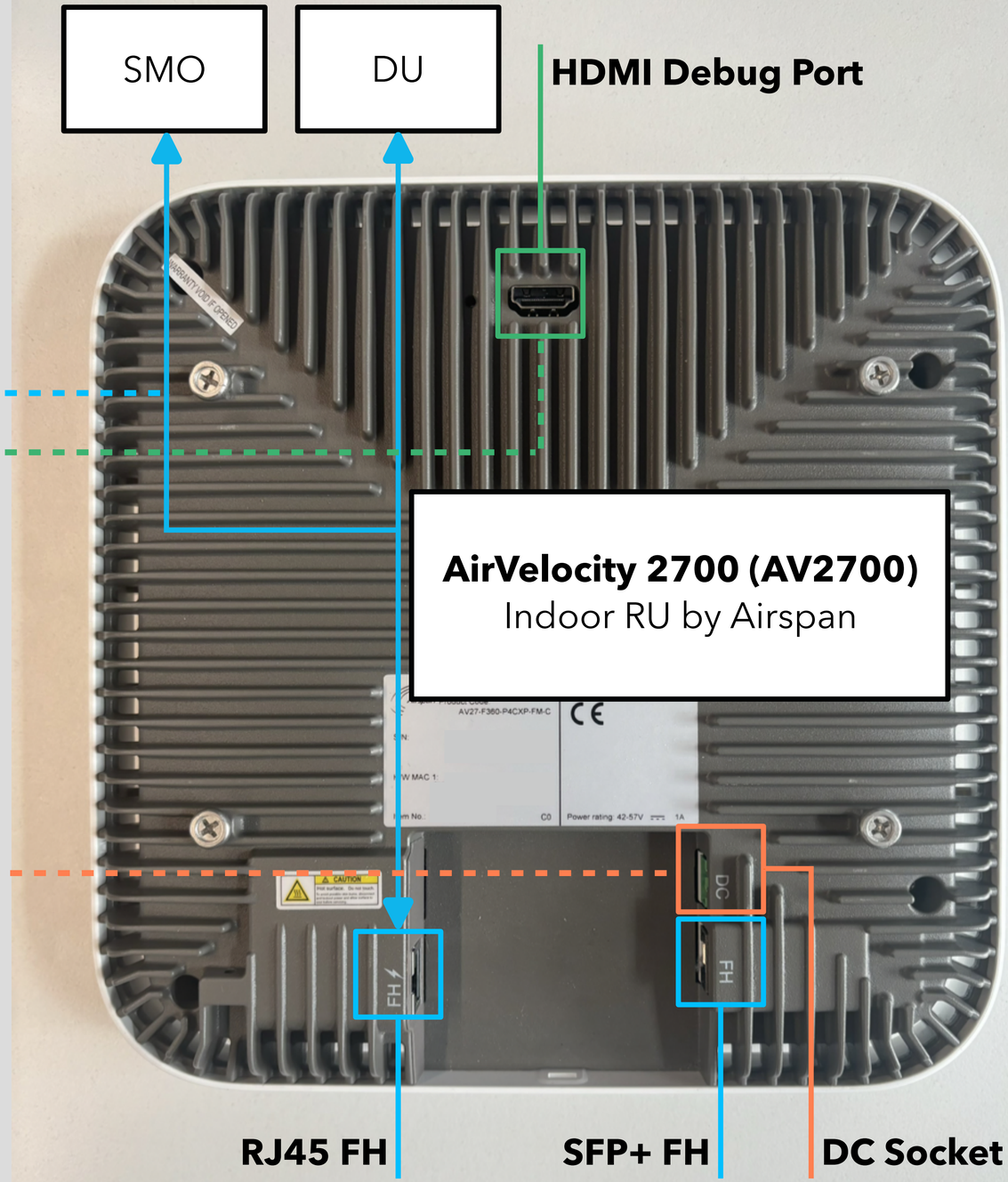
Threat Model

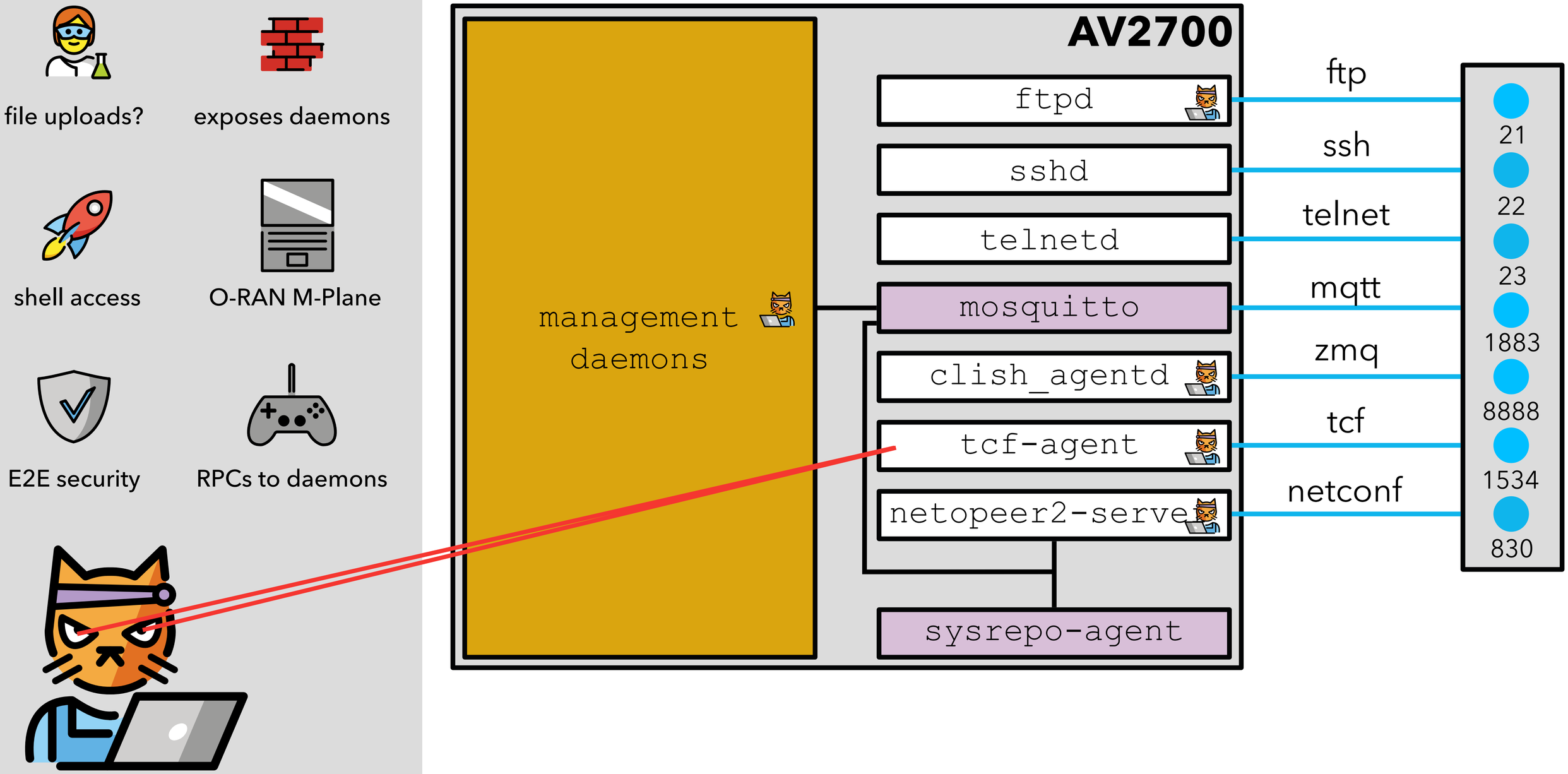
Has Ethernet access to the RU (C1)

Has full interface access to the RU (C2)

Can steal the RU (C3)

Can redeploy the RU (C4)



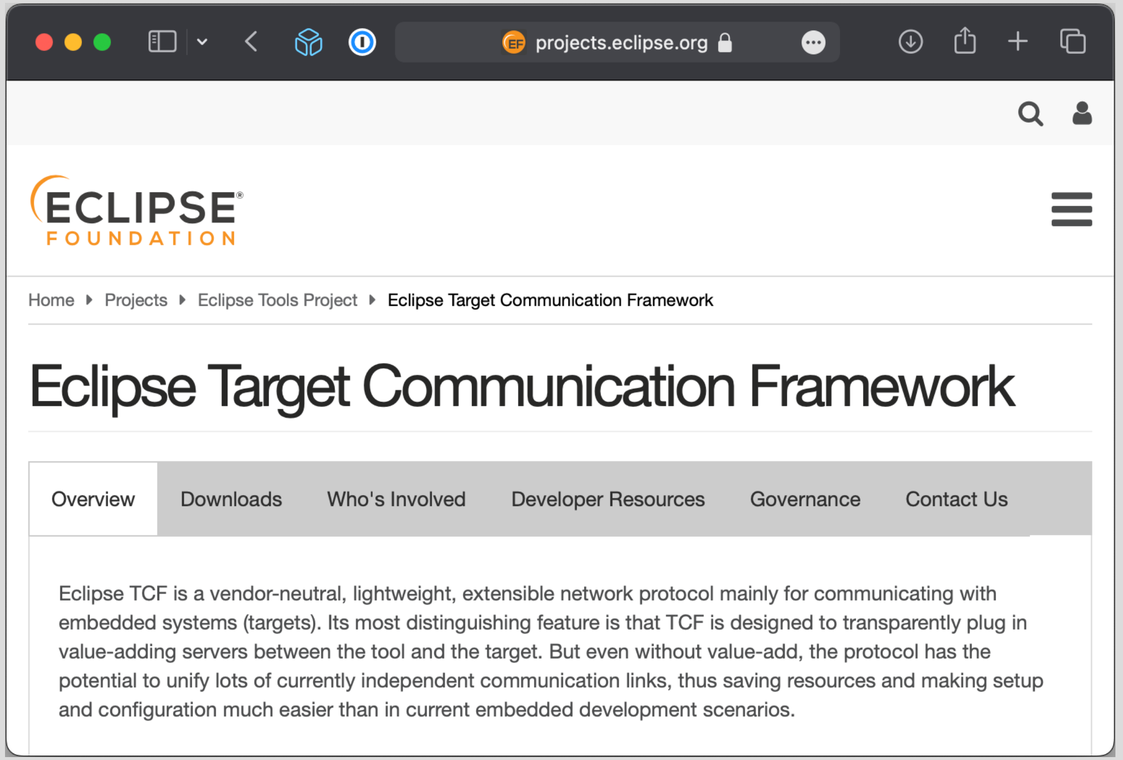

file uploads?
exposes daemons
shell access
O-RAN M-Plane
E2E security
RPCs to daemons
AV2700
management daemons
ftpd
sshd
telnetd
mosquitto
clish_agentd
tcf-agent
netopeer2-server
sysrepo-agent
ftp
ssh
telnet
mqtt
zmq
tcf
netconf
21
22
23
1883
8888
1534
830

Finding 1: Exposed TCF Agent

Target Communication Framework (TCF)

communicate to built-in FPGAs

broadcasts on UDP port 1534



https://projects.eclipse.org/projects/tools.tcf

Finding

Targ

communica
built-in FP

Wireshark · Packet 9 · 2023-03-29-tcf-eclipse-launch-terminal.pcapng

```
> Frame 9: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface en15, id 0
> Ethernet II, Src: Airspan_00:05:88 (00:a0:0a:00:05:88), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.137, Dst: 192.168.1.255
> User Datagram Protocol, Src Port: 1534, Dst Port: 1534
v Data (246 bytes)
    Data: 5443463202000000049443d5443503a3139322e3136382e312e3133373a31353334004e61…
```

```
0000  ff ff ff ff ff ff 00 a0  0a 00 05 88 08 00 45 00   ........ ......E·
0010  01 12 42 36 40 00 40 11  72 cc c0 a8 01 89 c0 a8   ··B6@·@· r·......
0020  01 ff 05 fe 05 fe 00 fe  79 2f 54 43 46 32 02 00   ........ y/TCF2··
0030  00 00 49 44 3d 54 43 50  3a 31 39 32 2e 31 36 38   ··ID=TCP :192.168
0040  2e 31 2e 31 33 37 3a 31  35 33 34 00 4e 61 6d 65   .1.137:1 534·Name
0050  3d 54 43 46 20 41 67 65  6e 74 00 4f 53 4e 61 6d   =TCF Age nt·OSNam
0060  65 3d 4c 69 6e 75 78 20  34 2e 31 39 2e 30 2d 78   e=Linux  4.19.0-x
0070  69 6c 69 6e 78 2d 76 32  30 31 39 2e 31 00 55 73   ilinx-v2 019.1·Us
0080  65 72 4e 61 6d 65 3d 72  6f 6f 74 00 41 67 65 6e   erName=r oot·Agen
0090  74 49 44 3d 34 39 38 62  39 65 30 33 2d 33 30 39   tID=498b 9e03-309
00a0  34 2d 34 33 61 38 2d 39  35 66 33 2d 64 31 62 63   4-43a8-9 5f3-d1bc
00b0  66 64 32 62 34 31 64 66  00 54 72 61 6e 73 70 6f   fd2b41df ·Transpo
00c0  72 74 4e 61 6d 65 3d 54  43 50 00 53 65 72 76 69   rtName=T CP·Servi
00d0  63 65 4d 61 6e 61 67 65  72 49 44 3d 34 39 38 62   ceManage rID=498b
00e0  39 65 30 33 2d 33 30 39  34 2d 34 33 61 38 2d 39   9e03-309 4-43a8-9
00f0  35 66 33 2d 64 31 62 63  66 64 32 62 34 31 64 66   5f3-d1bc fd2b41df
0100  2d 30 00 50 6f 72 74 3d  31 35 33 34 00 48 6f 73   -0·Port= 1534·Hos
0110  74 3d 31 39 32 2e 31 36  38 2e 31 2e 31 33 37 00   t=192.16 8.1.137·
```

OS = Linux Xilinx

user name = root ?!

port = 1534

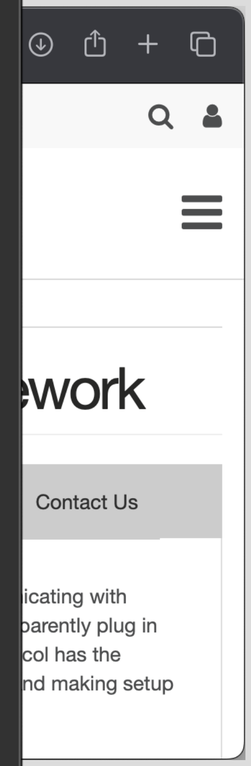
host = 192.168.1.137

Bytes 42-287: Data (data.data)

Show packet bytes

Help

Close



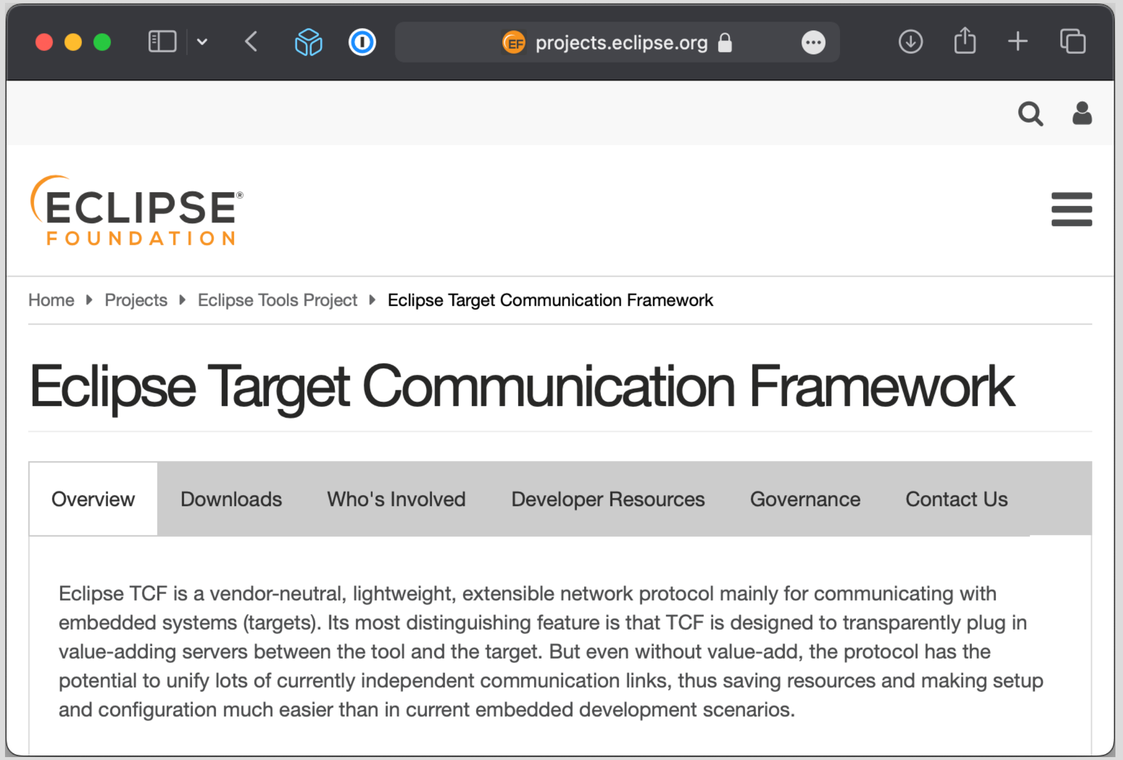
Finding 1: Exposed TCF Agent

Target Communication Framework (TCF)

communicate to built-in FPGAs

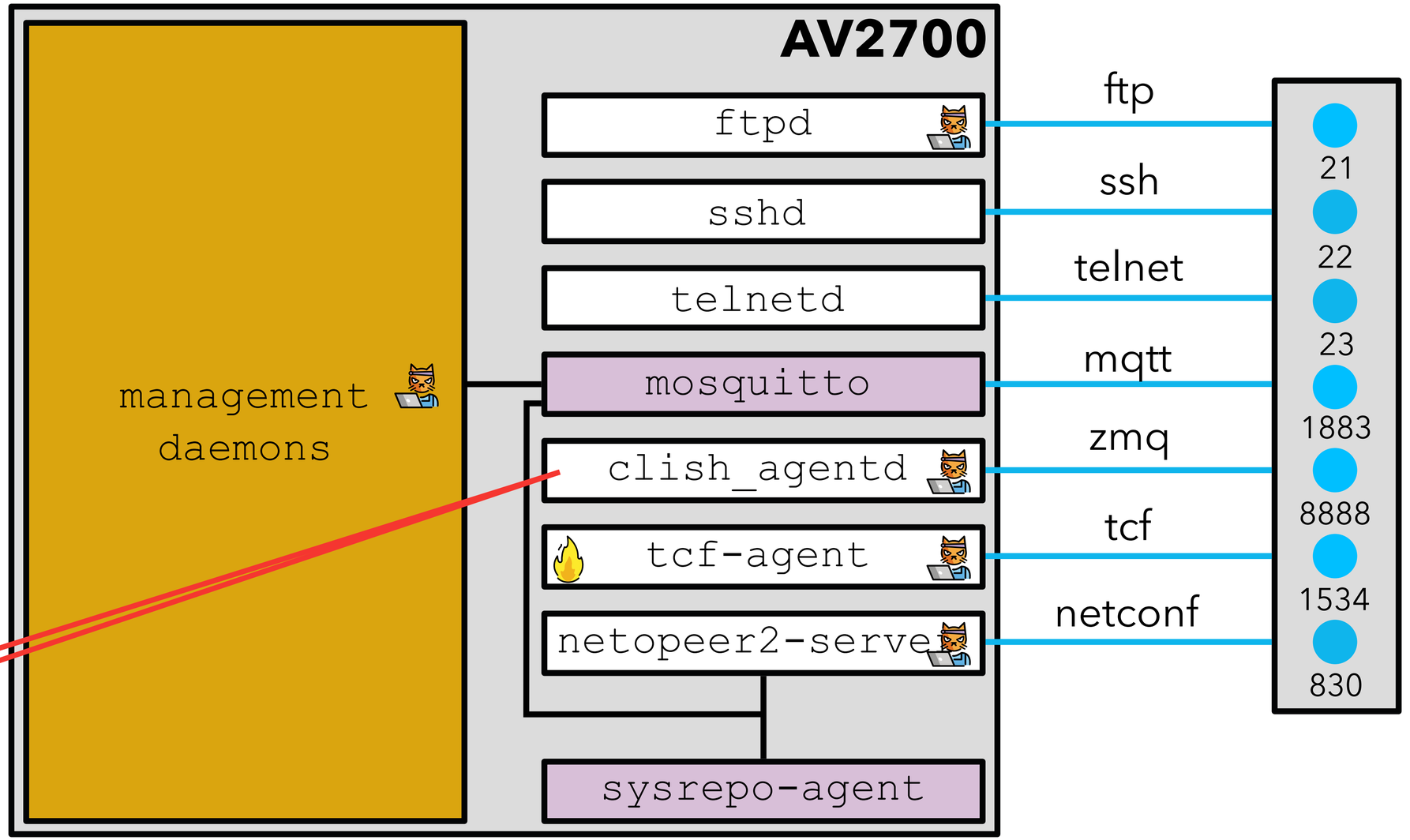
broadcasts on UDP port 1534

exposes a root terminal

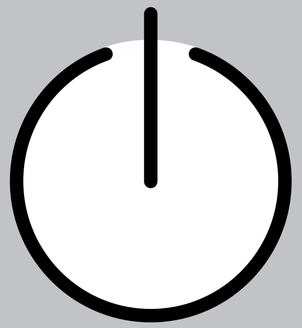


https://projects.eclipse.org/projects/tools.tcf

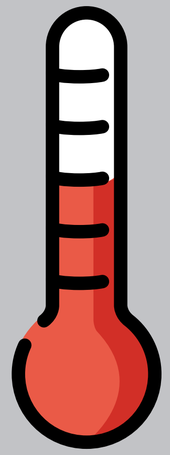
F1 -> Root Shell Access



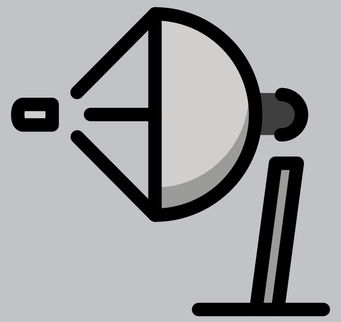
Finding 2: Missing Access Control



restart RU



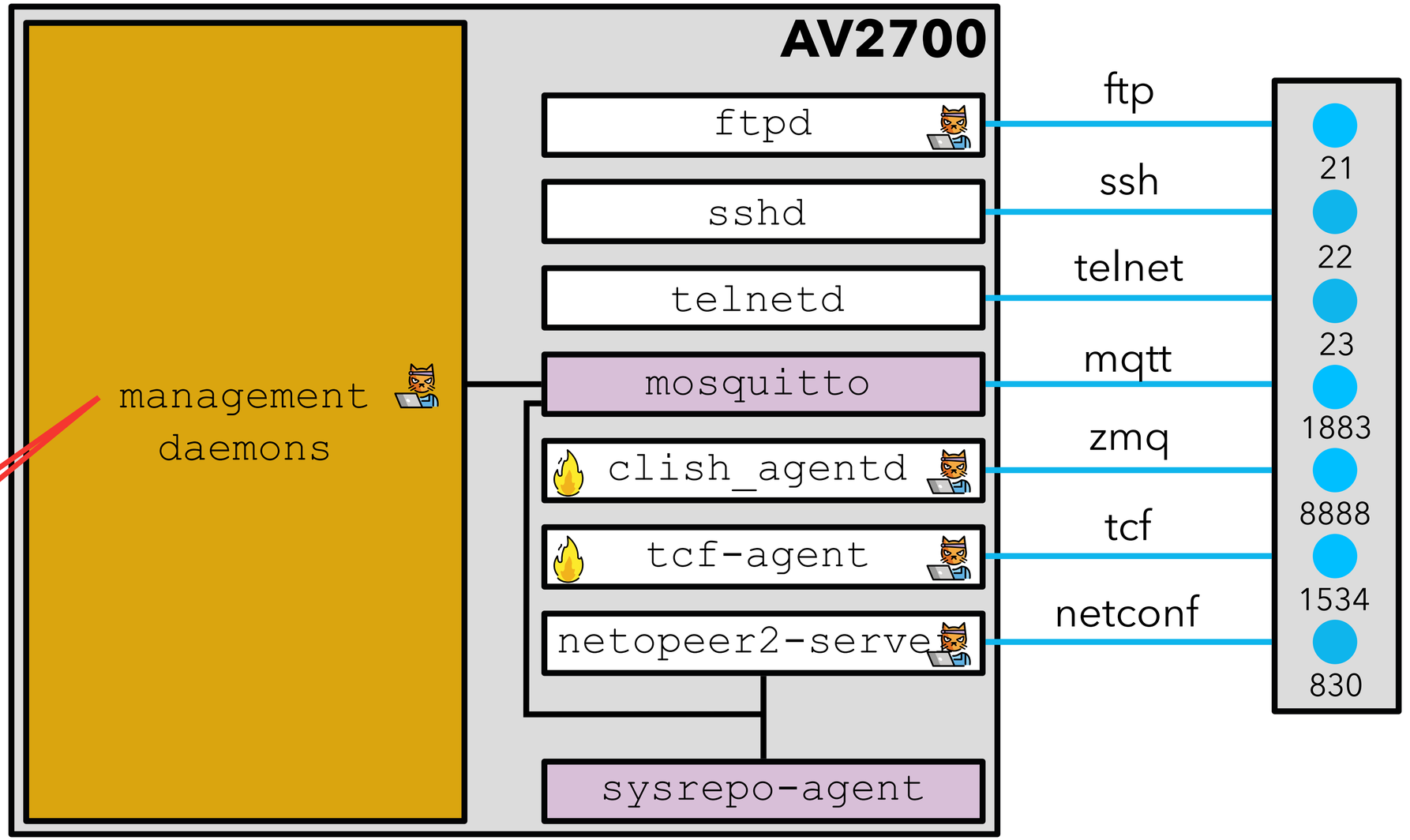
set alarm temperature



modify sending power

F1 -> Root Shell Access

F2 -> RU Reconfiguration



Finding 3: Memory Corruption Vulnerabilities

fortified function -> DoS

unfortified function -> RCE?

```
void* buffer = calloc(1, 0x102c);
void* build_id = cJSON_GetObjectItem(json_obj,
  "build_id");

if (build_id != 0)
{
  __strcpy_chk(buffer, *(build_id + 32), 64);

  […]

  void* buffer_ptr = buffer + 0x188;
  void* filename_field =
    cJSON_GetObjectItem(json_obj, "file-name");
  if (filename != 0)
  {
    strcpy(buffer_ptr - 0x84,
      *(file_name_field+32));
  }
}
```

Finding 4: Command Injection Vulnerabilities

adversary-controlled string input

heap buffer with 5 usable bytes -> full RCE

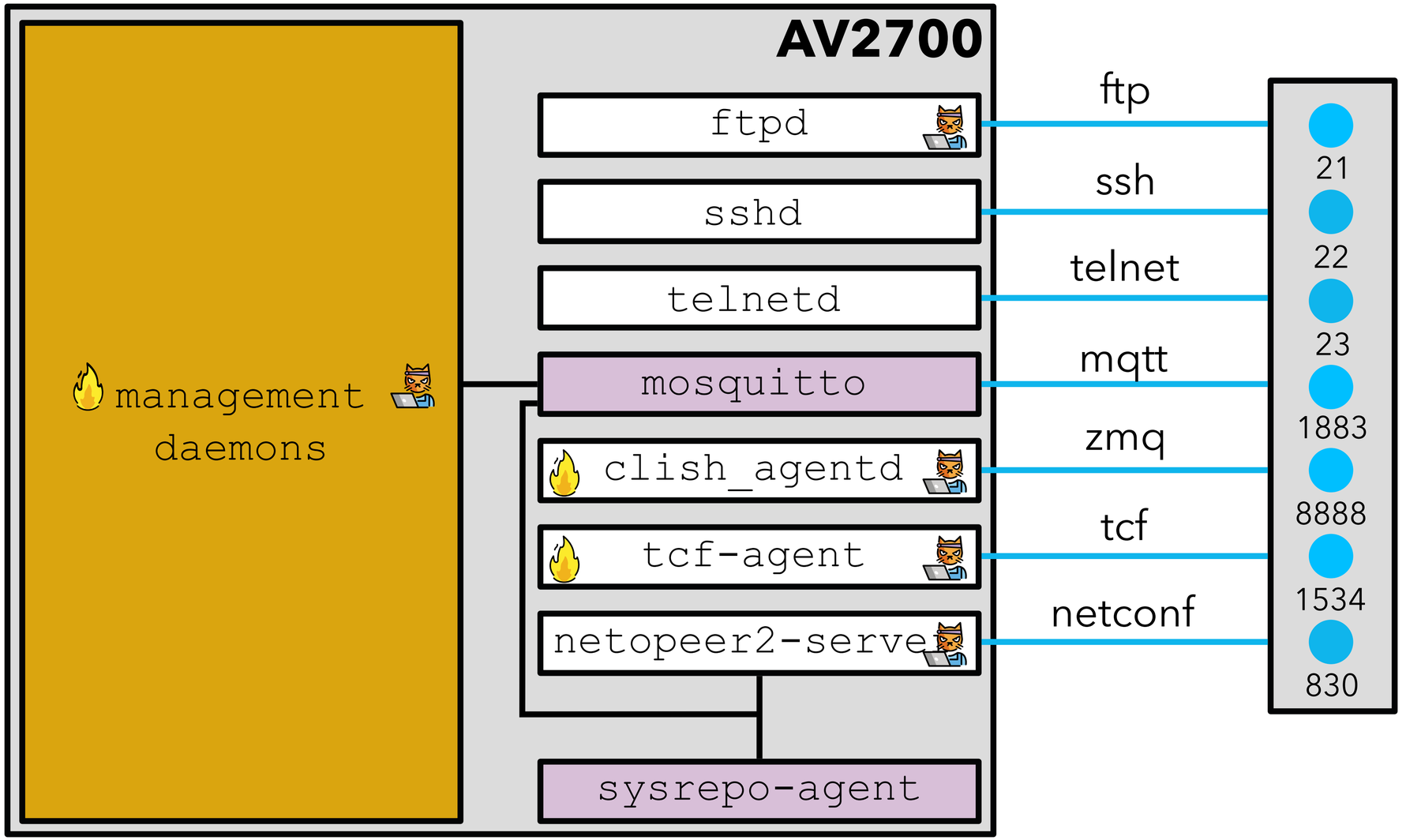
```
void create_interfaces(char *inf, int vlan_id)
{
  char if_name[10];
  char cmd_buff[100];

  __sprintf_chk(if_name, 1, 10, "%s.%d",
    inf, vlan_id);

  if(!check_if_inf_exists(if_name))
  {
    __sprintf_chk(cmd_buff, 1, 100,
      "vconfig add %s %d", inf, vlan_id);

    system(cmd_buff);
  }
}
```

F1 -> Root Shell Access

F2 -> RU Reconfiguration

F3 -> DoS … & RCE?

F4 -> RCE



Impact on the Cellular Network

impact on the radio unit

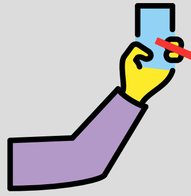
reconfiguration

DoS

full control

potential follow-up attacks

users via UEs



SMO

DU

HDMI Debug Port

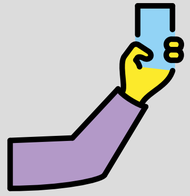
AirVelocity 2700 (AV2700)
Indoor RU by Airspan

RJ45 FH

SFP+ FH

DC Socket

Impact on the Cellular Network



impact on the radio unit

reconfiguration

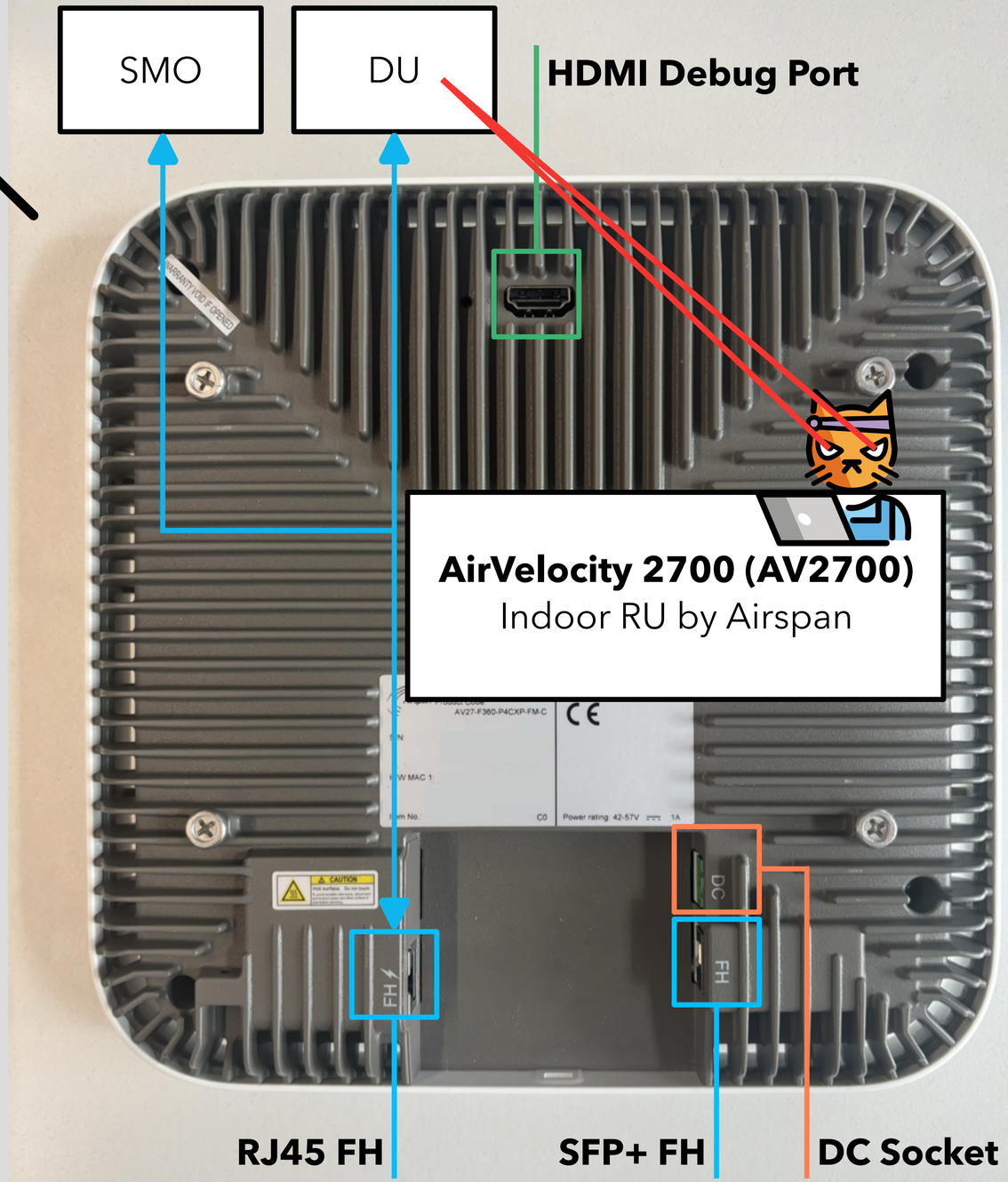
DoS

full control

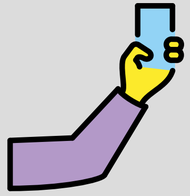
potential follow-up attacks

users via UEs

O-RAN DU



Impact on the Cellular Network



impact on the radio unit

reconfiguration

DoS

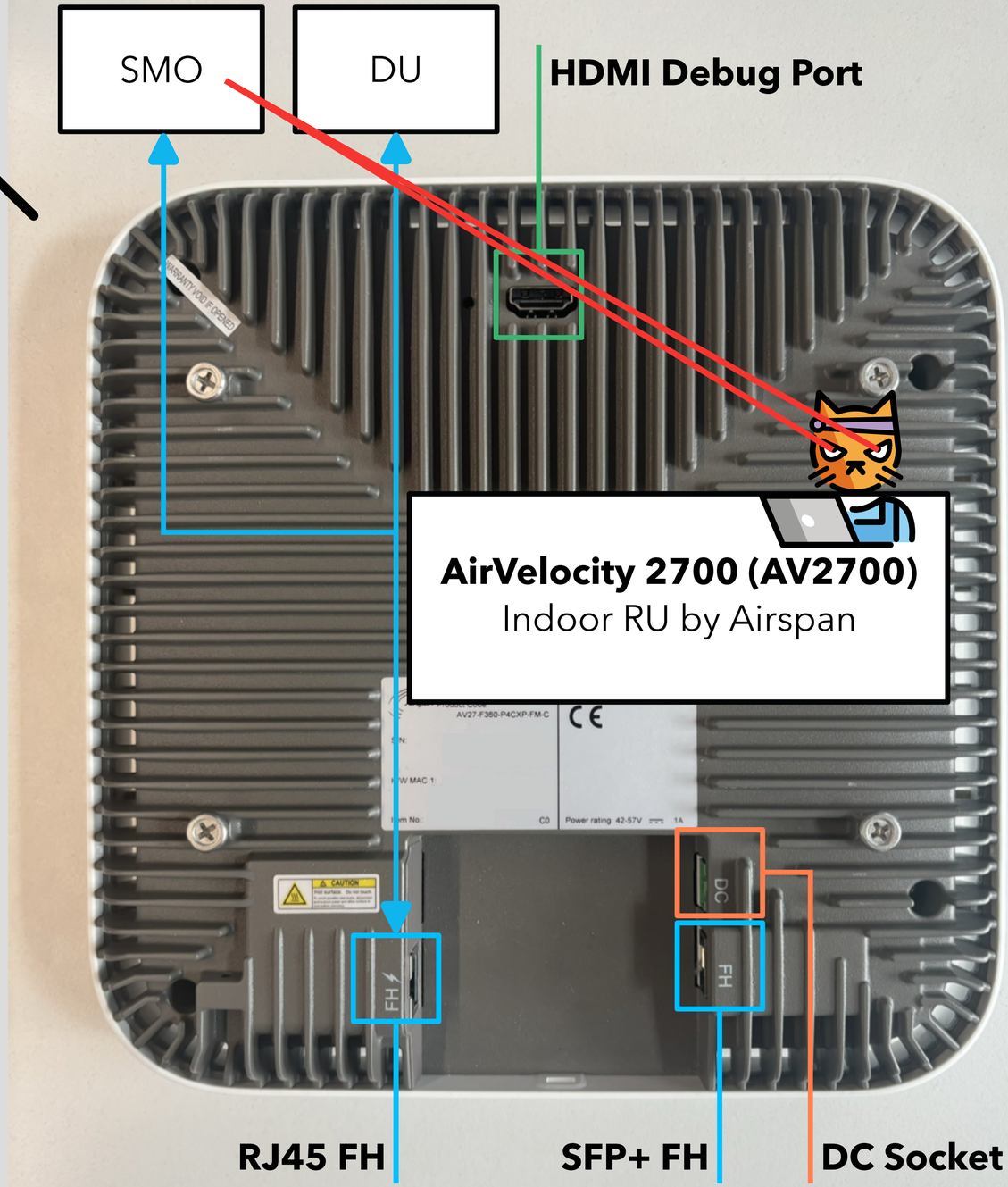
full control

potential follow-up attacks

users via UEs

O-RAN DU

O-RAN SMO



Oh No My RAN! Breaking Into an O-RAN 5G Indoor Base Station

Leon Janzen, Lucas Becker, Colin Wiesenäcker, Matthias Hollick
{ljanzen,lbecker,cwiesenaecker,mhollick}@seemoo.de