RACECAR BRAINS

"BE SCARED BECAUSE I'M A SURGEON NOW"

Stan – Japan Team

(the guy with the TikTok hoodie)

Disclaimer

- This is not really a technical talk (I mean, could be worse) More like a little unfinished story
- "15 minutes is too short lol" -- *Me modifying the slides*

Prologue: in the 90s

- Back in the days...
- Cars were easy to tune
- For ~400$, you get a proper engine retune and limtations removed
- For Hondas, Spoon was one of ze bestests (it's a word)
- Not the cheapest but the most popular aftermarket tuning shop

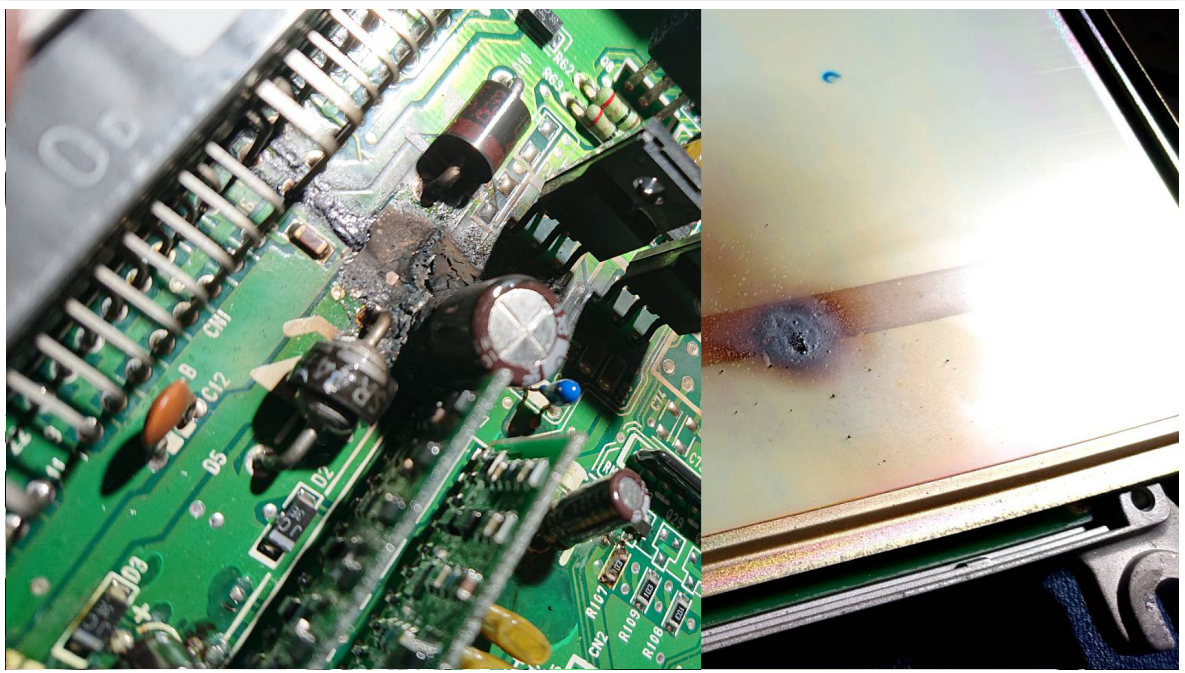
* I (street) race cars in Japan
* Not drifting, mostly time attack with focus on high speed corners
* Had a few cars since arriving there, Hondas grew on me

The protagonist

1989 Honda Civic ("Falken EG6")

The twist

* One day, the Civic started coughing...
  ... a lot.
* Diagnosed it for 3 days before checking the ECU...
  ...which was slowly burning components :)



(pet pet pet)

Repair the ECU... and dump it.

* Handed the ECU over to Tuner-san, ex-Spoon employee
* He repaired it and decided to dump the ROM...
* ... using the same machine he had for years

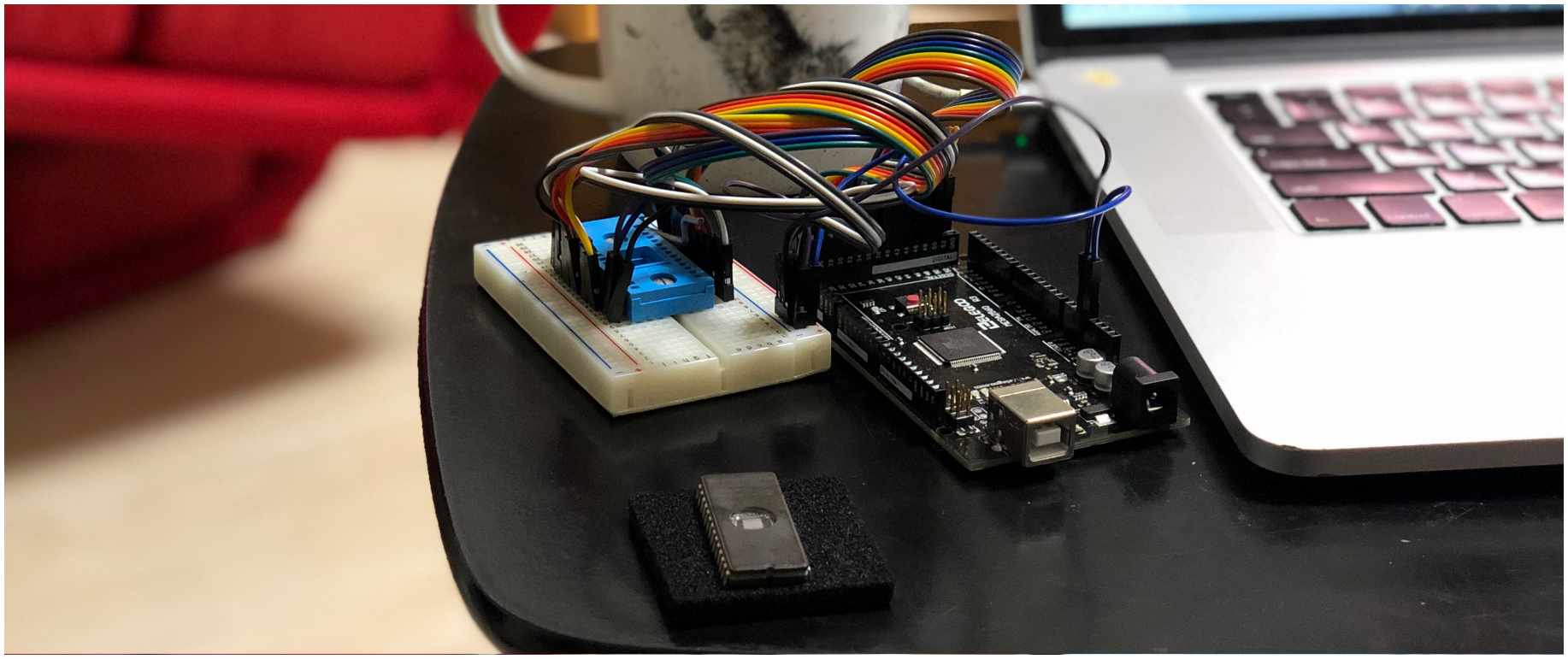
(scratch scratch)

"Stan's ECU"

* 28-pin Dual Inline Package (DIP)
* 32K (256 kilobits)
* EPROM (bit of a pain to work with unless you have the right tools)

But dumping is not too hard

* Connect a lot of wires:
  * 15 address lines (15 bits)
  * 8 data lines
  * 5v + GND
* Can do that with an Arduino and a bit of code, izi



Gotta dump 'em all!

```
p1kachu@nccgroupjp:perso$ la 2021-honda-p30-analysis/dumps/
total 912
-rwxr-xr-x@ 1 p1kachu  192K  _dump-to-file.py
-rwxr-xr-x@ 1 p1kachu  599B  _file-to-dump.py
-rw-r--r--@ 1 p1kachu   32K  fake-spoon-hiro-san.data
-rw-r--r--@ 1 p1kachu   32K  falken-eg6-zero.data
-rw-r--r--@ 1 p1kachu   32K  kouki-tuner-san-spl.data
-rw-r--r--@ 1 p1kachu   32K  kouki-tekunika.data
-rw-r--r--@ 1 p1kachu   32K  pgmfi-stock-p30.data
-rw-r--r--@ 1 p1kachu   32K  spoon-p30000-v6-rev9500-vtec5200.data
-rw-r--r--@ 1 p1kachu   32K  spoon-p30010-v5-rev9000-vtec5800.data
-rw-r--r--@ 1 p1kachu   32K  spoon-p30n01.data
```

(ls output modified for clarity)

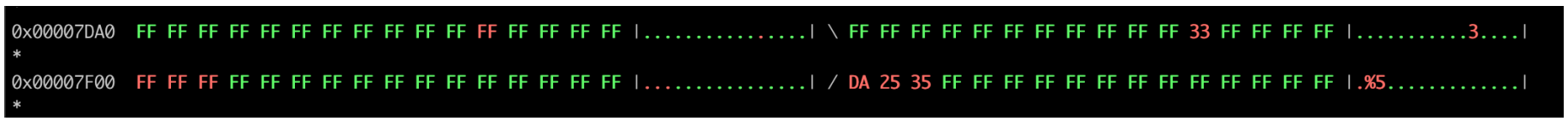
Now let's see what's inside those.

* Lurk around dead 10 years old japanese forums for answers
* Start writing down which bits are different and interesting
* Here, binwalk Stock vs. Spoon

```
p1kachu@tsukiko:dumps$ binwalk -Wi pgmfi-stock-p30.data spoon-p30000-v6-rev9500-vtec5200.data

OFFSET      pgmfi-stock-p30.data                                            spoon-p30000-v6-rev9500-vtec5200.data
--------------------------------------------------------------------------------
*
0x00001830  C0 B9 CD 0A F4 91 CE 0E 77 28 D4 90 CB 0C F4 90 |........w(......| \ C0 FF CD 0A F4 91 CE 0E 77 28 D4 90 CB 0C F4 90 |........w(......|
*
0x00006370  00 00 00 1E 2B E4 00 6F 01 1E 2B E2 00 23 01 1E |....+..o..+..#..| / 00 00 00 1E 2B C8 00 6F 01 1E 2B C8 00 23 01 1E |....+..o..+..#..|
0x00006380  2B E4 00 6F 01 1E 2B E2 00 23 01 33 73 9A 79 00 |+..o..+..#.3s.y.| \ 2B C8 00 6F 01 1E 2B C8 00 23 01 33 73 9A 79 00 |+..o..+..#.3s.y.|
0x00006390  80 66 86 CD 8C CD 8C 33 73 9A 79 00 80 66 86 CD |.f.....3s.y..f..| / 80 66 86 CD 8C CD 8C 33 73 9A 79 D7 83 66 86 CD |.f.....3s.y..f..|
*
0x00006430  29 26 CA CD D5 D8 D6 DA DB DE FF 3F F8 3F F0 3F |)&.........?.?.?| \ 29 26 CA CD D5 D8 C9 CD CE D1 FF 3F F8 3F F0 3F |)&.........?.?.?|
*
0x00006C70  FF FF FF FF 2D 2D FF 2D 2D 06 2D 0F 0F FF FF FF |....--.--.-.....| / FF FF FF FF 2D 2D FF 2D 2D 06 0F 0F 0F FF FF FF |....--.--.......|
*
0x00006CA0  0A 0B 0C 0C 0D 0E 11 00 13 14 15 16 17 18 00 00 |................| \ 0A 0B 0C 0C 0D 0E 11 00 13 14 15 00 17 18 00 00 |................|
*
0x00007030  E4 00 29 7A 96 A3 AA B2 B8 C9 C3 D2 29 7A 96 A3 |..)z........)z..| / E4 00 2D 8A A5 B4 AB B7 AC BD BB CA 2D 8A A5 B4 |..-.........-...|
0x00007040  AA B2 B8 C9 C3 D3 30 7F 99 A6 AC B2 B9 C7 C6 D4 |......0.........| \ AB B7 AC BD BB CA 35 8C A9 B7 AD B7 AD BB BE CB |......5.........|
0x00007050  30 80 99 A7 AC B3 B9 CA C7 D6 30 89 A1 AB B1 B7 |0.........0.....| / 35 8D A9 B8 AD B8 AD BE BF CD 35 8F AB BD B0 BC |5.........5.....|
0x00007060  BD CE C5 D2 42 90 A9 B4 BB BE C3 D2 CC D7 45 96 |....B.........E.| \ B1 C2 C1 CE 48 9B B6 C3 BA C4 B9 CA C7 D3 4C A5 |....H.........L.|
0x00007070  A9 B6 BC C0 C5 D4 CF DD 42 93 A8 B5 BC C3 C8 D8 |........B.......| / BA C5 BD C6 BB CA C8 D5 48 A2 BB CA BD C8 BC CB |........H.......|
0x00007080  CE DD 42 96 AB B8 BF C6 CC DB D4 DF 42 96 AB B9 |..B.........B...| \ C9 D7 48 A5 BE C9 C0 CB BF CE CB DB 48 A5 BB CA |..H.........H...|
0x00007090  C0 C4 CA DA D0 DF 3D 92 A7 B5 BE C3 C9 DA D2 E1 |......=.........| / C2 CD C1 D1 CE E2 43 9E B9 C8 C1 CC C1 D2 CF E2 |......C.........|
0x000070A0  4F A1 BA C6 CE D3 D7 E9 E0 EE 4F A0 B8 C7 CF D4 |O.........O.....| \ 57 AE CB DA D1 DC CD DE DA EB 57 B0 CB DB D2 DD |W.........W.....|
0x000070B0  DA EA E0 ED 53 9A B4 C0 C9 CF D4 E4 E0 ED 46 97 |....S.........F.| / D0 E0 DB E8 5B AD C6 D7 CF DB CC DC DD EE 4D A0 |....[.........M.|
0x000070C0  B3 C0 CA D2 DD ED E2 EB 53 9D B5 C4 CE D4 DA EE |........S.......| \ BC CC C5 D2 CA DA D5 E5 5B A8 C4 D2 CF DB D1 E2 |........[.......|
0x000070D0  E1 EE 64 AC C6 D3 DA E2 E6 F9 EB F6 6C BB D0 DB |..d.........l...| / DE EB 6E BB D5 E3 DC EA DC EF E6 F1 77 D2 E9 F9 |..n.........w...|
```

Speed limiter?



The checksum

* Simple byte addition (rolling at overflow)
* Total sum needs to be 0, else check engine lamp comes up
* Lots of unused bytes at the end, add random values until reaches 0

The Falken EG6's ZERO ECU

* Zero ECU: a bit of a mess:
  * Probably different revision of the same ECU
  * Different shop, a bit more aggressive
  * They don't seem to know exactly what they were doing :p
  * ... or maybe too well.
* Lots of versions for different cars (LOTS)
* Compare with some other firmwares from Tuner-san


p1kachu@tsukiko:dumps$ binwalk -Wi pgmfi-stock-p30.data falken-eg6-zero.data
OFFSET pgmfi-stock-p30.data falken-eg6-zero.data
0x00000030 A1 25 7F 4F 84 4F CE 4F 00 7F 31 00 B5 04 15 57 .%.O.O.O..1....W \ A1 25 7F 4F 84 4F CE 4F 00 00 31 00 B5 04 15 57 .%.O.O.O..1....W
0x000027D0 CB 1E 67 FA 72 C4 31 0B CB DA 77 03 C5 DB C1 CA ..g.r.1...w..... / CB 1E 67 30 07 C4 31 0B CB DA 77 03 C5 DB C1 CA ..g0..1...w.....
0x00003F50 56 F3 21 CE 55 C3 21 98 14 ED 12 06 C5 C1 C0 44 V.!.U.!........D \ 56 F3 21 CE 55 C3 21 98 14 ED 12 06 C5 C1 C0 00 V.!.U.!.........
0x00006000 00 FF FF FF 00 FF FF FF FF 00 00 00 00 00 FF 00 ..... / 00 FF 00 00 00 00 FF 00 00 00 00 00 00 00 FF 00 .....
0x00006010 00 00 00 FF FF FF 00 00 00 00 00 FF 0B 0B 0B 06 ..... \ FF FF 00 FF FF 00 00 00 00 00 00 00 0B 0B 0B 06 .....
0x00006370 00 00 00 1E 2B E4 00 6F 01 1E 2B E2 00 23 01 1E ....+..o..+..#.. / 00 00 00 1E 2B CC 00 6F 01 1E 2B CC 00 23 01 1E ....+..o..+..#..
0x00006380 2B E4 00 6F 01 1E 2B E2 00 23 01 33 73 9A 79 00 +..o..+..#.3s.y. \ 2B CC 00 6F 01 1E 2B CC 00 23 01 00 80 00 80 00 +..o..+..#......
0x00006390 80 66 86 CD 8C CD 8C 33 73 9A 79 00 80 66 86 CD .f.....3s.y..f.. / 80 00 80 00 80 00 80 00 80 00 80 00 80 00 80 00 .....
0x000063A0 8C CD 8C 7C 03 EB 03 5A 04 CA 04 39 05 39 05 D5 ...|...Z...9.9.. \ 80 00 80 7C 03 EB 03 5A 04 CA 04 39 05 39 05 D5 ...|...Z...9.9..
0x000071A0 CB DA D4 E2 7C C6 E6 D2 E2 ED DC EE E7 F4 78 C3 ....|.........x. / CB DA D2 DE 7C C6 E6 D2 E2 ED DC EE DD EA 78 C3 ....|.........x.
0x000071B0 E5 D2 E7 F6 E8 F8 ED F6 7A C4 EB D9 EC F6 E5 F4 ....z....... \ E5 D2 E7 F6 E8 F8 E3 EC 7A C4 EB D9 EC F6 E5 F4 ....z.......
0x000071C0 EA F2 7A C4 EB D9 EC F6 E5 F4 EA F2 01 03 04 06 ..z............. / E0 E8 7A C4 EB D9 EC F6 E5 F4 E0 E8 01 03 04 06 ..z.............
0x00007310 AB 9C 90 87 7D 79 5A 5A 5A 5A 31 1A 0C 00 00 00 ....}yZZZZ1..... \ AB 9C 90 87 7D 79 5A 5A 5A 5A 47 3B 2C 1D 15 11 ....}yZZZZG;,...
0x00007320 5A 5A 5A 5A 39 23 15 06 00 00 6F 6F 6F 6F 5A 40 ZZZZ9#....ooooZ@ / 5A 5A 5A 5A 49 3F 34 24 1C 18 5A 5A 5A 5A 4B 43 ZZZZI?4$..ZZZZKC
0x00007330 2F 23 1B 17 97 97 97 81 6F 60 4C 3E 36 32 A9 A9 /#......o`L>62.. \ 3B 2C 23 1F 5A 5A 5A 5A 4F 47 41 33 2A 26 6F 6F ;,#.ZZZZOGA3*&oo
0x00007340 A9 8C 77 6E 62 55 4B 46 AC AC AC 91 7E 76 6C 62 ..wnbUKF....~vlb / 6F 6F 61 56 4D 41 39 35 8C 8C 8C 7B 69 60 59 4D ooaVMA95...{i`YM
0x00007350 56 52 B3 B3 B3 9B 8A 82 76 69 5C 58 B8 B8 B8 AB VR......vi\X.... \ 46 42 97 97 97 81 6F 68 62 57 50 4C A1 A1 A1 87 FB....ohbWPL....
0x00007360 9D 91 82 74 69 65 C0 C0 C0 B5 A6 99 8A 7C 71 6D ...tie.......|qm / 73 6E 67 5E 55 51 A9 A9 A9 8C 77 71 6B 64 5A 56 sng^UQ....wqkdZV
0x00007370 C2 C2 C2 B7 A8 9B 90 85 7B 77 C2 C2 C2 B8 A9 9C ....{w...... \ AB AB AB 8E 7A 74 6E 68 5E 5A AC AC AC 91 7E 78 ....ztnh^Z....~x
0x00007380 90 87 7D 79 C2 C2 C2 B8 A9 9C 90 87 7D 79 C3 C3 ..}y........}y.. / 72 6C 62 5E B3 B3 B3 9B 8A 83 7C 74 68 64 B5 B5 rlb^......|thd..
0x00007390 C3 B9 AA 9C 90 87 7D 79 C4 C4 C4 BA AB 9C 90 87 ......}y........ \ B5 A2 93 8A 81 78 6D 69 B8 B8 B8 AB 9D 92 89 7F .....xmi........
0x000073A0 7D 79 C4 C4 C4 BA AB 9C 90 87 7D 79 C4 C4 C4 BA }y........}y.... / 75 71 C0 C0 C0 B5 A6 99 8E 85 7D 79 C2 C2 C2 B7 uq........}y....
0x000073B0 AB A2 98 8E 84 81 C4 C4 C4 BA AB A3 99 91 87 83 ..... \ A8 9B 90 87 7D 79 C2 C2 C2 B8 A9 9C 90 87 7D 79 ....}y........}y
0x000073C0 C4 C4 C4 BA AB A0 95 89 7E 7A C4 C4 C4 BA AB A0 ....~z...... / C4 C4 C4 BA AB 9C 90 87 7D 79 C4 C4 C4 BA AB 9C ....}y......
0x000073D0 94 88 7D 79 C4 C4 C4 BA AB A1 98 8C 81 7D 5A 5A ..}y.........}ZZ \ 90 87 7D 79 C4 C4 C4 BA AB 9C 90 87 7D 79 5A 5A ..}y........}yZZ

Modified in the ZERO ECU:
- Base A/F, A/F (high) and Ignition (high) maps
- Rev limiter at 9200 RPM
- Knock sensor disabled
- Oxygen heater sensor disabled
- Oxygen sensor disabled
- Debug mode enabled
- VTEC VSS check disabled

Strange ECU

```
* Speed limiter value hasn't been changed...
* ... even though I *know* it's not there anymore
* Checksum != 0 but no CEL
* Some debug "switches" have been activated here and there
```

Time to reverse

* OKI66207 architecture
* No IDA support at the time
* Old (OLD) project found on dead forums (asm662 lov u)
* Wrote an experimental IDA loader for it
  * kinda works
  * can play with IDA scripting and XREFS somehow
  * easier to mark stuff down in the code directly at least

Issues:
  * Some functions share code and IDA sucks at this
  * "DD flag" changes instruction decoding at runtime (THUMBS)
  * First time writting an IDA disassembler

Anyway, big mess, but workable.

```
0x68a Warning - notify_ana: DD flag changed to avoid ILLEGAL instruction
0x590b Warning - notify_ana: Instruction not found: 102 (0x66)
0x1e80 Warning - notify_ana: DD flag changed to avoid ILLEGAL instruction
0x592f Warning - notify_ana: DD flag changed to avoid ILLEGAL instruction
```

https://github.com/P1kachu/oki-66207-processor

Mystery Nb1: Invalid checksum

```
rom:282A                # ------------------------------------------------------------------------
rom:282A B4 EC 48               mov     ER0, off(0ECh)
rom:282D F9                     clr     A
rom:282E 77 40                  lb      A, 40h
rom:2830 90 35                  mul
rom:2832 50                     mov     X1, A
rom:2833 62 20 00               mov     DP, 20h
rom:2836 C4 EA 48               movb    R0, off(0EAh)
rom:2839
rom:2839                checksum_loop:                          # CODE XREF: rom:2842↓j
rom:2839 90 A8                  lc      A, [X1]
rom:283B C5 07 82 20            adc     A, 0[x2]
rom:283F 81                     dec     X2
rom:2840 70                     inc     X1
rom:2841 70                     inc     X1
rom:2842 30 F5                  jrnz    DP, checksum_loop
rom:2844 78                     lb      A, R0
rom:2845 D4 EA                  stb     A, off(0EAh)
rom:2847 B4 EC 16               inc     off(0ECh)
rom:284A B4 EC C0 00 02         cmp     off(0ECh), 200h
rom:284F CE 16                  jne     loc_2867        # checksum_ok
rom:2851 B4 EC 15               clr     off(0ECh)
rom:2854 78                     lb      A, R0
rom:2855
rom:2855                checksum_jump_instruction:              # checksum_ok
rom:2855 C9 10                  jeq     loc_2867
rom:2857 C4 EA 15               clrb    off(0EAh)
rom:285A 90 9D 11 60            lcb     A, 6011h
rom:285E CE 07                  jne     loc_2867        # checksum_ok
rom:2860 C5 EB 98 48            movb    0EBh, 48h
rom:2864 03 DE 21               jmp     loc_21DE
rom:2867                # ------------------------------------------------------------------------
rom:2867
rom:2867                loc_2867:                               # CODE XREF: rom:284F↑j
rom:2867                                                        # rom:checksum_jump_instruction↑j ...
rom:2867 D8 E4 03               jbr     off(0E4h).0, loc_286D # checksum_ok
rom:286A 03 64 29               jmp     loc_2964
```

```
* 3 conditions to reach `checksum_ok`
  * First one, unclear
  * Second one is actual valid checksum
   -> Replacing jeq by jmp is the go-to way to bypass it
  * Third one bypasses invalid checksum if byte @0x6011 is non-null
```

```
rom:600E FF                                     .byte 0FFh
rom:600F 00                                     .byte    0
rom:6010 FF                     vtec_vss_check: .byte 0FFh
rom:6011 FF                     debug_test_mode:.byte 0FFh
rom:6012 00                     auto_manual_enable:.byte 0
rom:6013 FF                     speed_limiter_setting_for_debug_mode:.
rom:6014 FF                                     .byte 0FFh
rom:6015 00                                     .byte    0
rom:6016 00                                     .byte    0
```

Since the ECU is in debug mode, it ignores the checksum

Mystery Nb2: No speed limiter (unresolved)

```
om:1828 77 C8                   lb      A, #0C8h
om:182A C7 2D                   cmp     A, off(2Dh)
om:182C CD 0A                   jge     maybe_bypass_speed_limiter
om:182E C5 B4 C0 B9             cmpb    0B4h, #0B9h     # Speed limiter value
om:1832
om:1832                 pgmfi_speed_limiter_jump_routine:       # Speed Limiter Jump Routine (Change from jge label_something (CD 0A) to two NOPs (00 00) to disable speed limiter)
om:1832 CD 0A                   jge     speed_limiter
om:1834 F4 91                   lb      A, off(91h)
om:1836 CE 0E                   jne     loc_1846
om:1838
om:1838                 maybe_bypass_speed_limiter:             # CODE XREF: rom:182C↑j
om:1838 77 28                   lb      A, #28h
om:183A D4 90                   stb     A, off(90h)
om:183C CB 0C                   sj      loc_184A
```

* Speed limiter triggered around 185kph with stock value
* Change to 0xff is the easiest way to bypass it
* Still stock on the ZERO ECU though...
* Code hasn't been NOPed out neither

That's it?

* Tried reflashing the EPROM with a "custom" FW to test assumptions
* Put the EPROM the wrong way around: EPROM has left the chat
* Sold the EG6 too so I need to coordinate with my good friend
* "NCCCon 2023: Computer science turning cars into BBQs"

Questions?

Thank you~