

Forensik in der Gebäudeautomation

Ziel des Beitrags

- Awareness schaffen durch Beispiele
- Kleine Einführung in Forensik

Drei Probleme

1. Alle Geräte gehen irgendwann einmal kaputt und werden entsorgt - nicht immer werden vertrauliche Informationen dabei sorgfältig entfernt
2. Hersteller von Geräten werden Opfer von "Spionen" und verlieren im Wettbewerb
3. Geräte funktionieren nicht und Hersteller kooperiert nicht

Dumpster Diving

- Nicht jede Art von Recycling ist wünschenswert

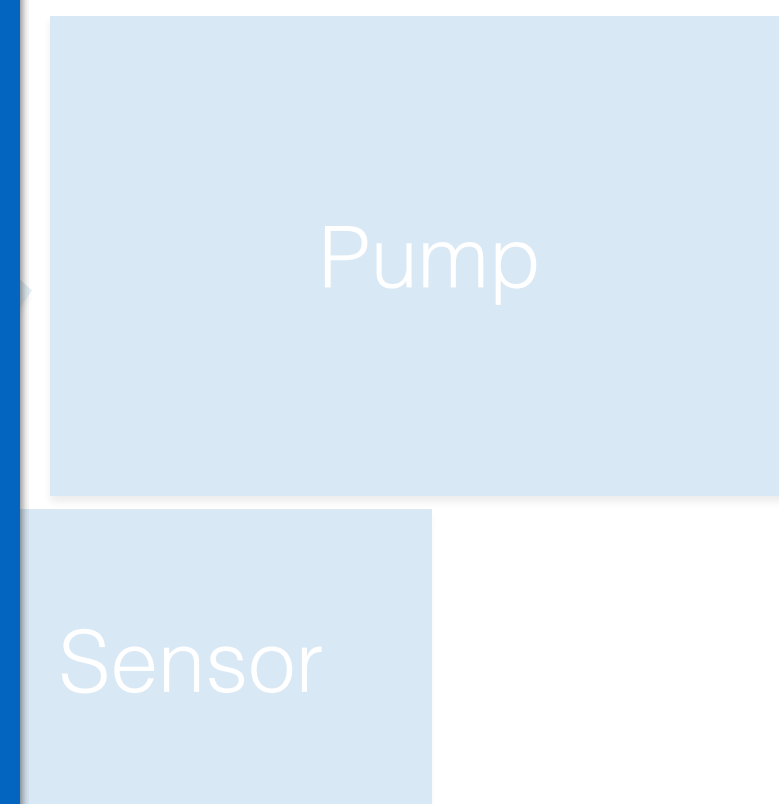
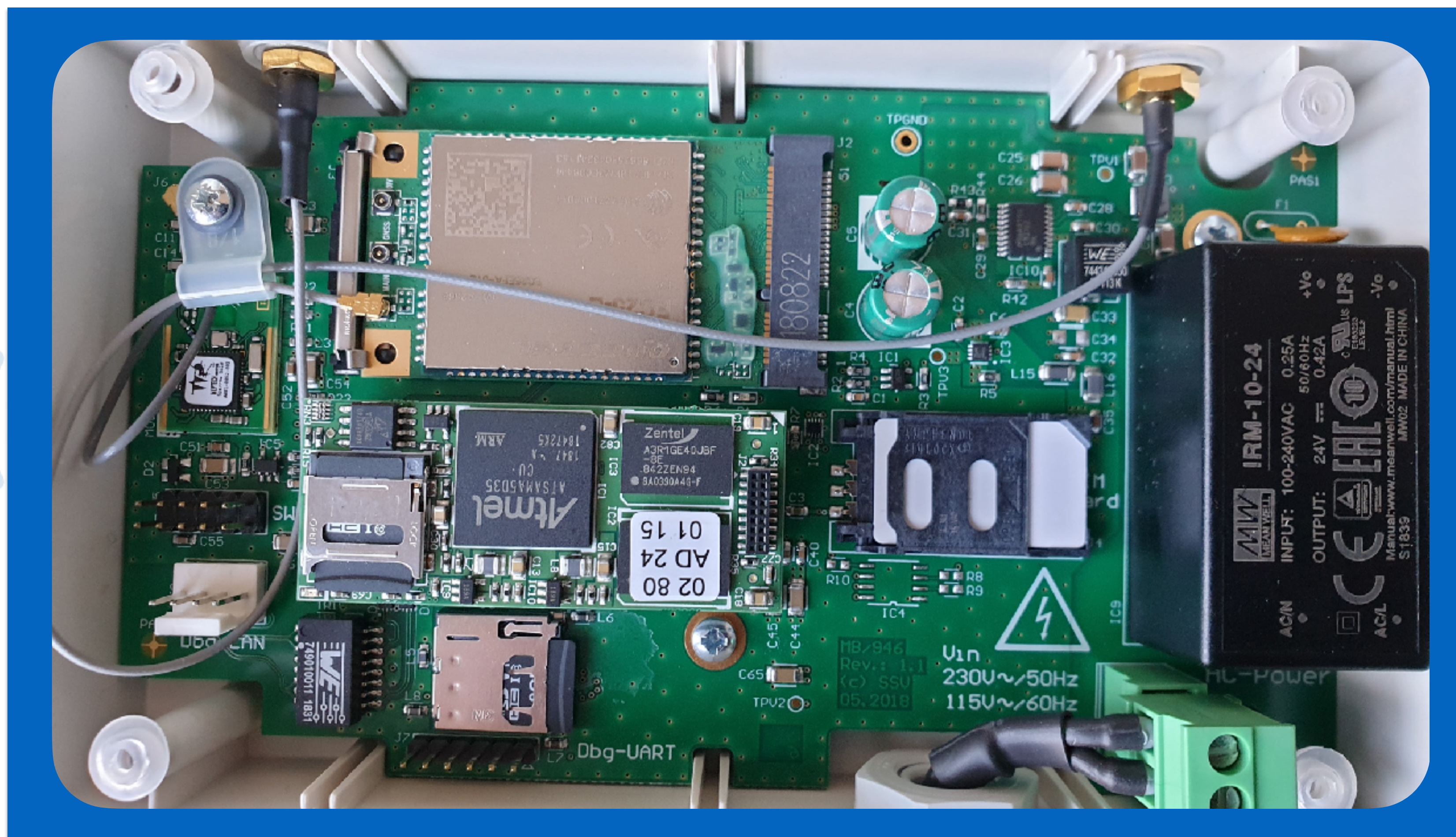


Awareness - was jeder wissen muss

- Jedes weggeworfene Gerät enthält potentiell
 - Zugangsdaten für weitere Systeme
 - Geheimnisse
 - Konfigurationen

Forensik

- Netzwerke überwachen
- Geräte "beschauen"
 - Reguläre Schnittstellen benutzen
 - Nicht vorgesehene Schnittstellen benutzen
 -

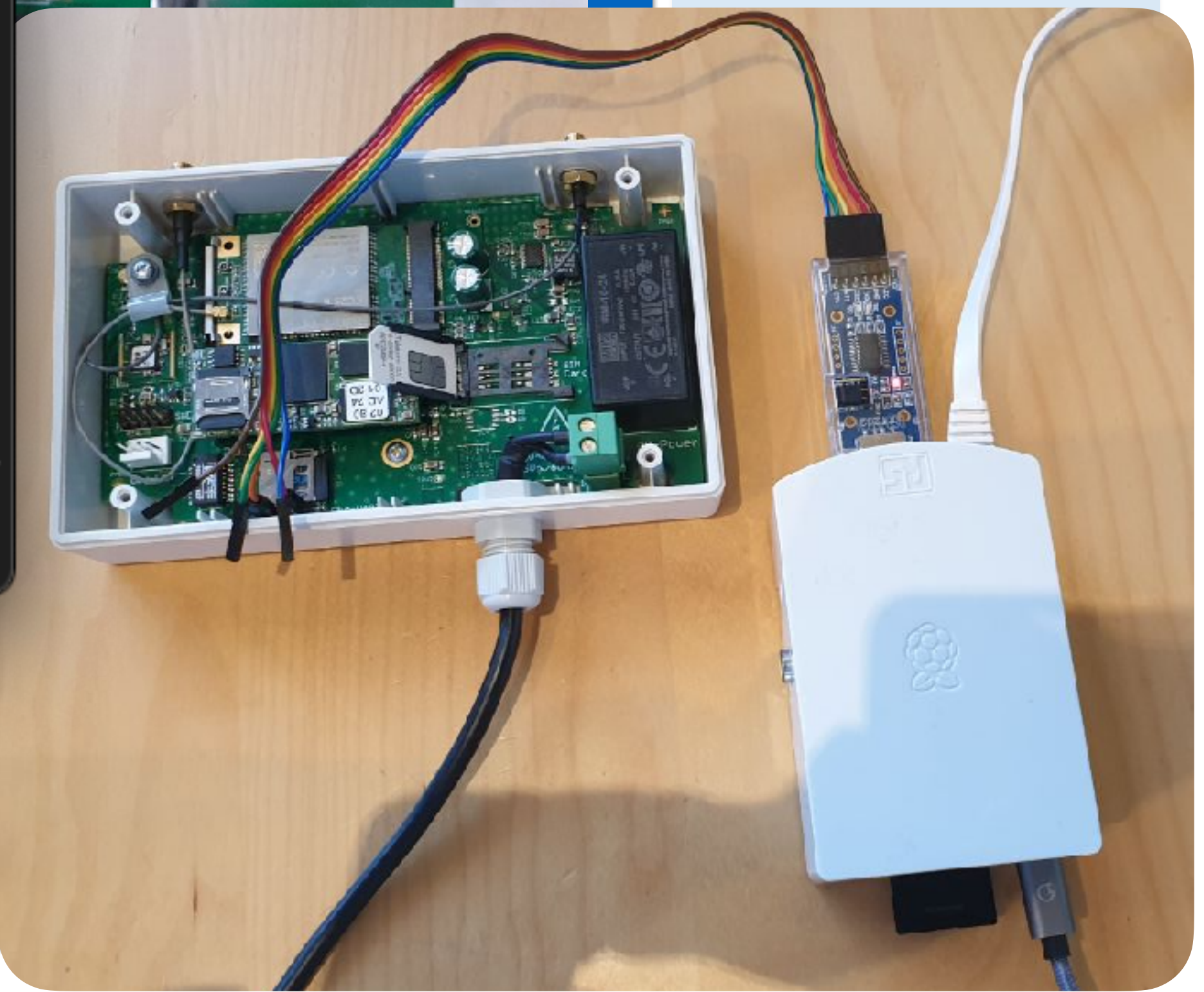


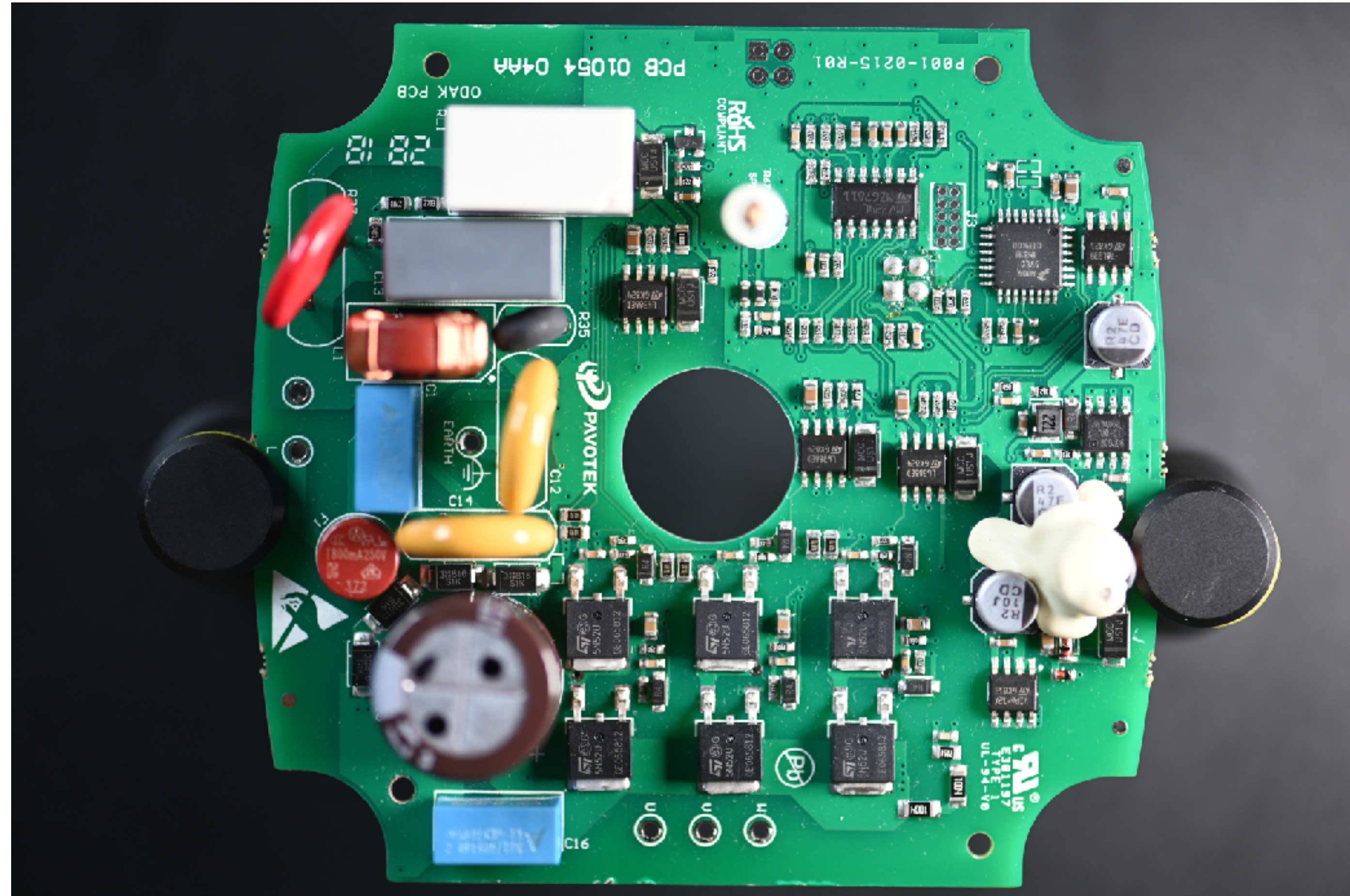

```
thm — pi@raspberrypi: ~ — ssh pi@139.30.241.16 — 107x31

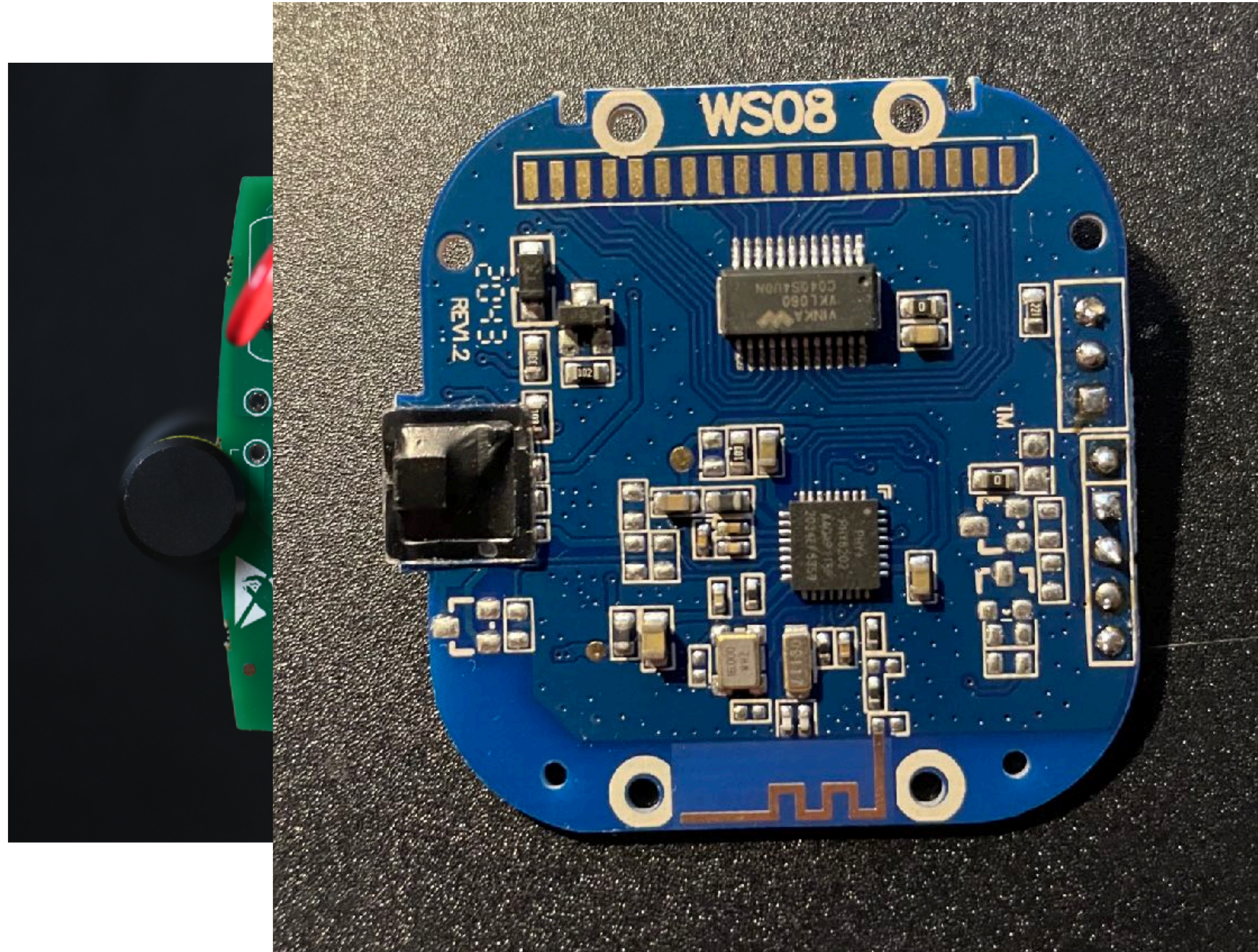
root      902      1 28 08:09 ?      00:00:12 /usr/local/bin/node --max_old_space_size=64 /usr/local/ksbd
systemd+  903      1  0 08:09 ?      00:00:00 /lib/systemd/systemd-resolved
root      905      1  0 08:09 ?      00:00:00 /bin/sh /etc/sshconfig/bin/wan-watch
root      907      1  0 08:09 ?      00:00:00 /usr/local/sbin/openvpn --config /etc/openvpn/ksbvpn.ssv-cf
root      923      2  0 08:09 ?      00:00:00 [kworker/0:3]
root      932      1  1 08:09 ttyS0    00:00:00 /bin/login --
webui     948      1  0 08:09 ?      00:00:00 /usr/sbin/lighttpd -f /etc/lighttpd/webconfig.conf
root      950      2  0 08:09 ?      00:00:00 [kworker/u2:2]
root      967      1  0 08:09 ?      00:00:00 /usr/local/bin/thread-tun-daemon /dev/ttyS1 fslthr0 -f -s i
root      971      1  0 08:09 ?      00:00:00 /usr/sbin/sshd -D -u0
root      974      2  0 08:09 ?      00:00:00 [kworker/0:4]
root     1309      1  0 08:09 ?      00:00:00 /bin/sh /etc/sshconfig/bin/ppp0-watch
root     1327    1309  0 08:09 ?      00:00:00 sleep 60
root     1362     932  0 08:09 ttyS0    00:00:00 -bash
root     1780     902  1 08:09 ?      00:00:00 journalctl -f -o json
root     1834      1  0 08:09 ?      00:00:00 /lib/systemd/systemd-timedated
root     1992      1  0 08:09 ?      00:00:00 /usr/sbin/watchdog -f
root     1994    1992  0 08:09 ?      00:00:00 [watchdog-test] <defunct>
root     2001      1  0 08:09 ?      00:00:00 /bin/sh /etc/sshconfig/bin/ssvfirmware checkfirmware
root     2112    2001  0 08:09 ?      00:00:00 /bin/sh /usr/local/sbin/ssvfsccheck match
root     2146    2112  0 08:09 ?      00:00:00 /bin/sh /usr/local/sbin/ssvfsccheck match
root     2147    2146  1 08:09 ?      00:00:00 mount
root     2148    2146  0 08:09 ?      00:00:00 grep /dev/mmcblk.p. on /media/rfs-ro type squashfs
root     2149    2146  0 08:09 ?      00:00:00 cut -d -f1
root     2232     902  0 08:09 ?      00:00:00 sh -c /etc/sshconfig/init.d/modem.sh status
root     2233    2232  0 08:09 ?      00:00:00 /bin/sh /etc/sshconfig/init.d/modem.sh status
root     2241     905  0 08:09 ?      00:00:00 sleep 10
root     2256    2233  0 08:09 ?      00:00:00 chat -V -t 1 ABORT no network service ATE0V1 OK AT+CSQ OK3
root     2260    1362  0 08:09 ttyS0    00:00:00 ps -ef
root@G94619S1424012D:~#
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Offline | ttyUSB0
```

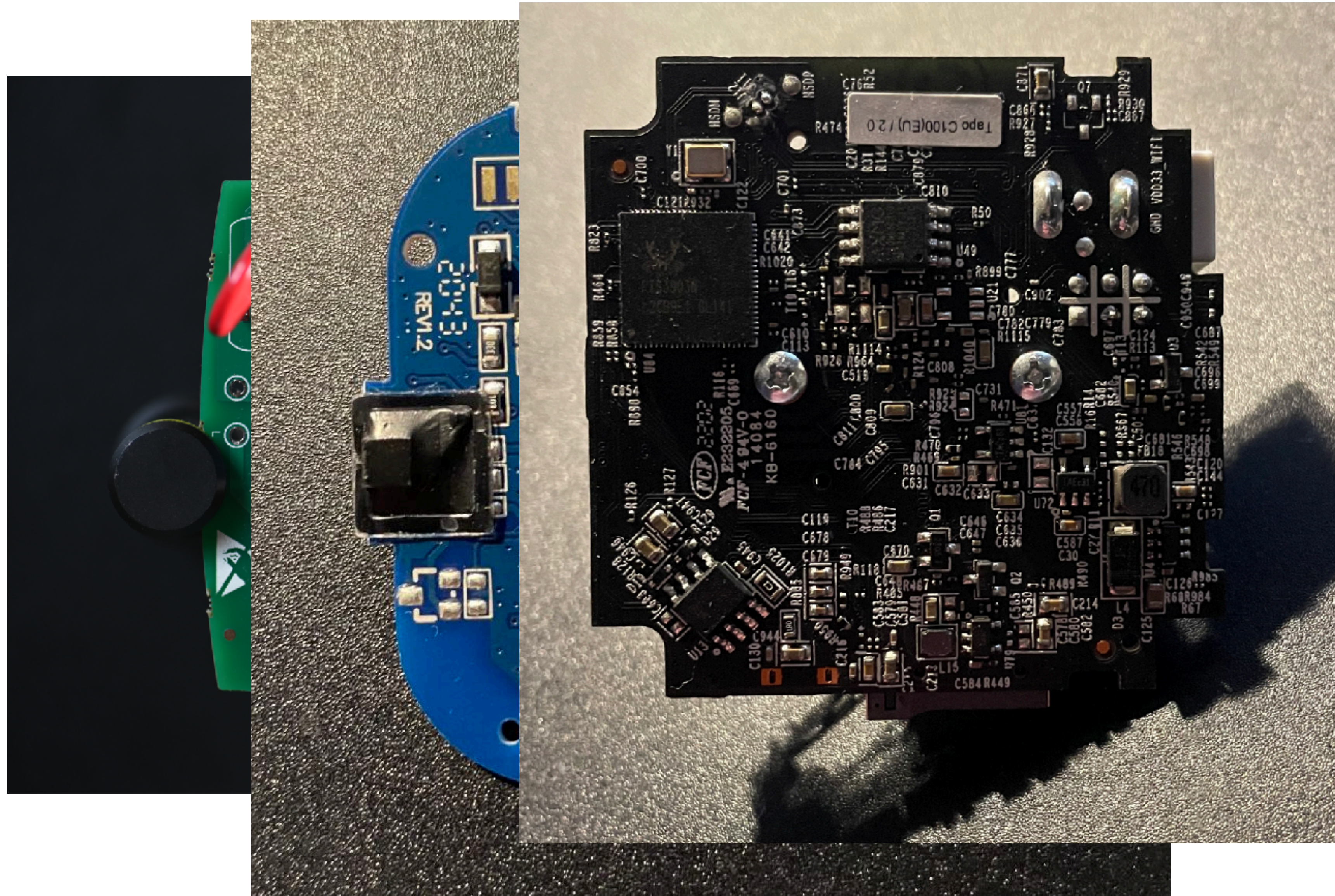


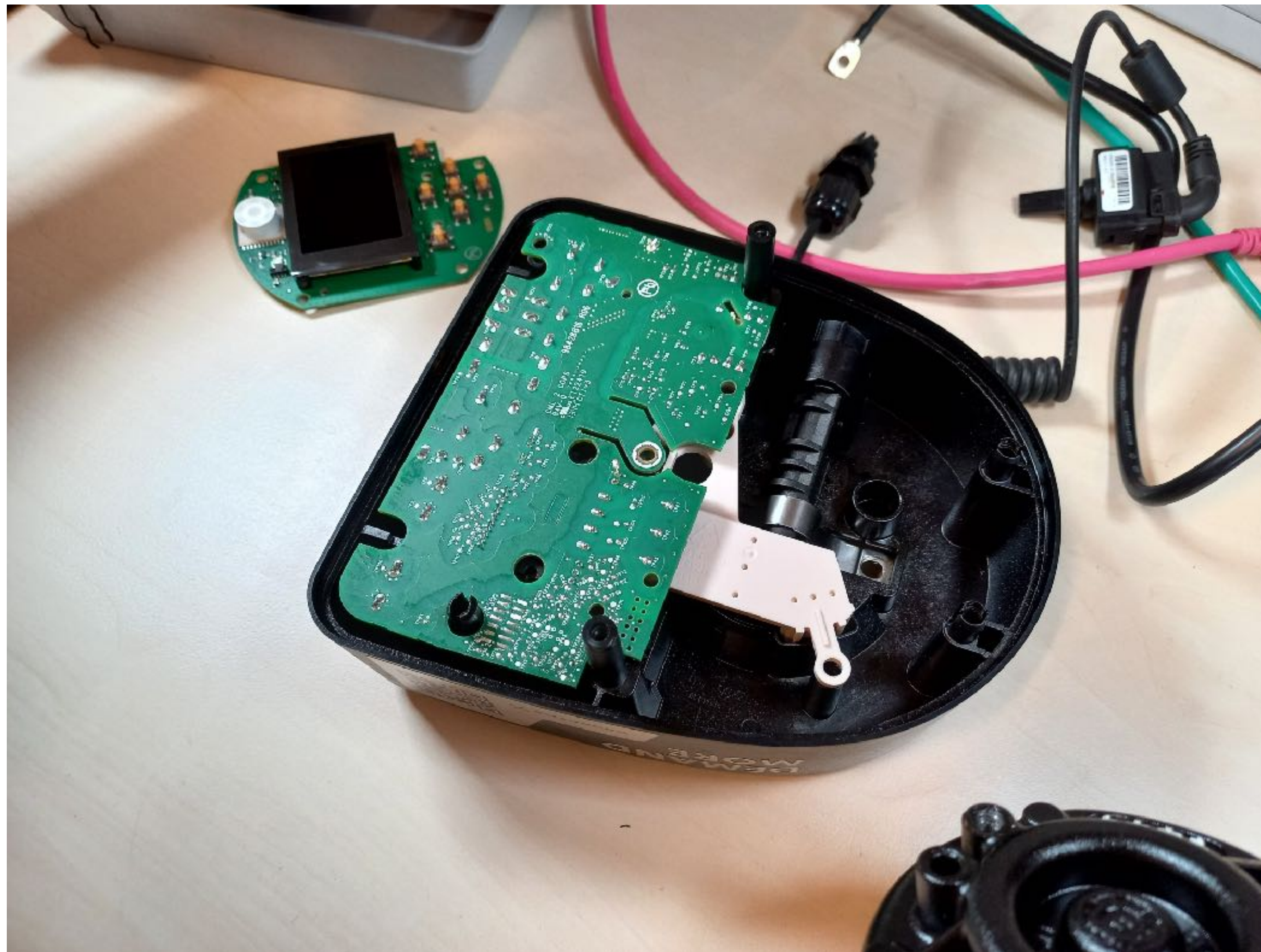
Pump

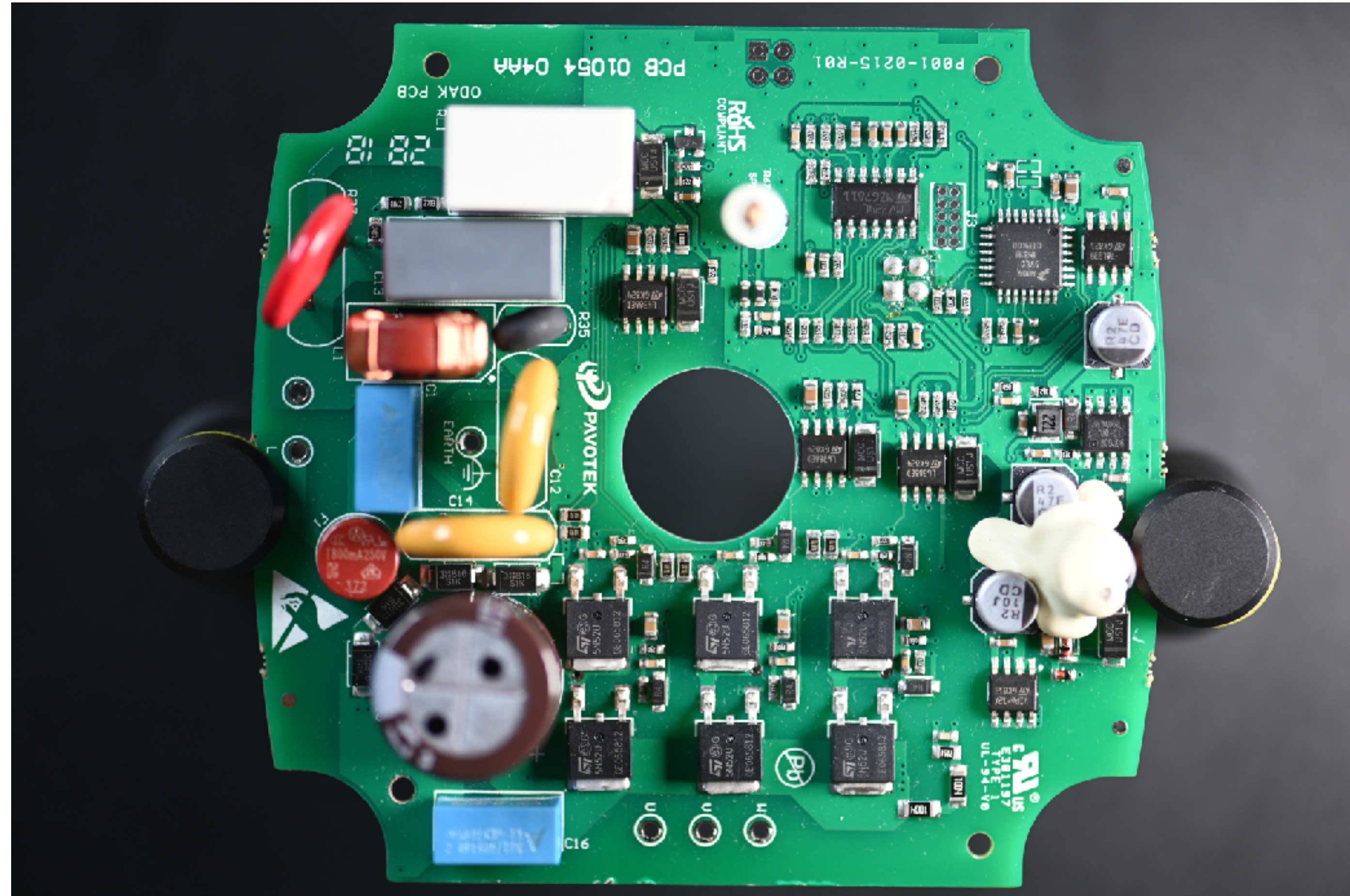


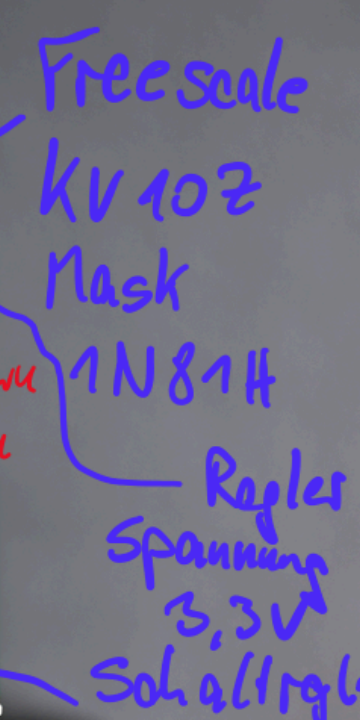


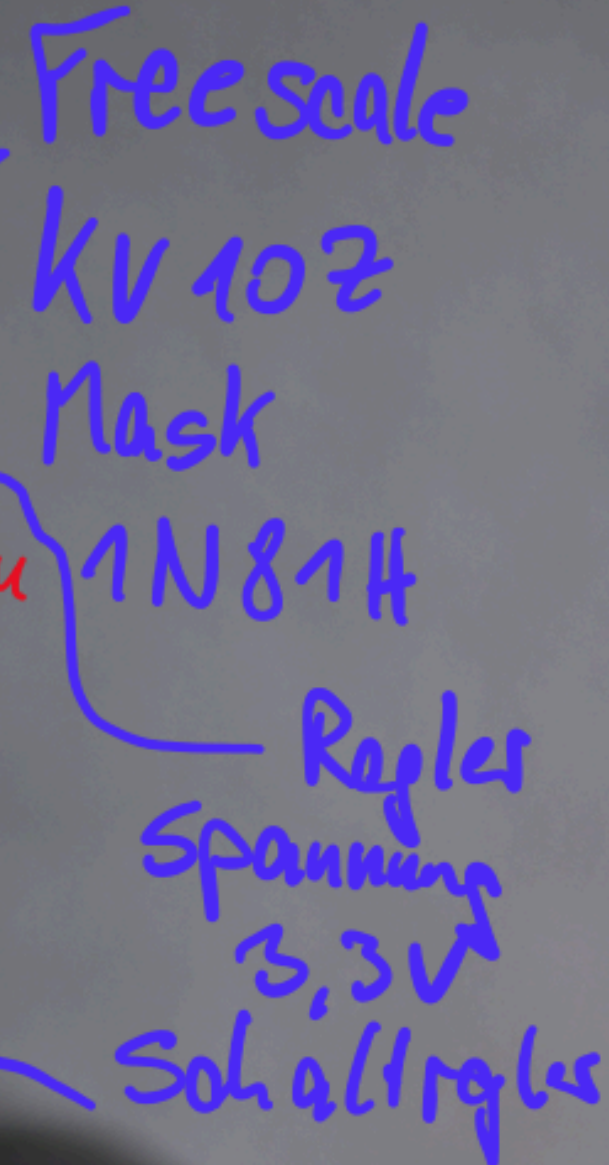


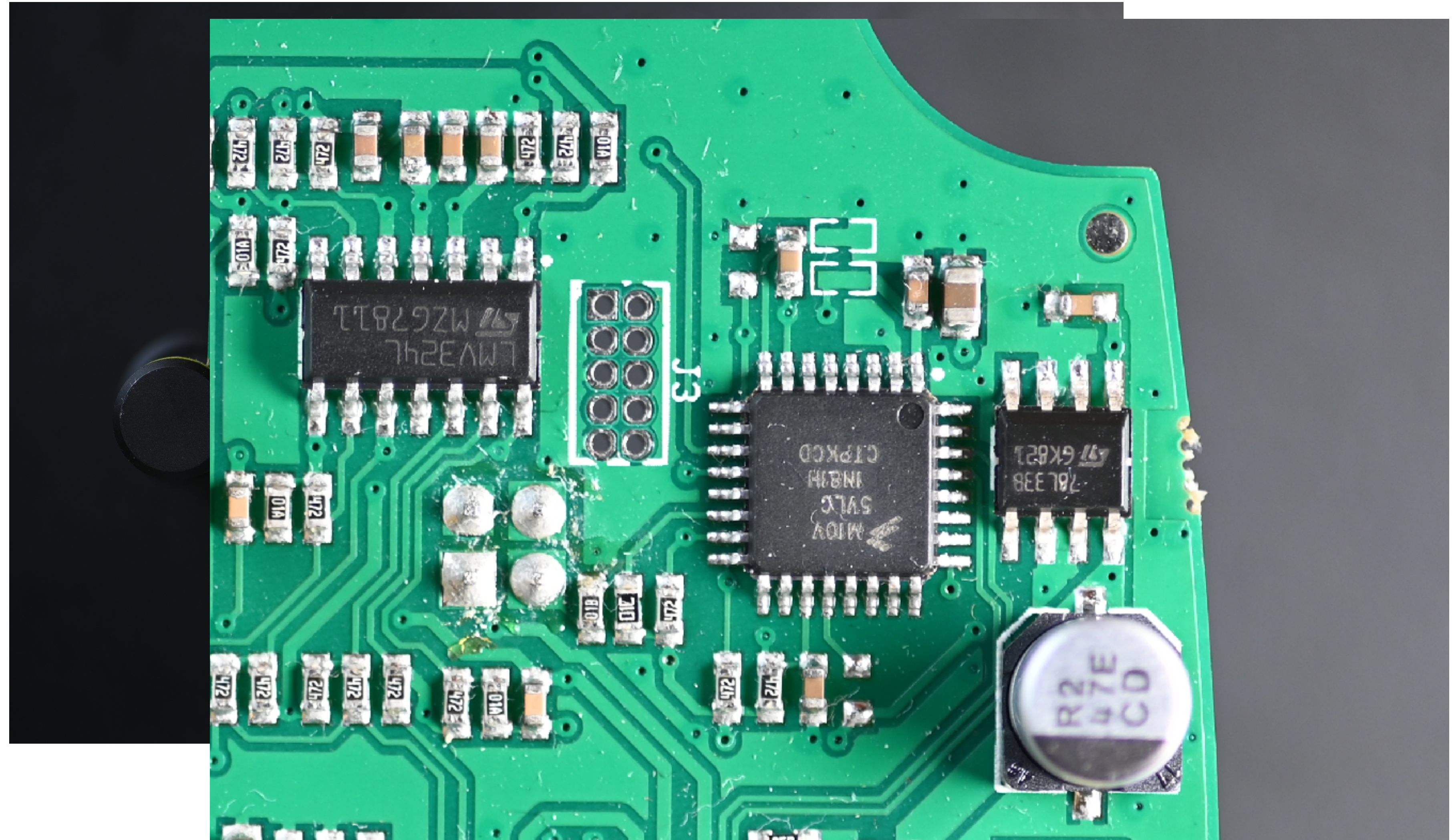


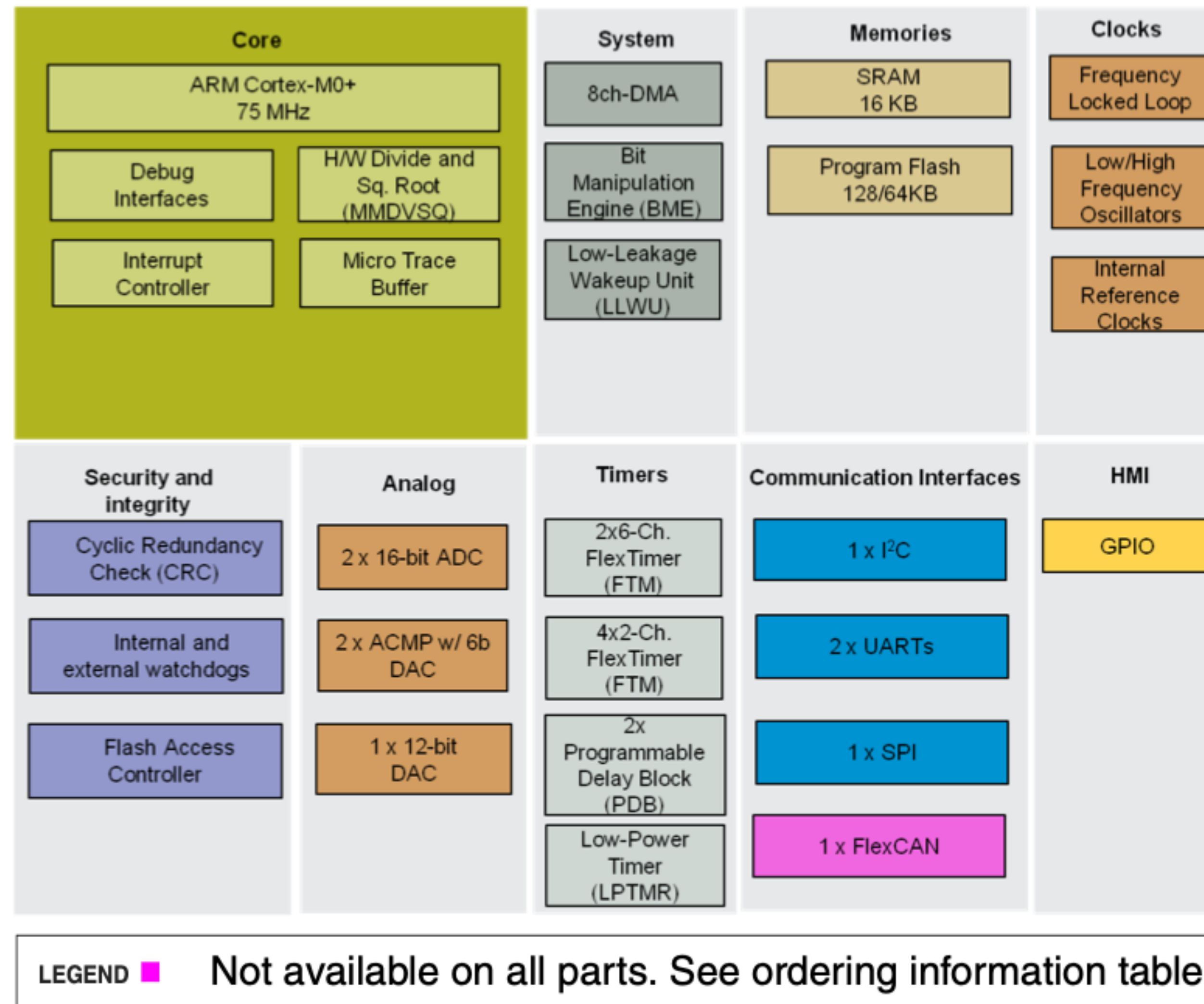


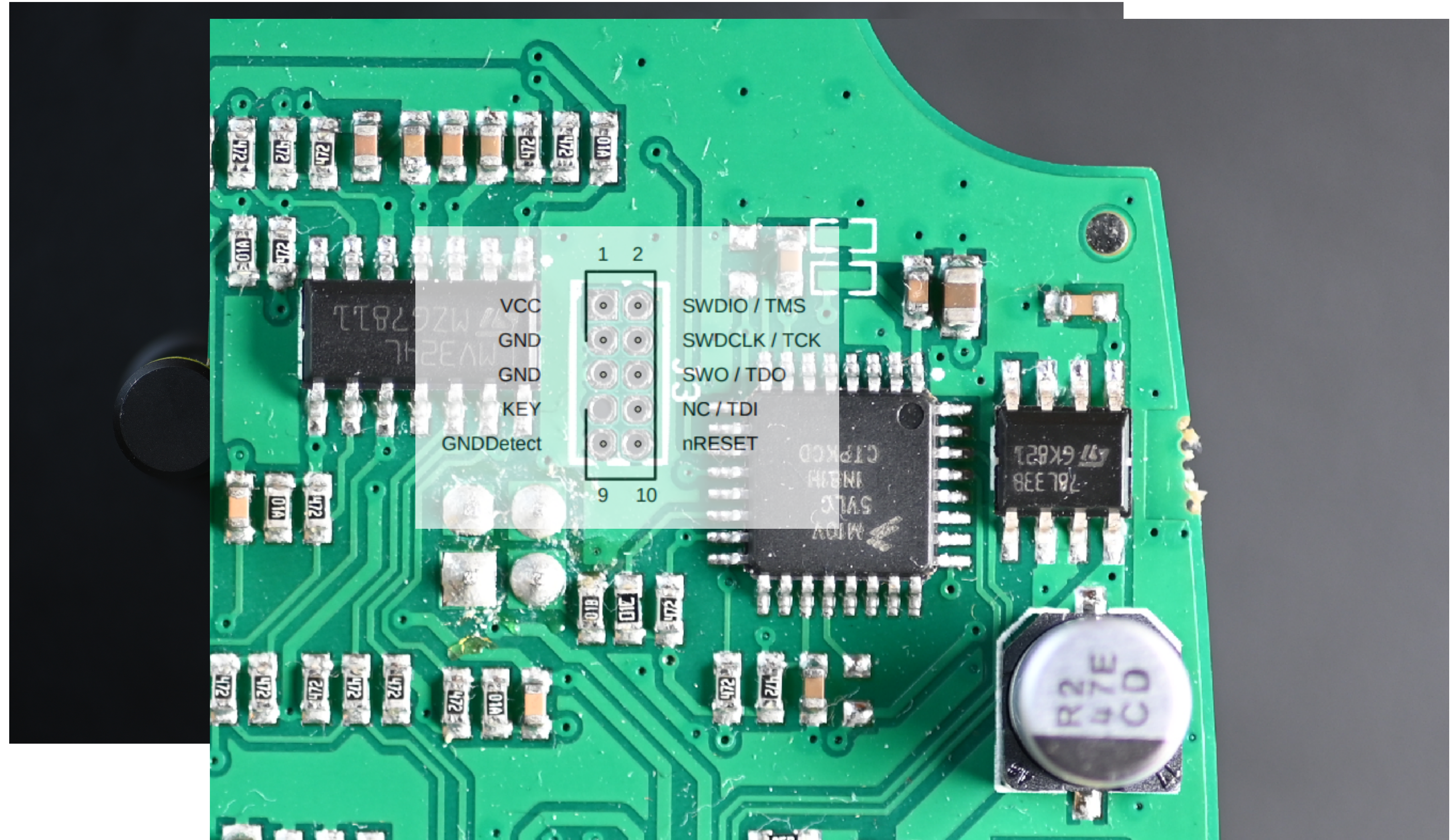


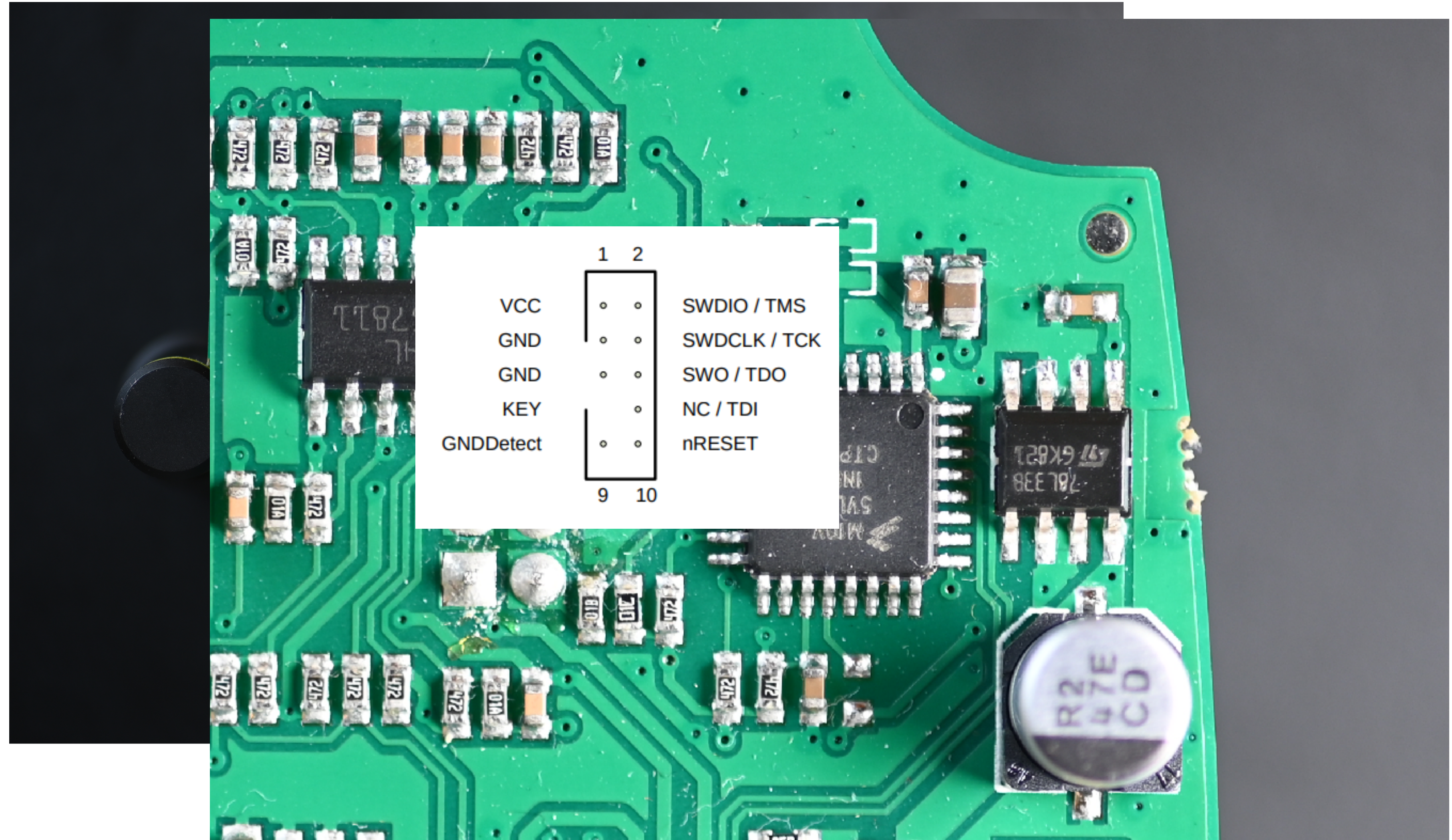


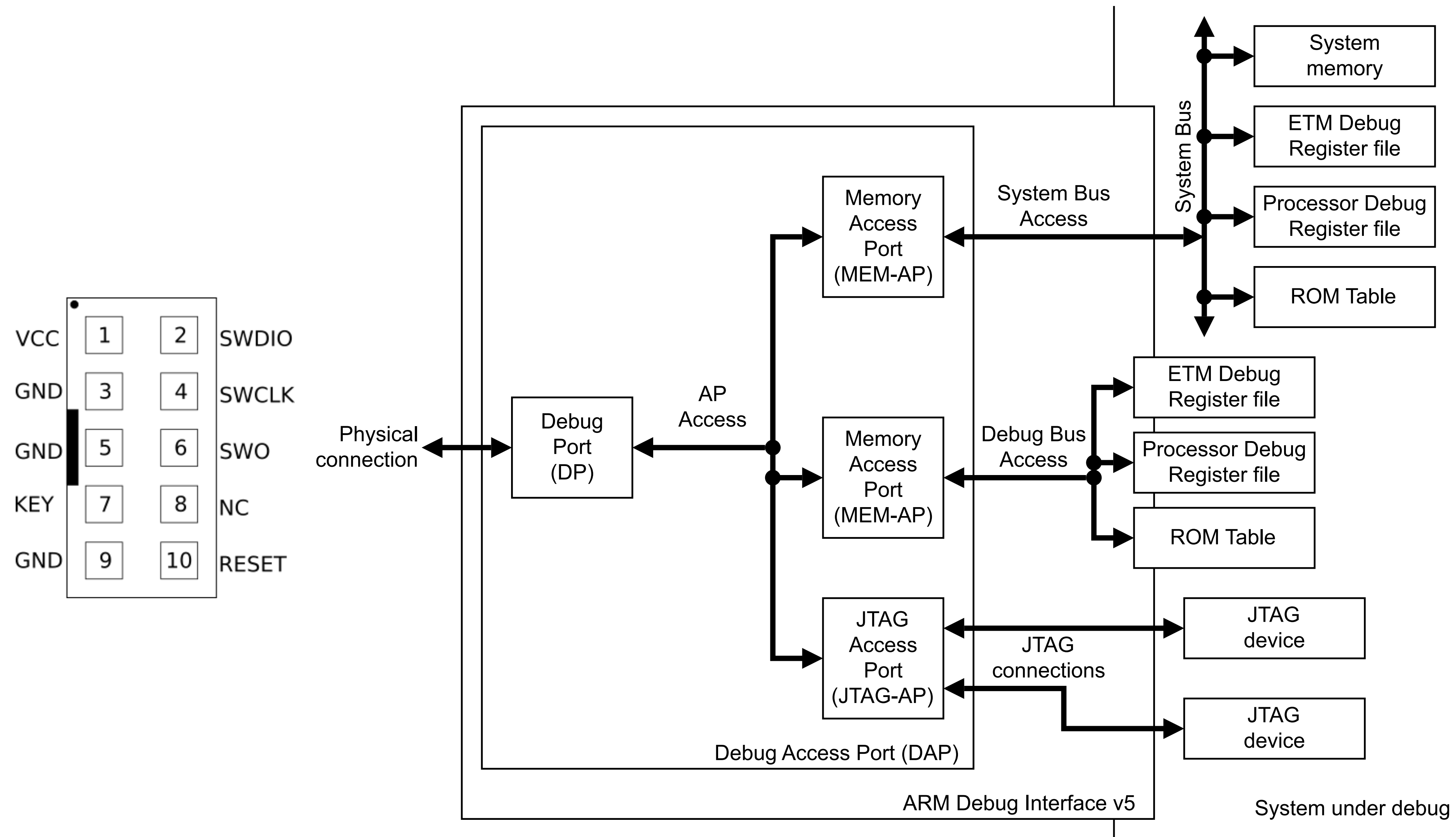


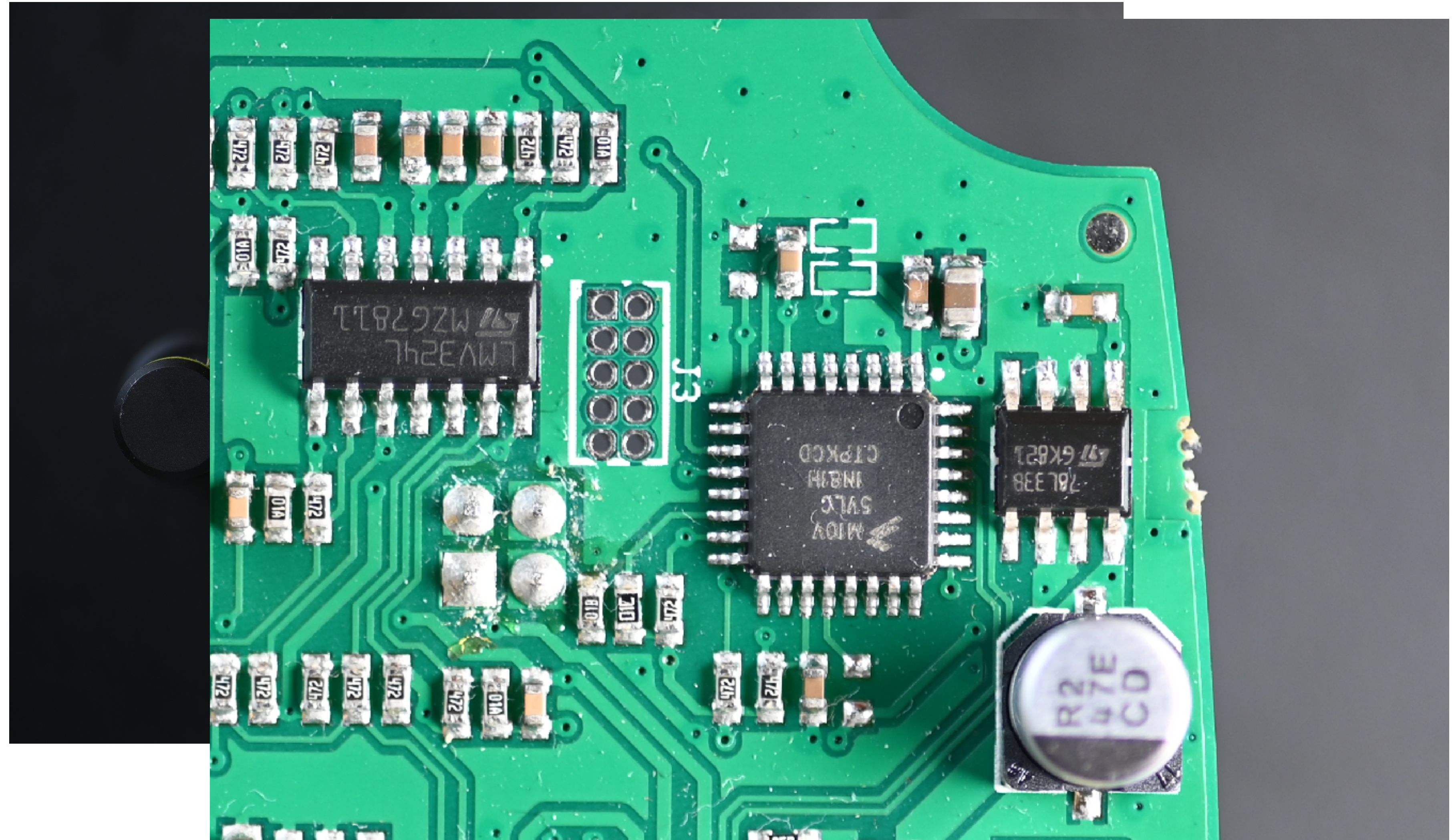


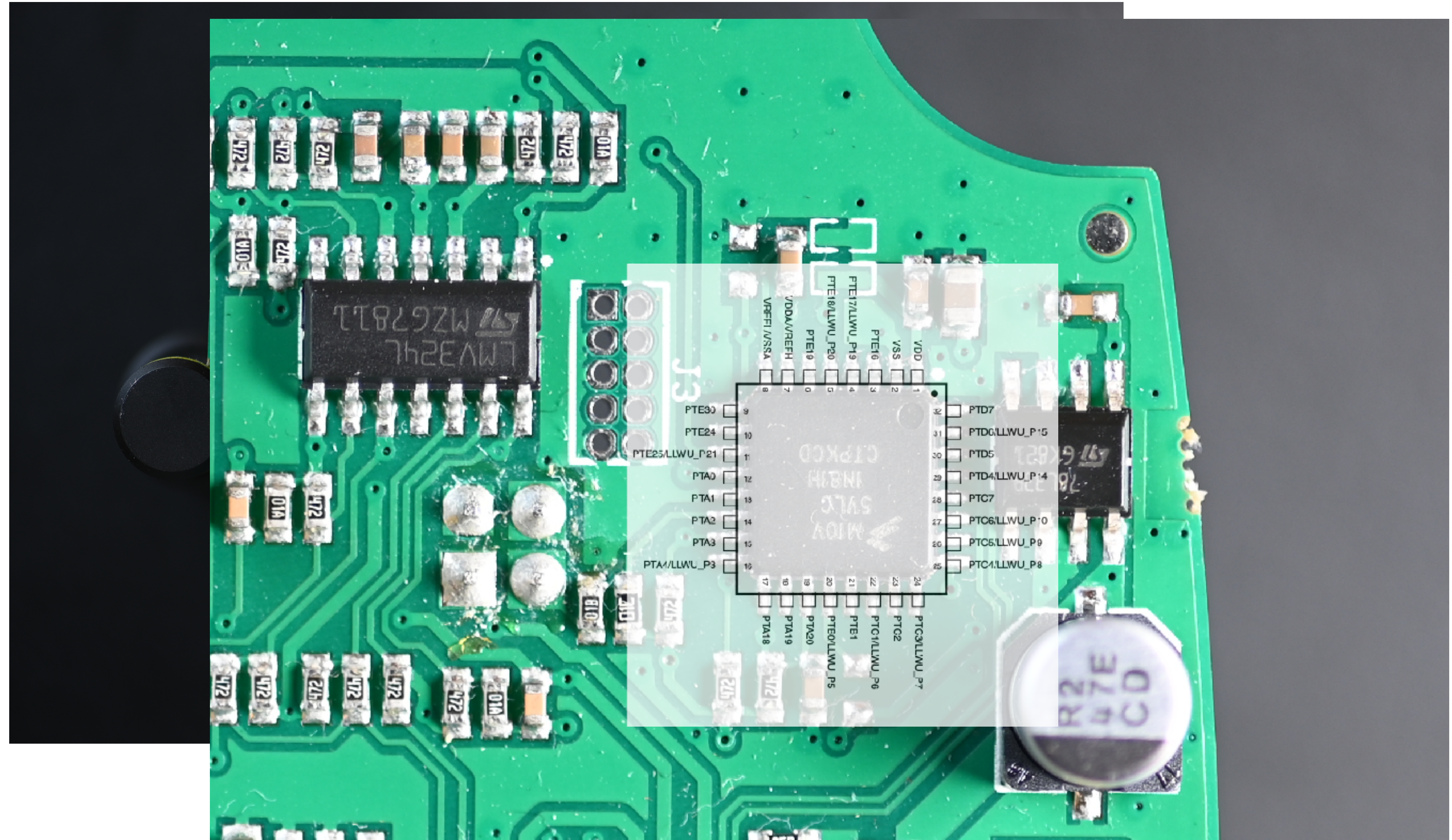


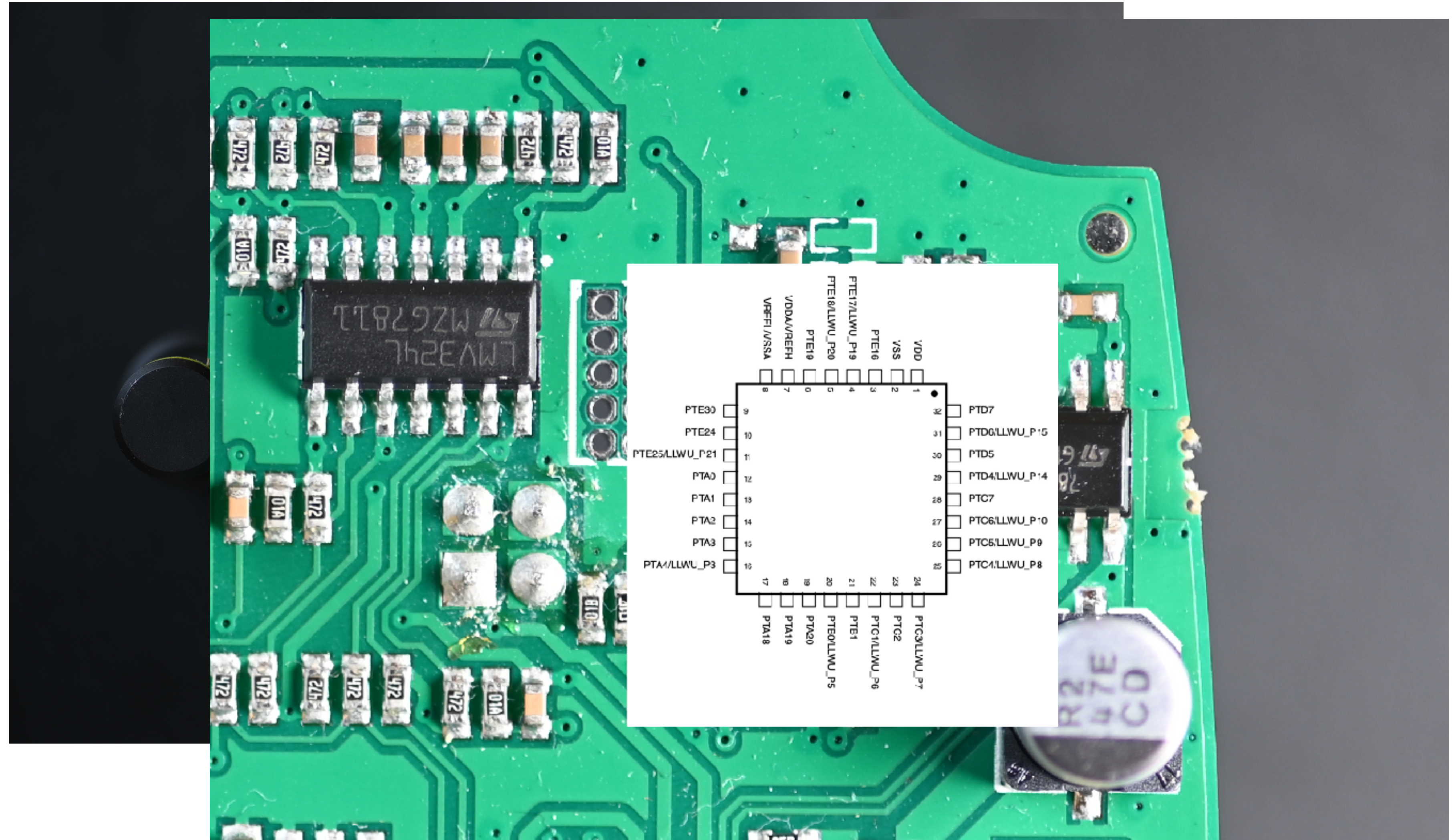


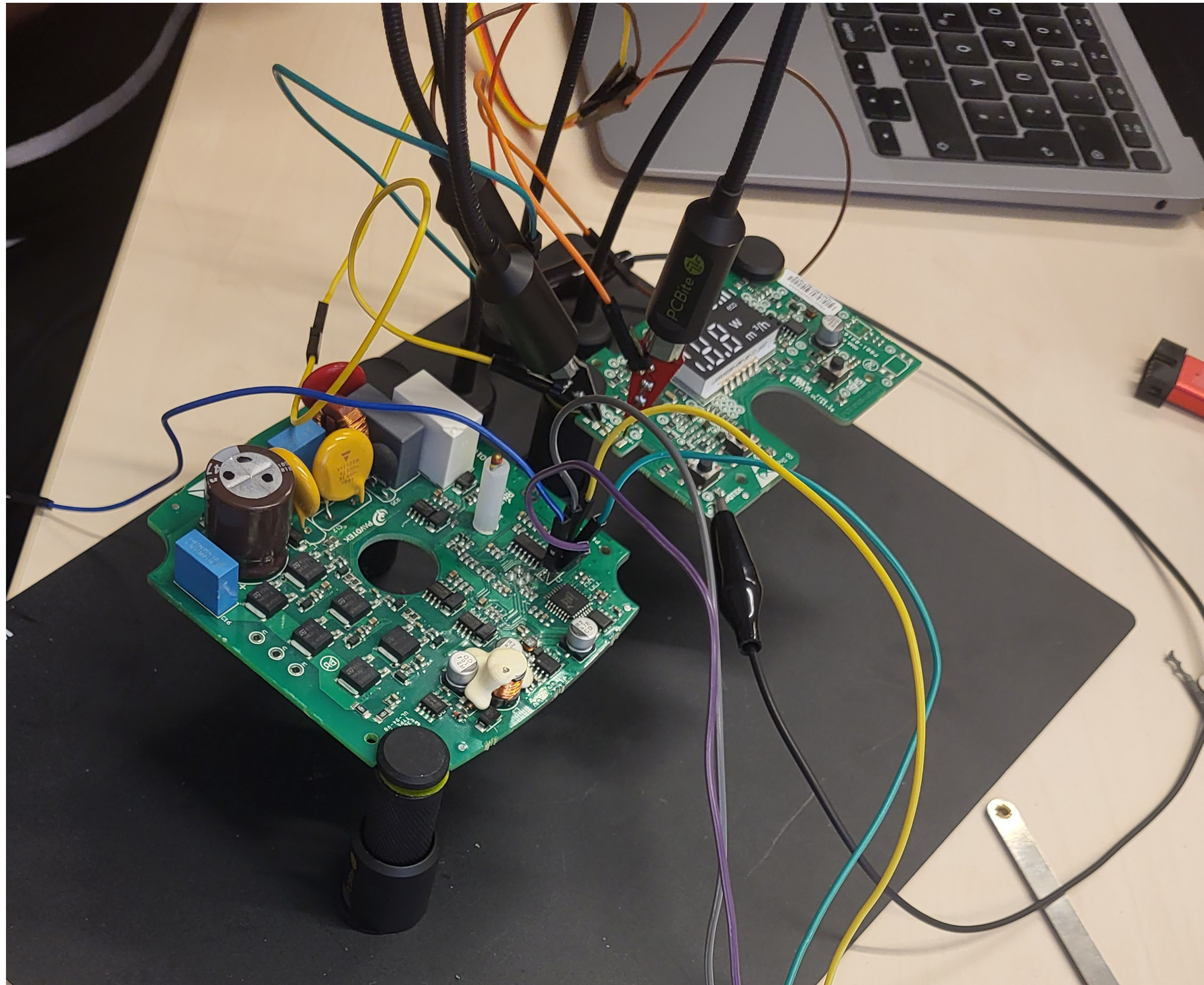


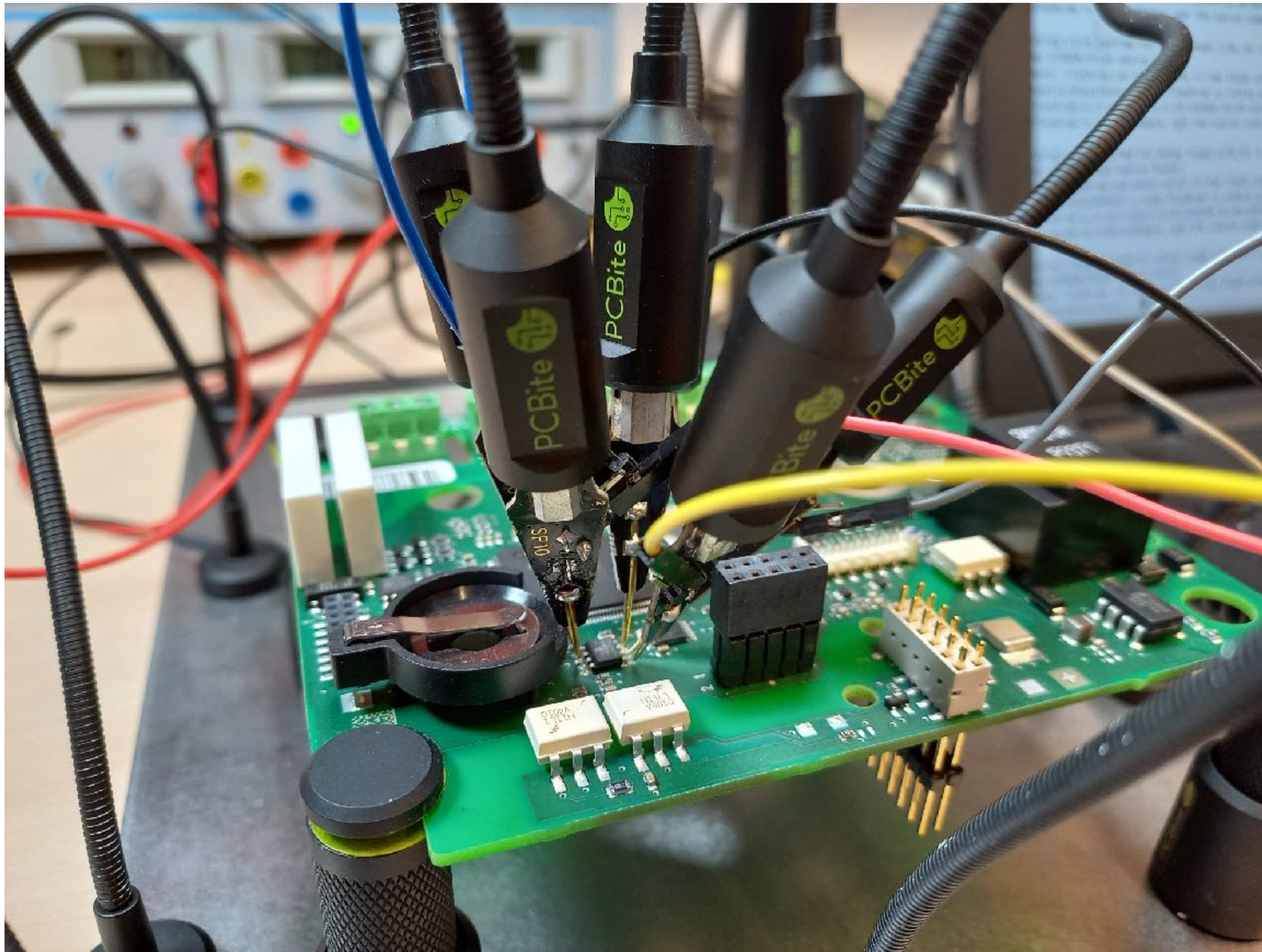






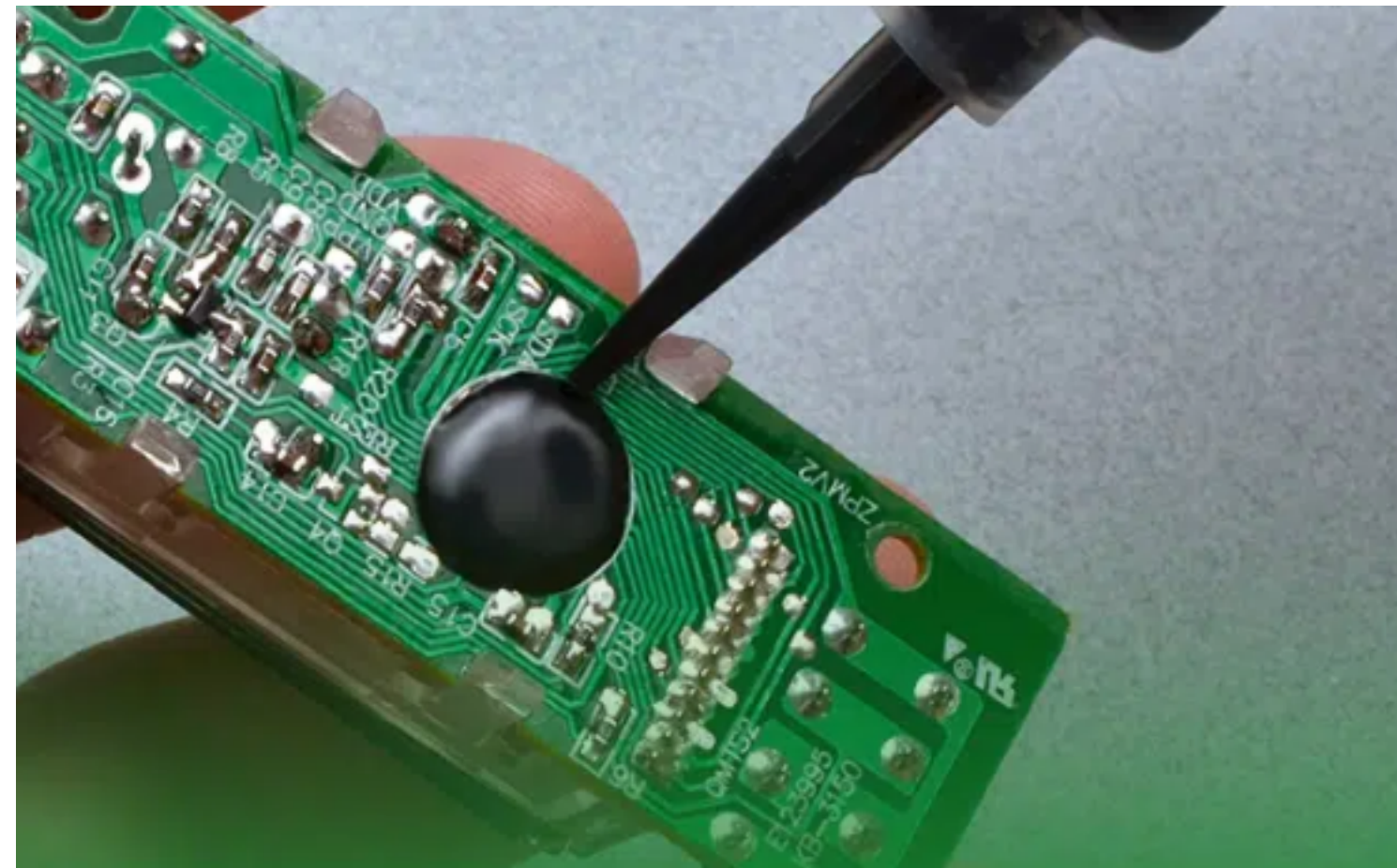






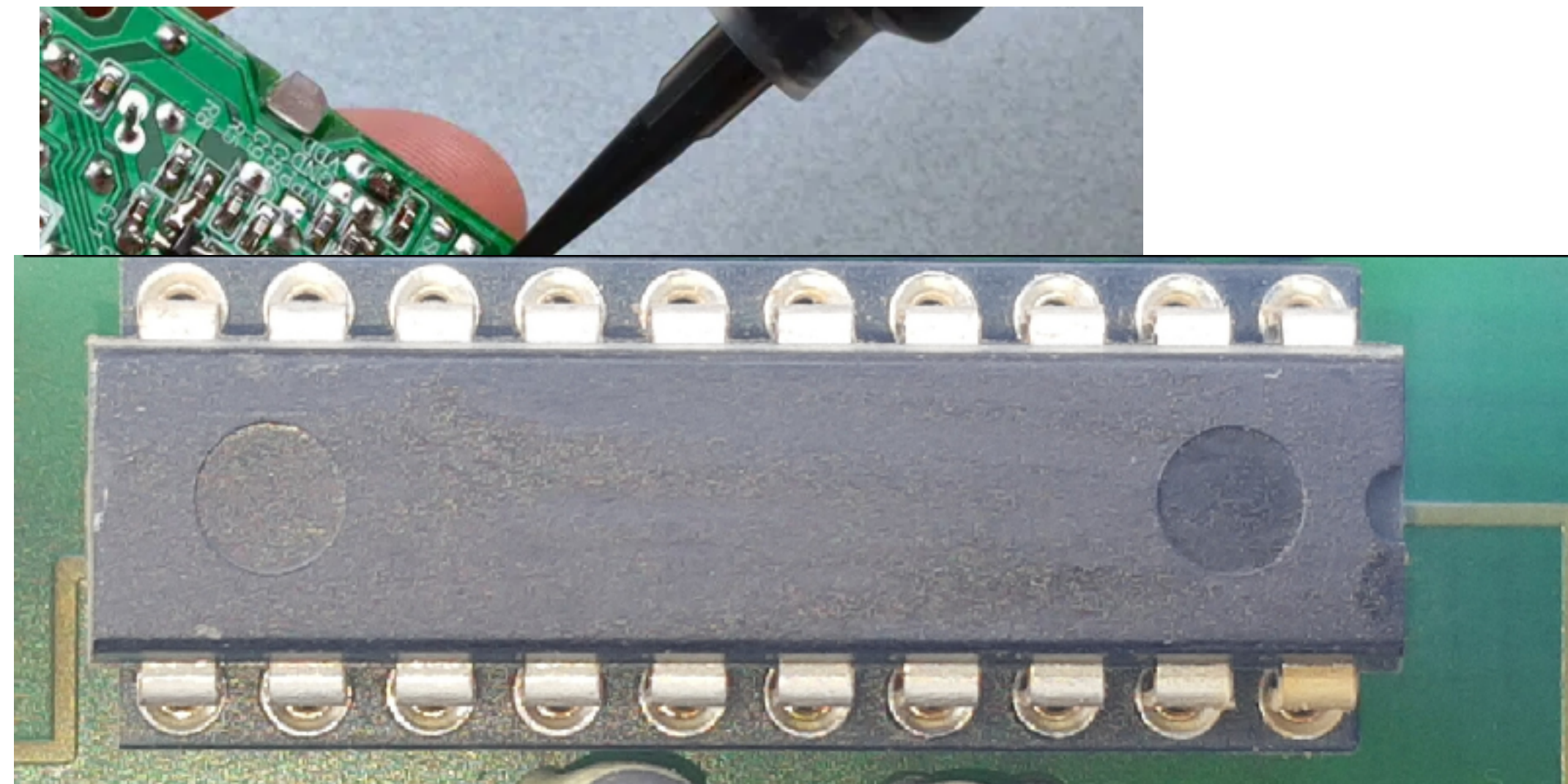
Gegenmaßnahmen

- Plastik Cover
- Labels abkratzen
- Fuses
- Verschlüsselung



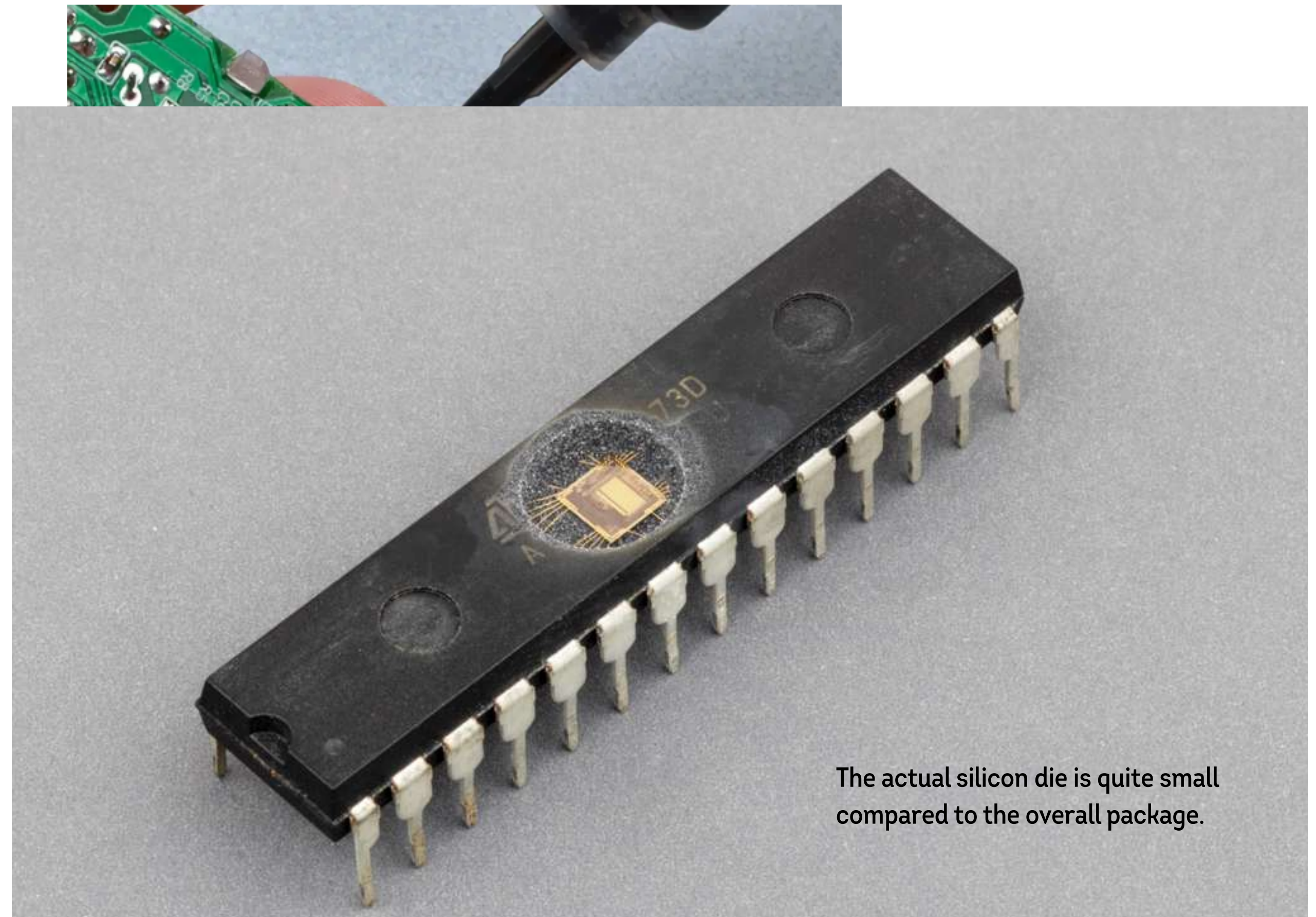
Gegenmaßnahmen

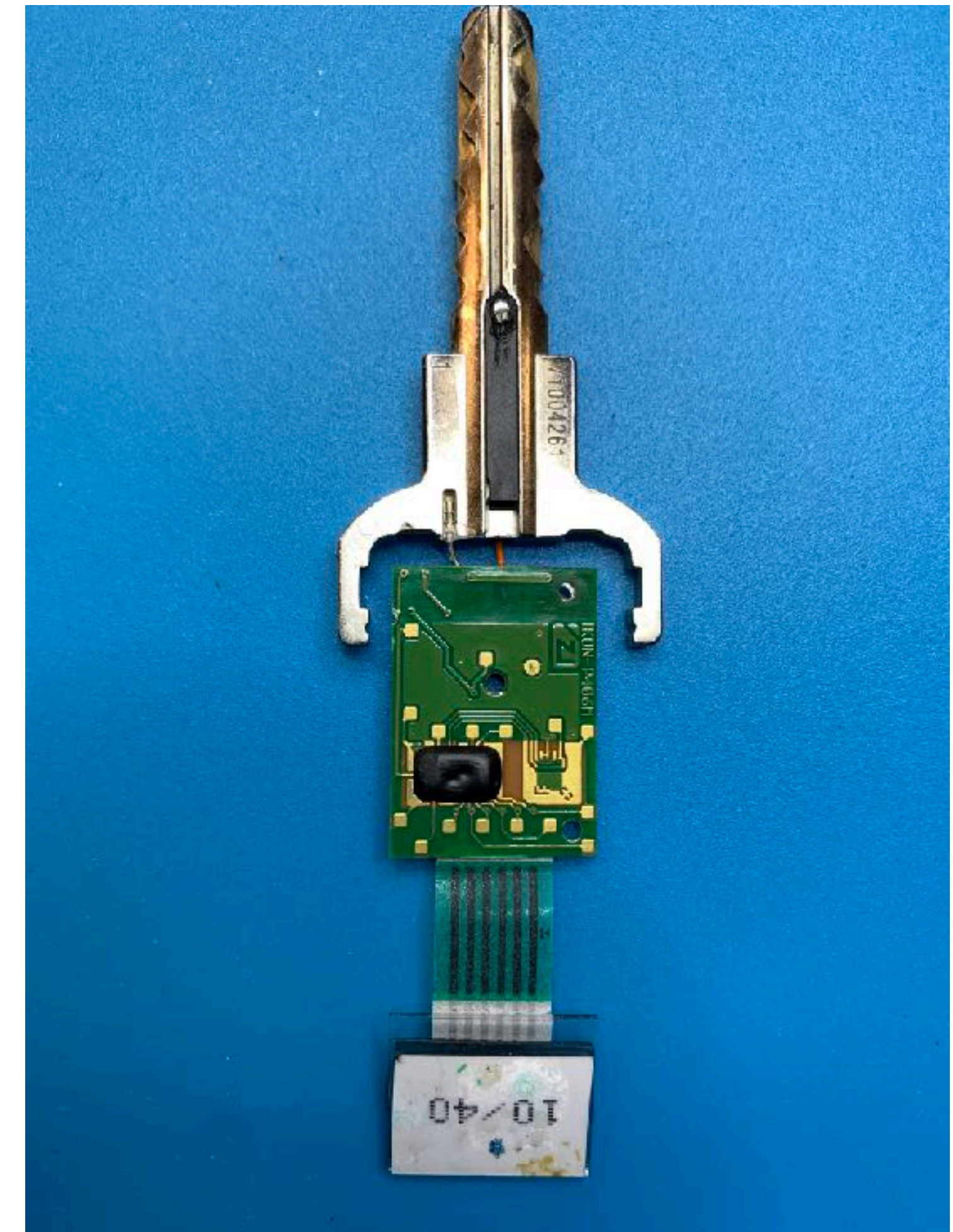
- Plastik Cover
- Labels abkratzen
- Fuses
- Verschlüsselung

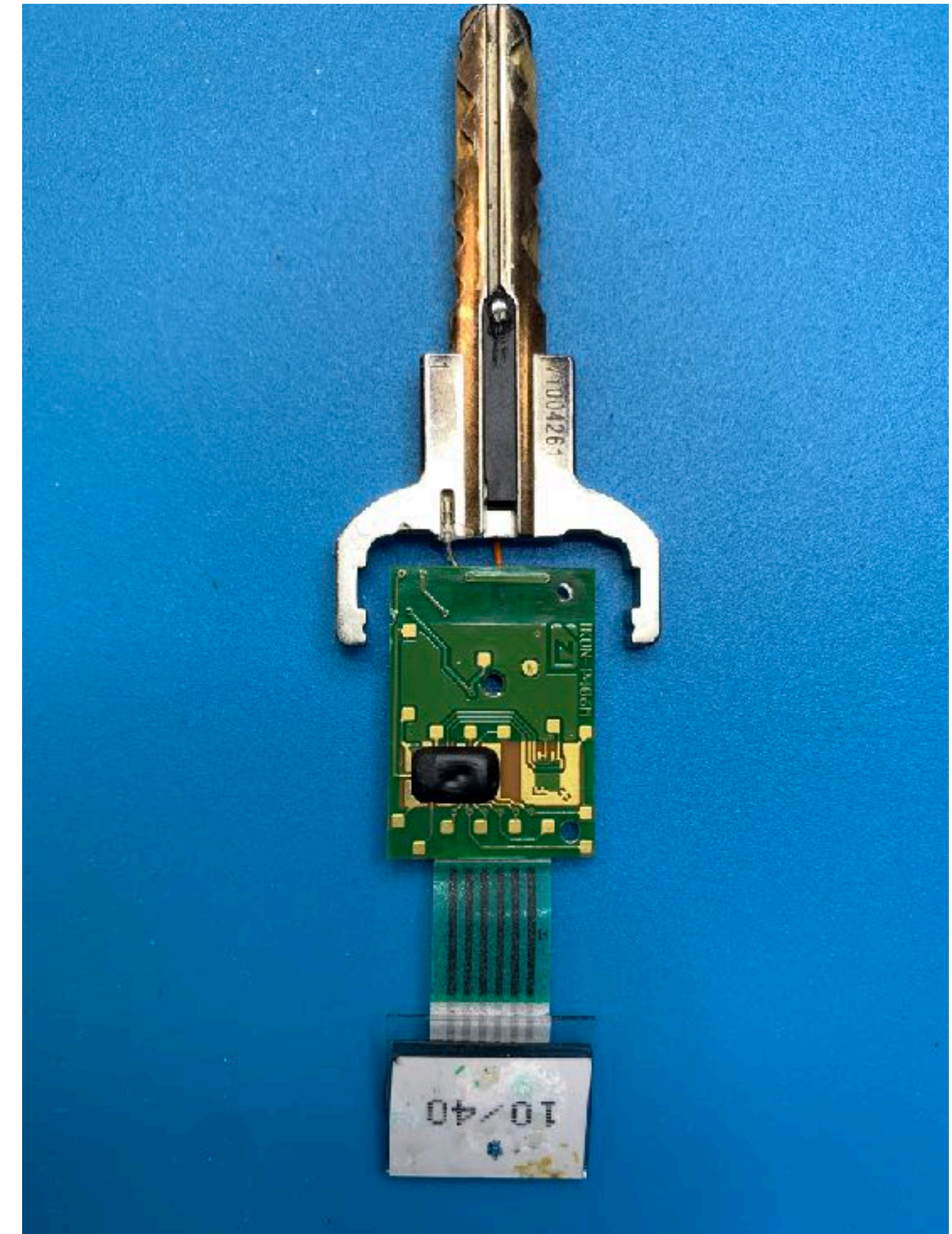
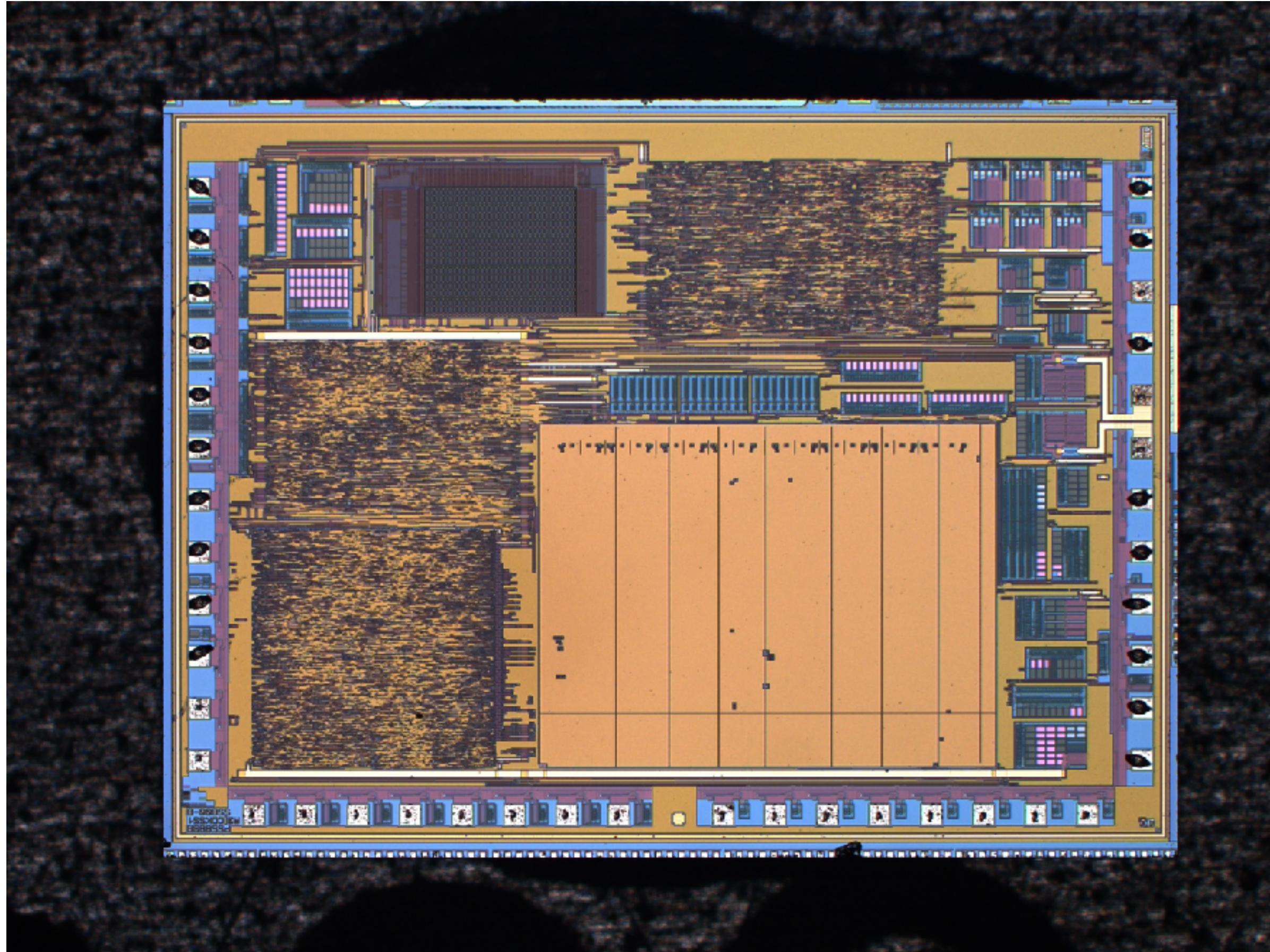


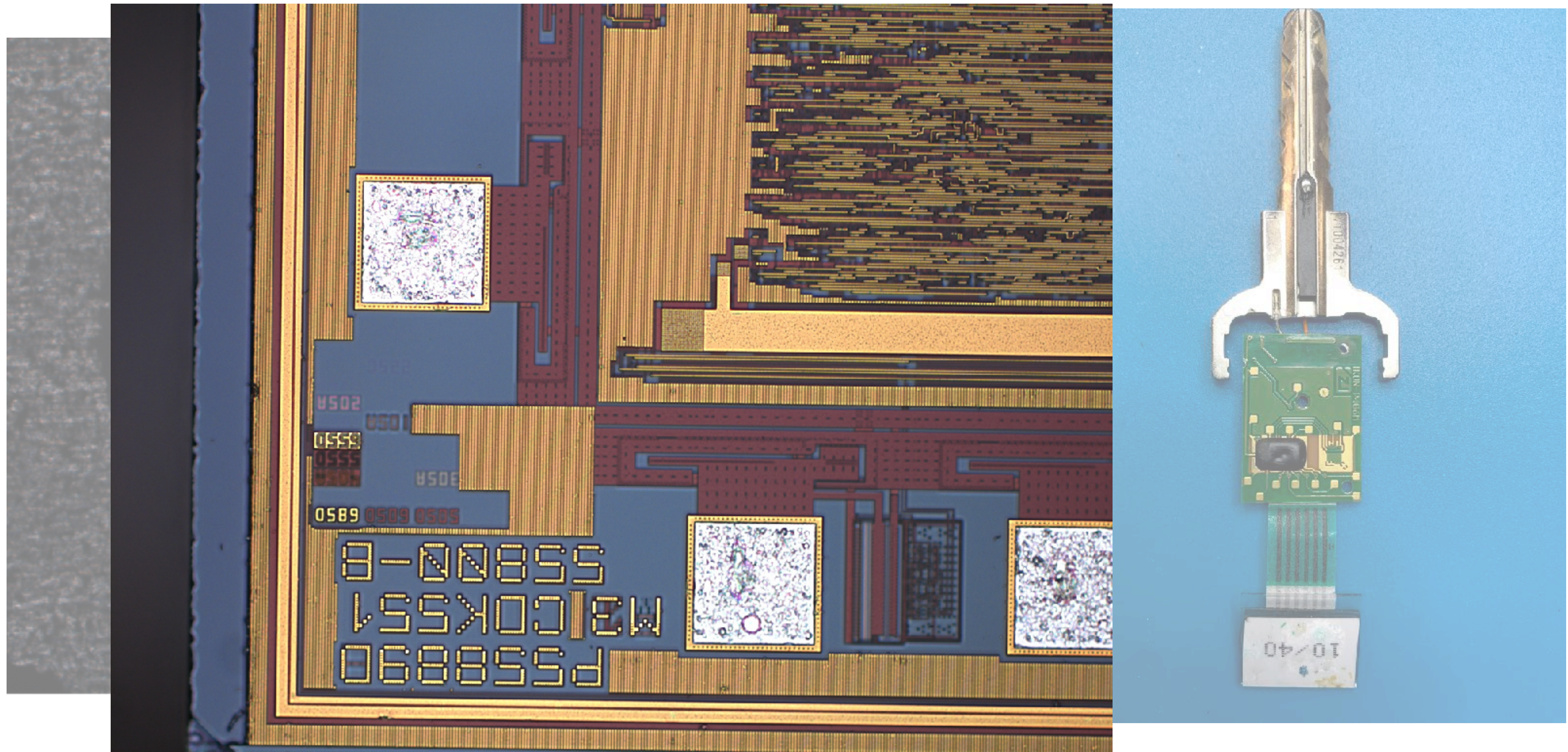
Gegenmaßnahmen

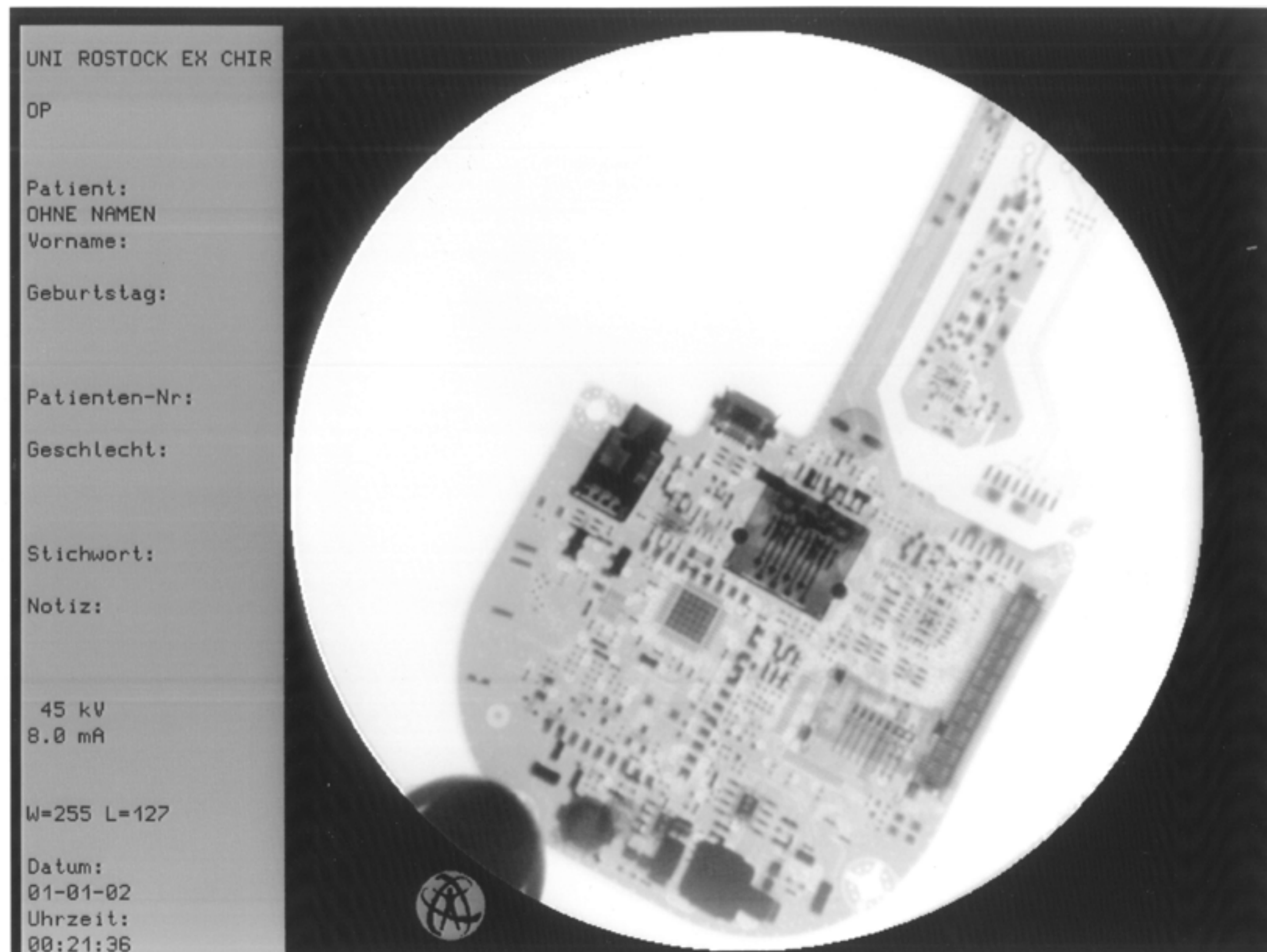
- Plastik Cover
- Labels abkratzen
- Fuses
- Verschlüsselung

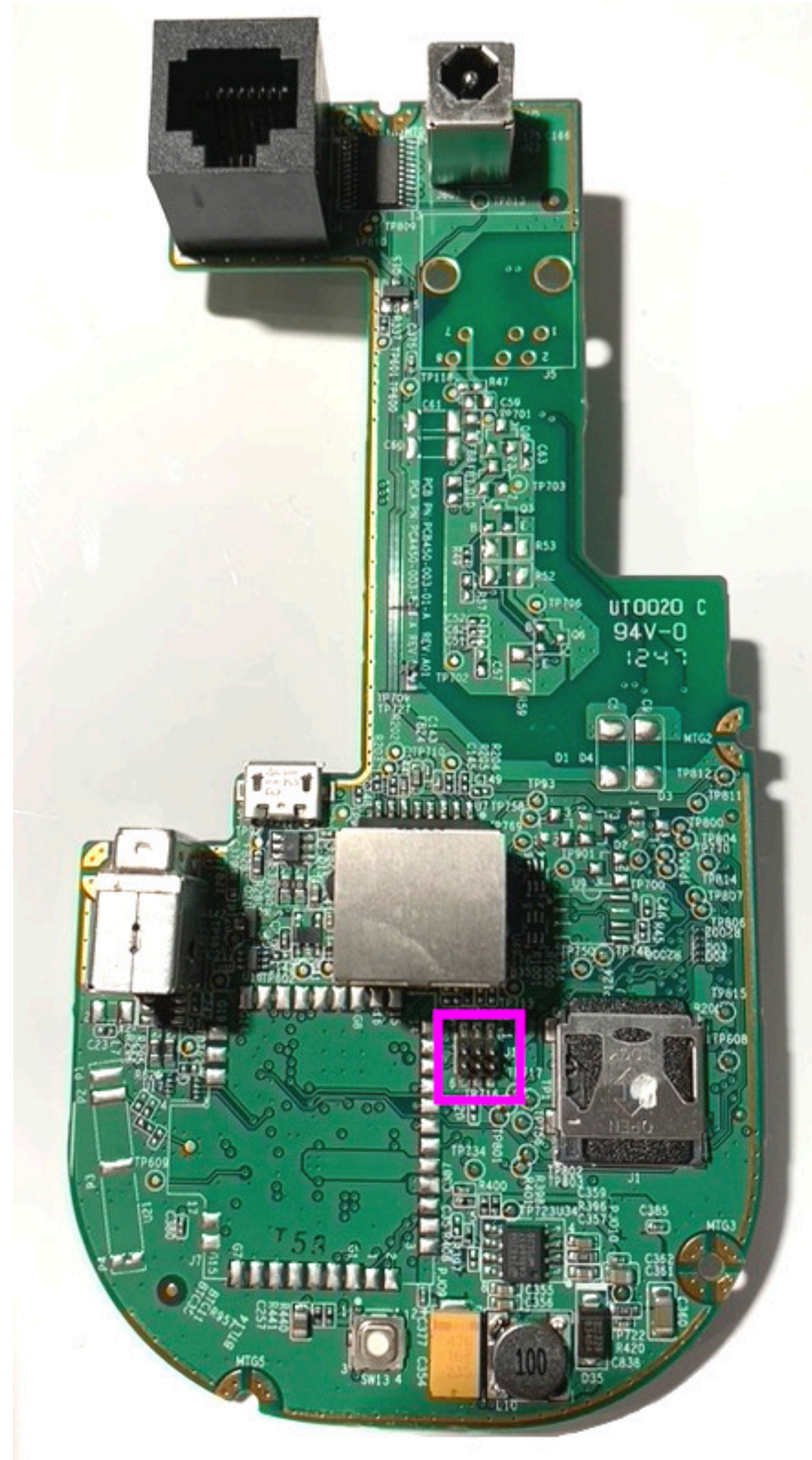




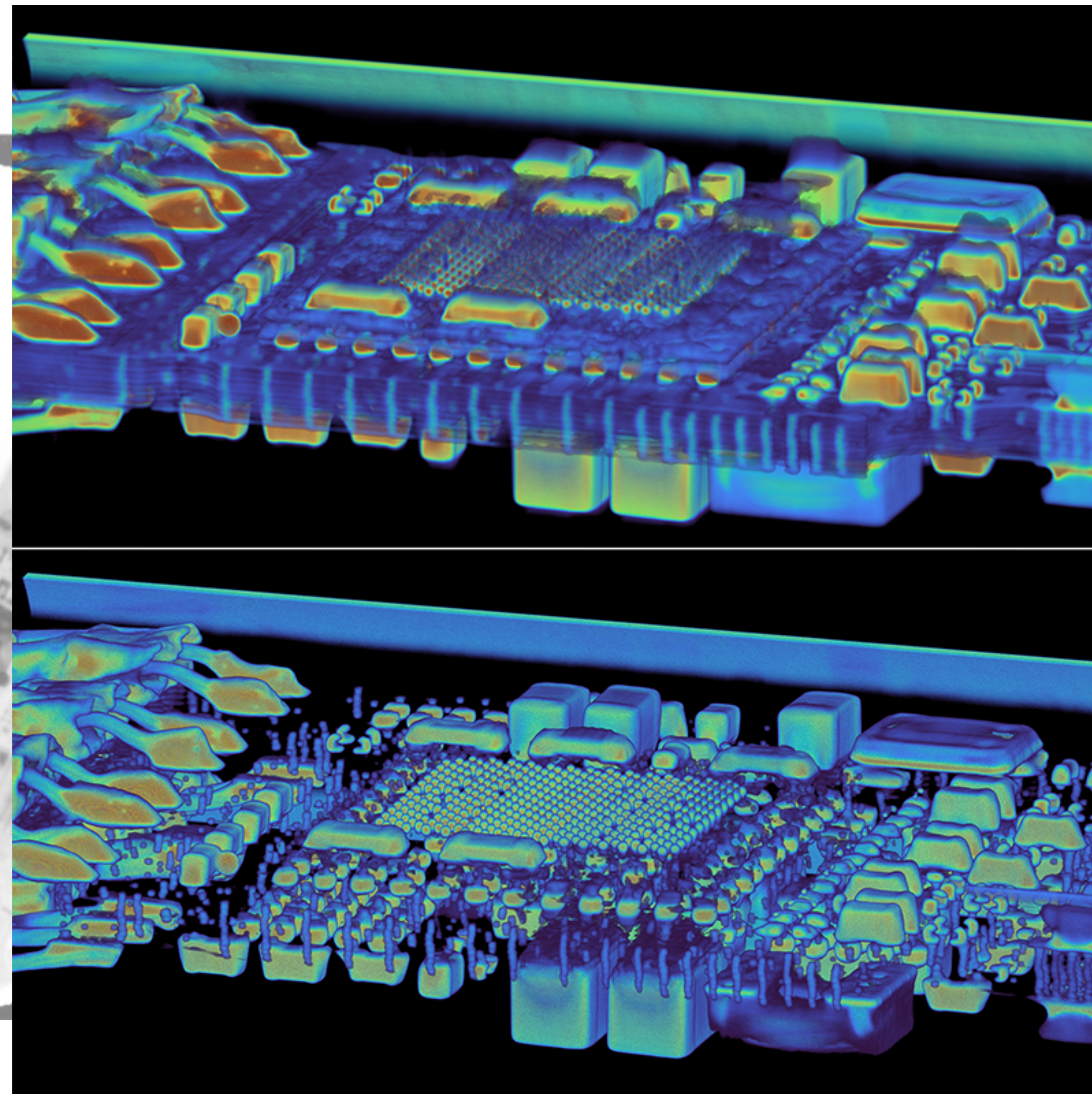
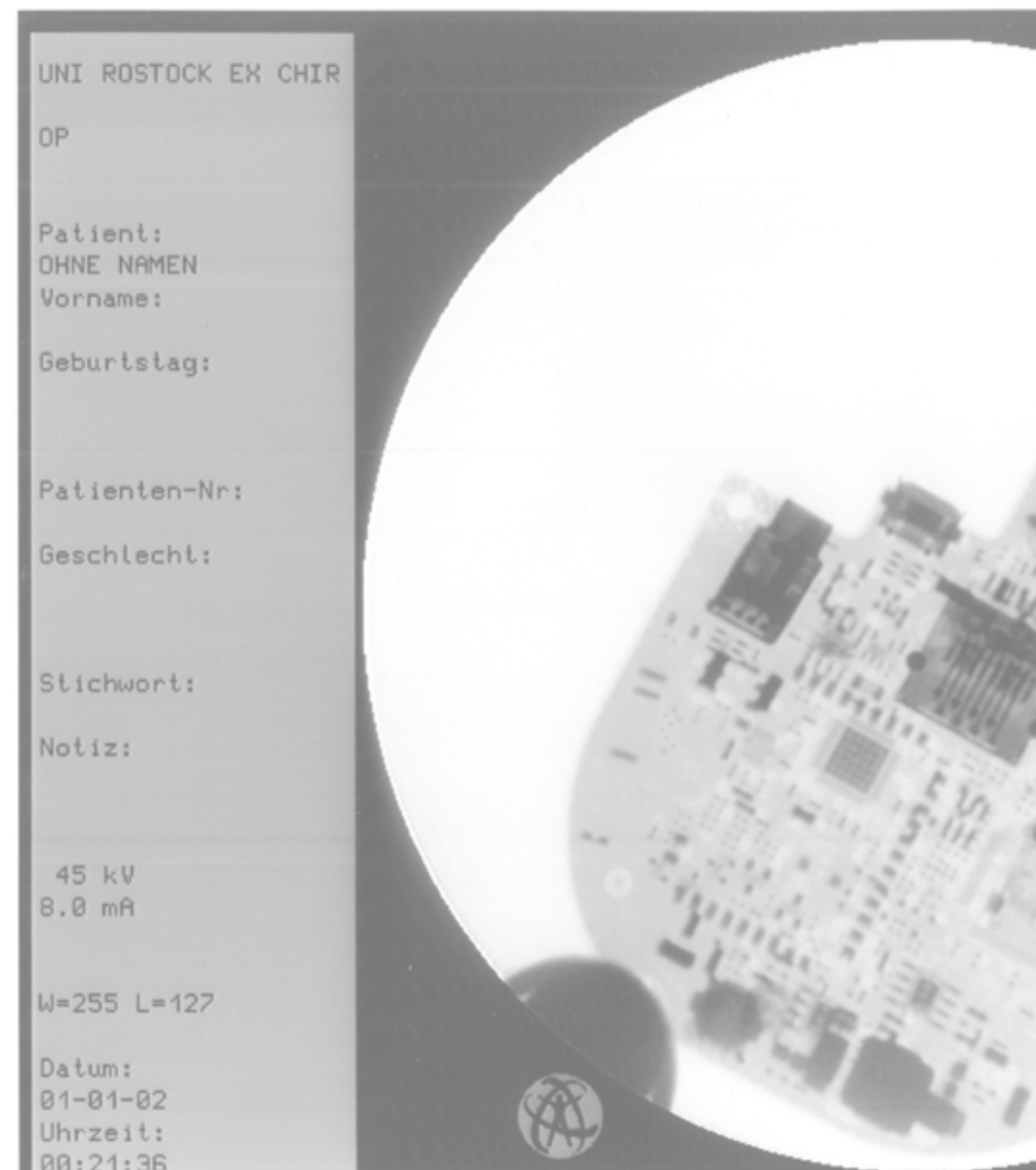


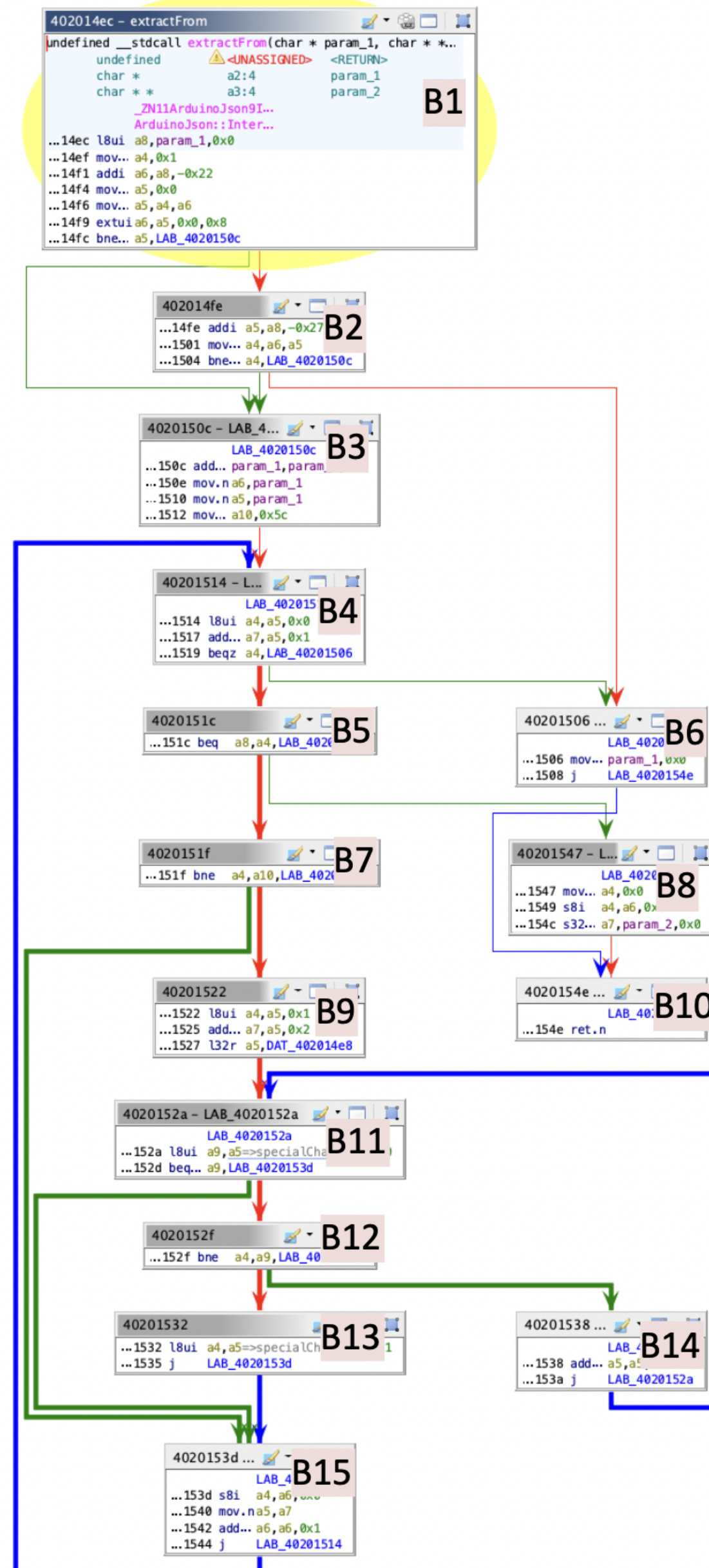


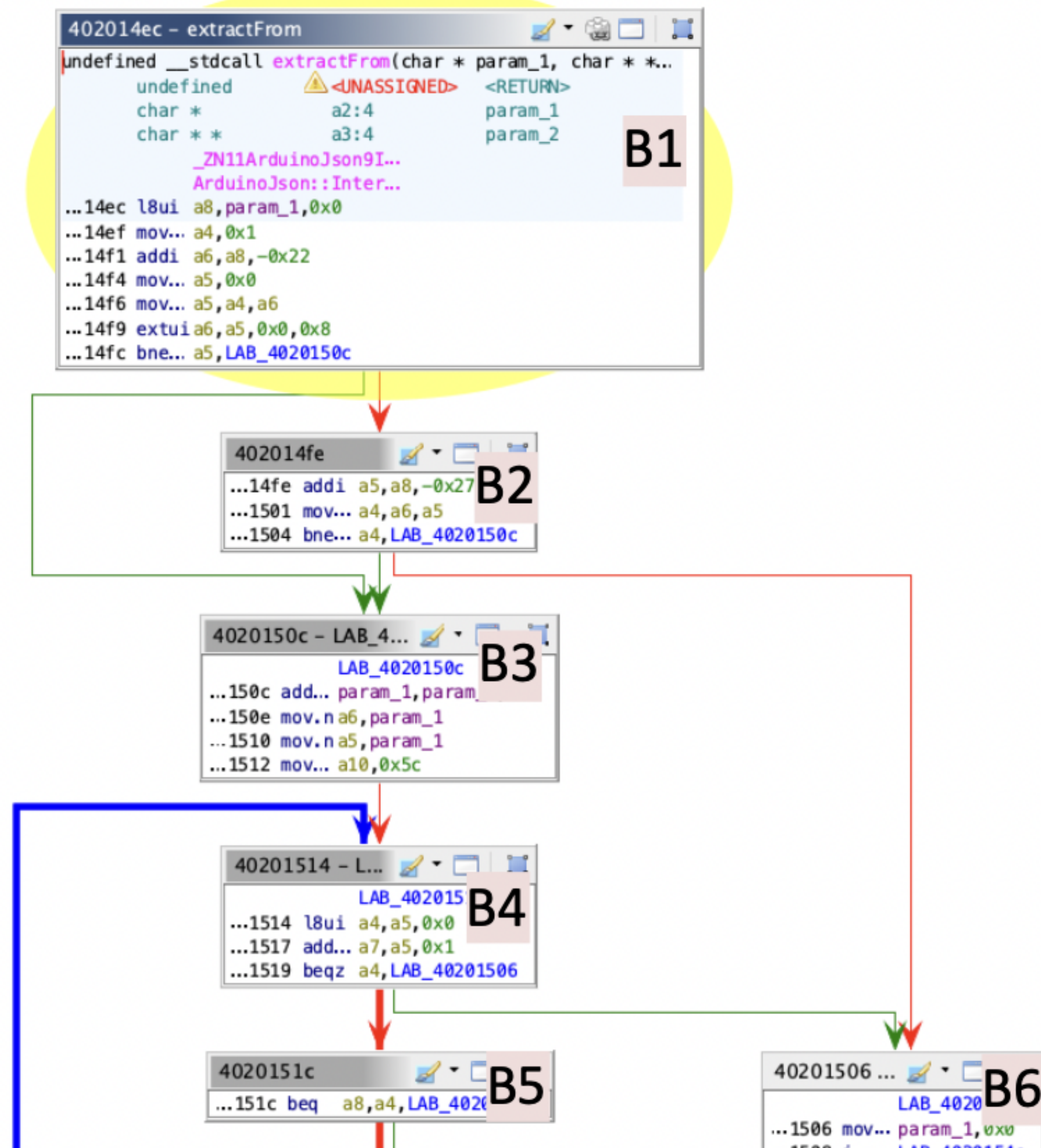












Listing: th_1_aj44firmware.elf
Decompile: extractFrom - (th_1_aj44firmware.elf)

Address	Disassembly	Comment	XREF
		Entry Point(*), setup:0800391e(c)	
08003964 f0 b5	push {r4,r5,r6,r7,lr}		
08003966 06 78	ldrb r6,[param_1,#0x0]		
08003968 22 2e	cmp r6,#0x22		
0800396a 03 d0	beq LAB_08003974		
0800396c 27 2e	cmp r6,#0x27		
0800396e 01 d0	beq LAB_08003974		
08003970 00 20	LAB_08003970 movs param_1,#0x0	XREF[1]: 08003986(j)	
08003972 f0 bd	LAB_08003972 pop {r4,r5,r6,r7,pc}	XREF[1]: 080039b6(j)	
08003974 01 30	LAB_08003974 adds param_1,#0x1	XREF[2]: 0800396a(j), 0800396e(j)	
08003976 df f8 40 c0	ldr.w r12,[DAT_080039b8]	= 08004CA8h	
0800397a 05 46	mov r5,param_1		
0800397c 04 46	mov r4,param_1		
0800397e 22 46	LAB_0800397e mov r2,r4	XREF[1]: 080039aa(j)	
08003980 12 f8 01 3b	ldrb.w r3,[r2],#0x1		
08003984 00 2b	cmp r3,#0x0		
08003986 f3 d0	beq LAB_08003970		
08003988 9e 42	cmp r6,r3		
0800398a 11 d0	beq LAB_080039b0		
0800398c 5c 2b	cmp r3,#0x5c		
0800398e 09 d1	bne LAB_080039a4		
08003990 63 78	ldrb r3,[r4,#0x1]		
08003992 a2 1c	adds r2,r4,#0x2		
08003994 64 46	mov r4,r12		
08003996 27 79	LAB_08003996 ldrb r7,[r4,#0x4]=>DAT_08004cac	XREF[1]: 080039ae(j) = 62h = 66h	
08003998 27 b1	cbz r7,LAB_080039a4		
0800399a bb 42	cmp r3,r7		
0800399c 04 f1 02 0e	add.w lr,r4,#0x2		
080039a0 04 d1	bne LAB_080039ac		
080039a2 63 79	ldrb r3,[r4,#0x5]=>DAT_08004cad	= 08h	
080039a4 05 f8 01 3b	LAB_080039a4 strb.w r3,[r5],#0x1	XREF[2]: 0800398e(j), 08003998(j)	
080039a8 14 46	mov r4,r2		
080039aa e8 e7	b LAB_0800397e		
080039ac 74 46	LAB_080039ac mov r4,lr	XREF[1]: 080039a0(j)	
080039ae f2 e7	b LAB_08003996		
080039b0 00 23	LAB_080039b0 movs r3,#0x0	XREF[1]: 0800398a(j)	
080039b2 2b 70	strb r3,[r5,#0x0]		
080039b4 0a 60	str r2,[param_2,#0x0]		
080039b6 dc e7	b LAB_08003972		

```

1 /* ArduinoJson::Internals::QuotedString::extractFrom(char*, char**) */
2
3 char * ArduinoJson::Internals::QuotedString::extractFrom(char *param_1,char **param_2)
4 {
5     char cVar1;
6     undefined1 *puVar2;
7     char *pcVar3;
8     char *pcVar4;
9     char cVar5;
10    char *pcVar6;
11    undefined1 *puVar7;
12    char *pcVar8;
13
14    cVar1 = *param_1;
15    if ((cVar1 == '\"') || (cVar1 == '\\')) {
16        pcVar3 = param_1 + 1;
17        pcVar6 = pcVar3;
18        pcVar8 = pcVar3;
19        while( true ) {
20            pcVar4 = pcVar6 + 1;
21            cVar5 = *pcVar6;
22            if (cVar5 == '\0') break;
23            if (cVar1 == cVar5) {
24                *pcVar8 = '\0';
25                *param_2 = pcVar4;
26                return pcVar3;
27            }
28            if (cVar5 == '\\') {
29                cVar5 = pcVar6[1];
30                pcVar4 = pcVar6 + 2;
31                puVar2 = &specialChars;
32                do {
33                    puVar7 = puVar2;
34                    if (puVar7[4] == '\0') goto LAB_080039a4;
35                    puVar2 = puVar7 + 2;
36                } while (cVar5 != puVar7[4]);
37                cVar5 = puVar7[5];
38            }
39            pcVar8 = cVar5;
40            pcVar6 = pcVar4;
41            pcVar8 = pcVar8 + 1;
42        }
43    }
44    return (char *)0x0;
45 }
```


ArduinoJson::Internals::QuotedString::extractF...

setup:0800391e(c)

```

08003964 f0 b5      push      {r4,r5,r6,r7,lr}
08003966 06 78      ldrb      r6,[param_1,#0x0]
08003968 22 2e      cmp      r6,#0x22
0800396a 03 d0      beq      LAB_08003974
0800396c 27 2e      cmp      r6,#0x27
0800396e 01 d0      beq      LAB_08003974

```

LAB_08003970

XREF[1]: 08003986(j)

```

08003970 00 20      movs     param_1,#0x0

```

LAB_08003972

XREF[1]: 080039b6(j)

```

08003972 f0 bd      pop      {r4,r5,r6,r7,pc}

```

LAB_08003974

XREF[2]: 0800396a(j), 0800396e(j)

```

08003974 01 30      adds     param_1,#0x1
08003976 df f8 40 c0  ldr.w     r12,[DAT_080039b8]
0800397a 05 46      mov     r5,param_1
0800397c 04 46      mov     r4,param_1

```

= 08004CA8h

LAB_0800397e

XREF[1]: 080039aa(j)

```

0800397e 22 46      mov     r2,r4
08003980 12 f8 01 3b  ldrb.w   r3,[r2],#0x1
08003984 00 2b      cmp     r3,#0x0
08003986 f3 d0      beq     LAB_08003970
08003988 9e 42      cmp     r6,r3
0800398a 11 d0      beq     LAB_080039b0
0800398c 5c 2b      cmp     r3,#0x5c

```


Decompile: extractFrom - (th_1_aj44firmware.elf)

```

1
2 /* ArduinoJson::Internals::QuotedString::extractFrom(char*, char**) */
3
4 char * ArduinoJson::Internals::QuotedString::extractFrom(char *param_1, char **param_2)
5
6 {
7     char cVar1;
8     undefined1 *puVar2;
9     char *pcVar3;
10    char *pcVar4;
11    char cVar5;
12    char *pcVar6;
13    undefined1 *puVar7;
14    char *pcVar8;
15
16    cVar1 = *param_1;
17    if ((cVar1 == '\"') || (cVar1 == '\\')) {
18        pcVar3 = param_1 + 1;
19        pcVar6 = pcVar3;
20        pcVar8 = pcVar3;
21        while( true ) {
22            pcVar4 = pcVar6 + 1;
23            cVar5 = *pcVar6;
24            if (cVar5 == '\\0') break;
25            if (cVar1 == cVar5) {
26                *pcVar8 = '\\0';
27                *param_2 = pcVar4;
28                return pcVar3;
29            }
30            pcVar6 = pcVar4;
31        }
32    }
33    return 0;
34}

```


Password raten

```
bin:*:1:1:bin:/bin:
```

```
...
```

```
gopher:*:13:30:gopher:/usr/lib/gopher-data:
```

```
ftp:*:14:50:FTP User:/var/ftp:
```

```
nobody:*:99:99:Nobody:/:
```

```
apache:*:48:48:Apache Httpd:/var:
```

```
httpd:x:49:49:HTTP Daemon:/home/httpd:/bin/false
```

```
ddc4000:$1$4vcDgPXJ$ZZNI3pboITnWIFULfxTtF0:0:0:ddc4000:/:/bin/sh
```

```
kesroot:$1$91922309$pVILbpE4xZJQpGV97z37a/:0:0:default user:/:/bin/sh
```

```
dcssh:$1$14005813$qLu7Z7VbpxkOoJxBZTmco/:599:550:dcssh:/home/dcssh:/bin/sh
```


Zurückschreiben von Daten

- Ändern von Passwörtern
- Ändern der Software
 - Umgebung von Schutzmechanismen
 - Beheben von Fehlern
- Austausch von kryptografischen Schlüsseln

Password selbst festlegen

```
bin:*:1:1:bin:/bin:
```

```
...
```

```
gopher:*:13:30:gopher:/usr/lib/gopher-data:
```

```
ftp:*:14:50:FTP User:/var/ftp:
```

```
nobody:*:99:99:Nobody:/:
```

```
apache:*:48:48:Apache Httpd:/var:
```

```
httpd:x:49:49:HTTP Daemon:/home/httpd:/bin/false
```

```
ddc4000:$1$XXXX:0:0:ddc4000:/:/bin/sh
```

```
kesroot:$1$XXXX:0:0:default user:/:/bin/sh
```

```
dcssh:$1$14005813$qLu7Z7VbpxkOoJxBZTmco/:599:550:dcssh:/home/dcsssh:/bin/sh
```


**One man's trash
is another man's identity.**



**Dumpster diving
can expose your personal information.**



