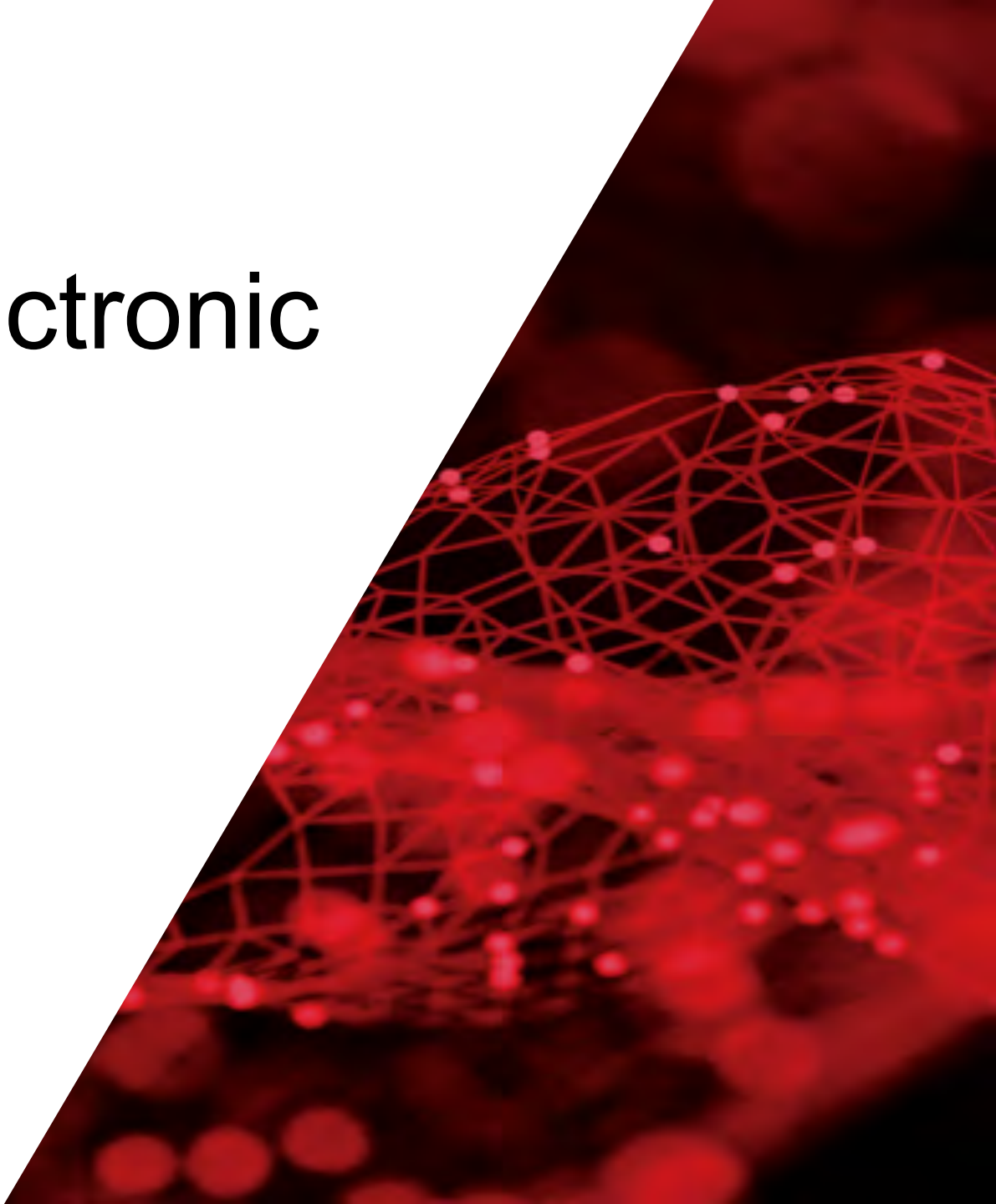
Heavy Trucks and Electronic Logging Devices:

What Could Go Wrong?

Corey Thuen
@CoreyThuen

IOActive®



Talk Overview

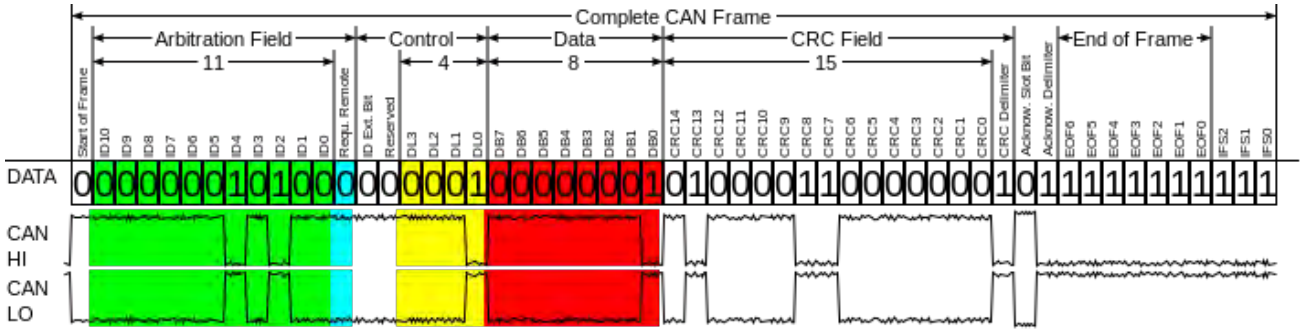
- CAN primer
- Heavy trucking
- ELD analysis
- Cyber truck challenge
- Summary of findings (This work is high level on purpose)

A Very Brief CANBus Primer

Arbitration ID

8 byte (max) payload

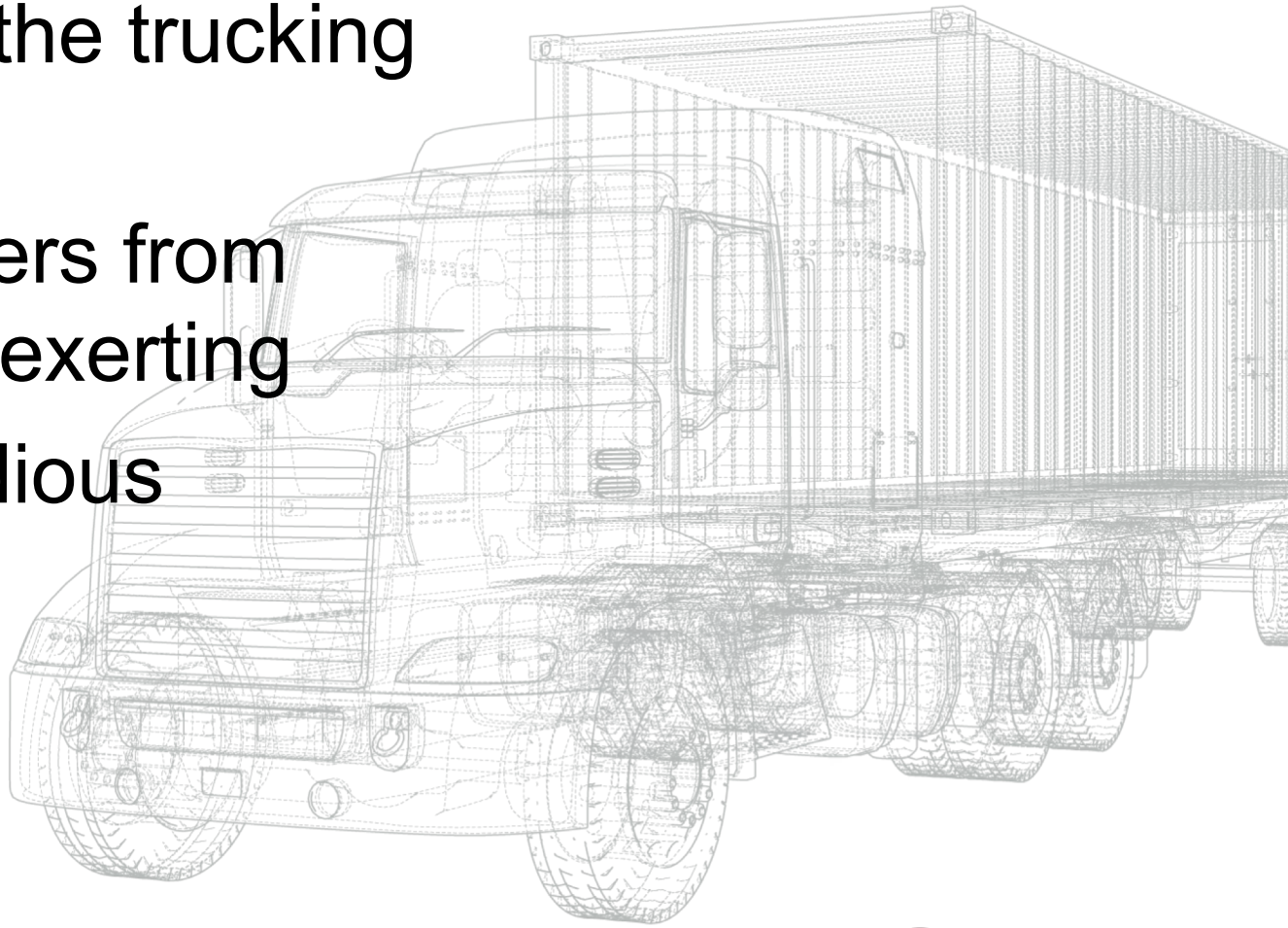
e.g. 0x310#FFFF0102



IOActive

Trucking Overview

- US ***heavily*** depends on the trucking industry
- Regulations prevent drivers from driving too long and overexerting
- Checking logbooks is tedious and they can be falsified



IOActive.


PEOPLE ARE GOING
AROUND OUR REGULATION?
IT'S OK, WE ADDED MORE
imgflip.com

ELD Requirements

- 444 pages of awesome
- Effective December 2017

Insert Quality Assurance Requirements Here

- The identity of the person who performed or led the test
- The outcome of the test (pass/ fail)
- Any comments related to the test

- For each failed test procedure:
  - The identification of all tests that will need to be re-run as a result of the deficiency/defect.

Testing Procedures

1.11 Quality Assurance

Insert the Quality Assurance program here.

1.12 Automated Testing Process

No automated testing will be done as part of the ELD procedures testing.

1.13 ELD Test Procedures

Individual test procedures will be grouped according to requirement type in the following chapters:

- Chapter 1: Accounts, Inputs and Vehicle Interface
- Chapter 2: Processing, Monitoring and Recording
- Chapter 3: Outputs and Data Transfer

Technical Testing Approach

1.14 ELD Procedures Testing Overview

Testing of the ELD procedures will be a step-by-step completion of the test procedures which have been developed to verify the requirements in the RTM.

1.15 Objectives

Testing is to be used to verify conformance of the ELD with the FMCSA requirements.

1.16 Test Items

1.16.1 General

When necessary, Commercial Motor Vehicles (CMVs) will be used for bus interfaces.

IOActive.

Actually, There Is ***Some*** Good in 444 Pages…

_Plan_and_Procedures_10-17-2016_WORD.docx 123 / 444

registration.

(3)ELD Providers will be required to complete a test procedure to ensure their data is properly formatted before they can begin submitting driver's ELD data to the FMCSA server.

(c)ELD data transmission must be accomplished in a way that protects the privacy of the driver(s).

(d)At roadside, if both the vehicle operator and law enforcement have an available data connection, the vehicle operator will initiate the transfer of ELD data to an authorized safety official. In some cases, an ELD may be capable of converting the ELD file to an XML format using an FMCSA-provided schema and upload it using information provided in the WSDL file using SOAP via RFC 7230, RFC 7231, and RFC 5246, Transport Layer Security (TLS) Protocol Version 1.2 (incorporated by reference, see § 395.38).

4.10.1.2 Wireless Data Transfer Through E-Mail

(a) The ELD must attach a file to an email message to be sent using RFC 5321 Simple Mail Transfer Protocol (SMTP) (incorporated by reference, see § 395.38), to a specific email address, which will be shared with the ELD providers during the technology registration process.

(b)The file must have the format described in section 4.8.2.1 of this appendix and must be encrypted using the Secure/Multipurpose Internet Mail Extensions as described in RFC 5751 (incorporated by reference, see § 395.38), and the RSA algorithm as

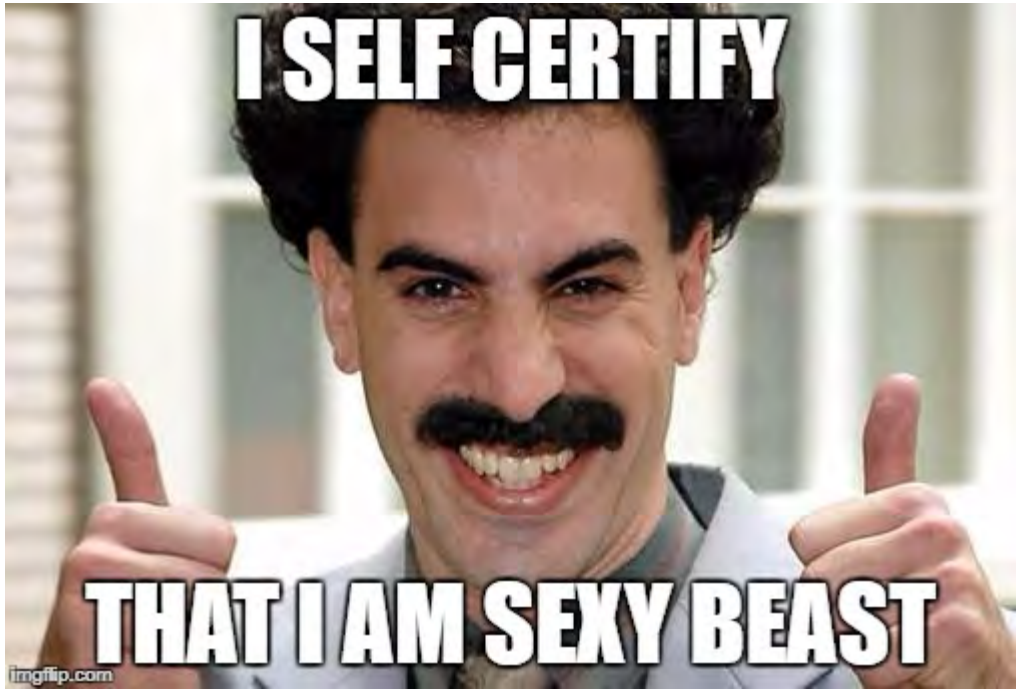
115

IOActive

You Might Say:

“Wow! 444 pages of requirements. That must be really difficult to get qualified. How do I do it?”

Self-Certification!



IOActive.

Over 70 Registered ELDs

United States Department of Transportation

About DOT | Our Act

FMCSA
Federal Motor Carrier Safety Administration

LOGIN |

Registered ELDs

The listed devices are self-certified by the manufacturer. The Federal Motor Carrier Safety Administration does not endorse any electronic logging devices. Click **here** to return to the homepage.

View

Device Name	Model Number	Software Version	ELD Identifier	Image	User Manual	Company	Contact Company (Phone)	Contact Company (Email)	Company Website
TRUXBOX ELD	TTB1.01	4.0.0	TTB1.01	ELD2.png	TruxTrax - Truxbox ELD User manual1.07.pdf	TruxTrax inc	514.704.5879	support@truxtrax.com	https://www.truxtrax.com
E-Log Plus	ELP0100	Build 1.0.1712.7443	ELP0100	Product Image-HOS-Geometris.jpg	E-log Plus HOS User Guide.pdf	E-Log Plus	8778434773	info@e-logplus.com	www.e-logplus.com
HOS247 ELD	FLT2	2.2 and up	ELD247	HOS247_ELD.png	HOS247_ELD_userguide.pdf	HOS247 LLC	415-839-9977	hello@hos247.com	www.hos247.com
ELD Chrome	Cab-Mate Open	4	CMOP01	CabMate Open.jpg	ELD Instruction Booklet.pdf	Pedigree Technologies, LLC	855-838-6941	eld@pedigreetechnologies.com	http://www.eldcertified.com
ELD Chrome	Cab-Mate Connect	4	CMCN01	CabMate Connect.jpg	ELD Instruction Booklet.pdf	Pedigree Technologies, LLC	855-838-6941	eld@pedigreetechnologies.com	http://www.eldcertified.com
ELD Fleet	G3000	1.0.1625.6584	ELDFLT	ELDFLeet.jpg	GPS Trackit ELDFleet User Guide.pdf	Global Tracking Communications, Inc.	877-628-7404	FleetAdvisor@GPSTrackit.net	http://gpstrackit.com/eld-fleet/
ELD Fleet	L4000	1.0.1625.6584	ELDFLT	ELDFLeet.jpg	GPS Trackit ELDFleet User Guide.pdf	Global Tracking Communications, Inc.	877-628-7404	FleetAdvisor@GPSTrackit.net	http://gpstrackit.com/eld-fleet/
ONE20 F-ELD for Android	PT30	1.1 or higher	ONE20A	ONE20_F-ELD_img.png	ONE20_F-ELD_User_Guide_v1.1.pdf	ONE20, Inc.	1-888-986-6320	f-eld@one20.com	www.ONE20.com
HCSSELD	GEO83A	1.0.1702.6723	GEO83A	eLogsSheet.png	HCSS eLogs User Guide.pdf	HCSS	7132704000	sales@hcss.com	www.hcss.com
Qv21 ELD Compliance Module	Qv21ELD	V2.26	TN0262	Qv21_ELD_CM.png	Qv21_ELD_UG.pdf	Qv21 Technologies, Inc.	855-853-7821	Info@qv21.com	www.qv21.com

1 2 3 4 5 6 7 8

IOActive.

Still Under Contention

New bill introduced to house:
H.R. 3282, the ELD Extension Act of 2017

"Many significant technological concerns remain unresolved, including certification of devices, connectivity problems in remote locations, cyber vulnerabilities, and the ability of law enforcement to access data."

ELD Acquisition

- ELDs from three manufacturers
- Consumer off the shelf
- Suppliers chosen at random

Off to a Great Start…

https://app.bigroad.com/mobile-signin-redirector?emailAddress=foo@example.com&password=xaffbm

Hello,

I've invited you to join Foo Company on BigRoad. Please follow the instructions to get started.

Thanks,

Step 1

Download the BigRoad mobile app from:

https://get.bigroad.com

Step 2

Sign into the app by tapping this link on your phone:

https://app.bigroad.com/mobile-signin-redirector?emailAddress=foo@example.com&password=xaffbm

If the link doesn't work, you can sign into the BigRoad app using the following email address and password:

Email address: foo@example.com

Password: xaffbm

Once you're signed in, you can change your password by tapping the menu icon, selecting Settings and then My Profile.

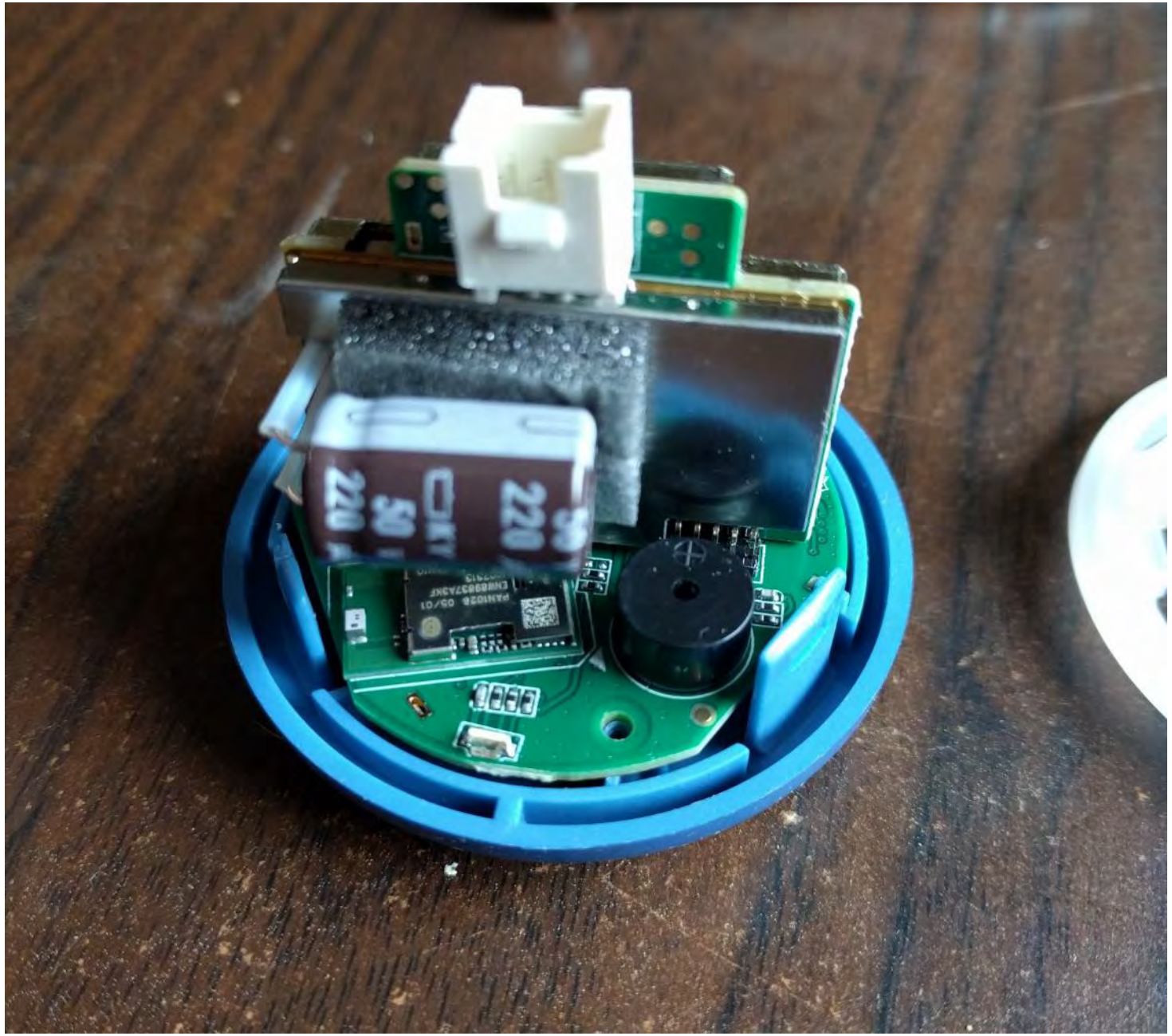
BigRoad THE ESSENTIAL APP FOR DRIVERS & FLEETS

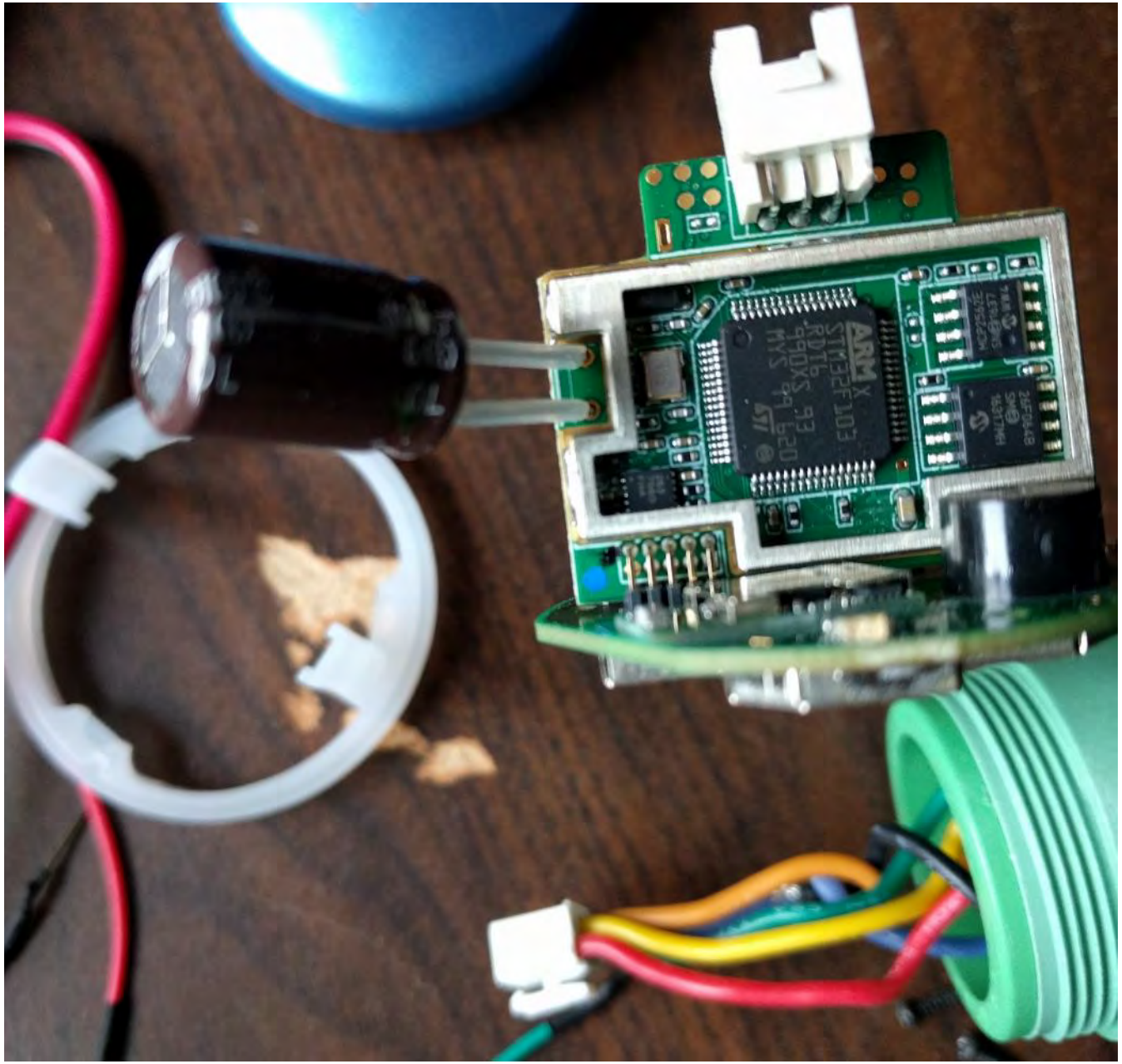
FREE TRIAL FOR FLEET OPERATORS SIGN IN

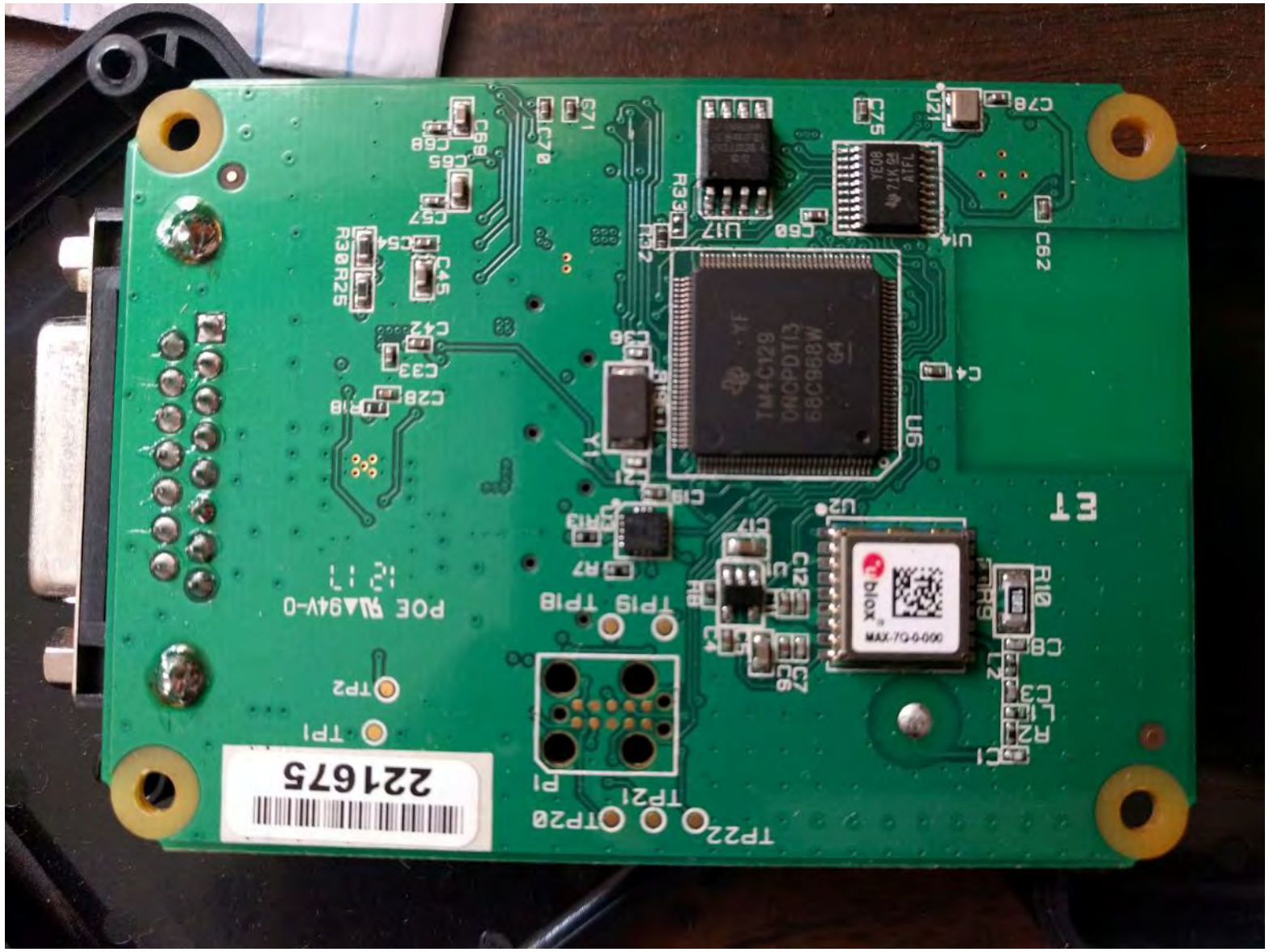
IOActive

Hardware Analysis

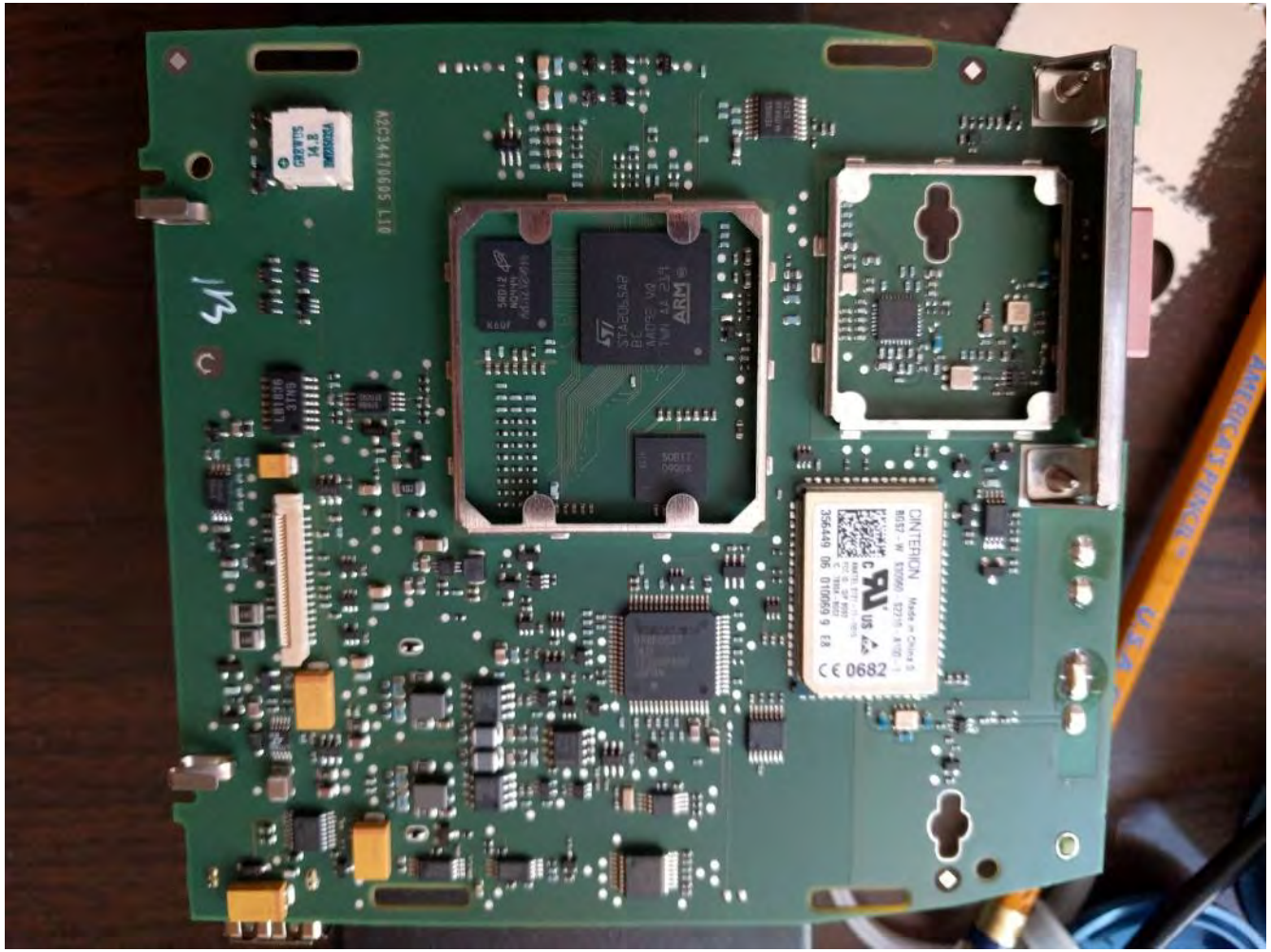
IOActive®

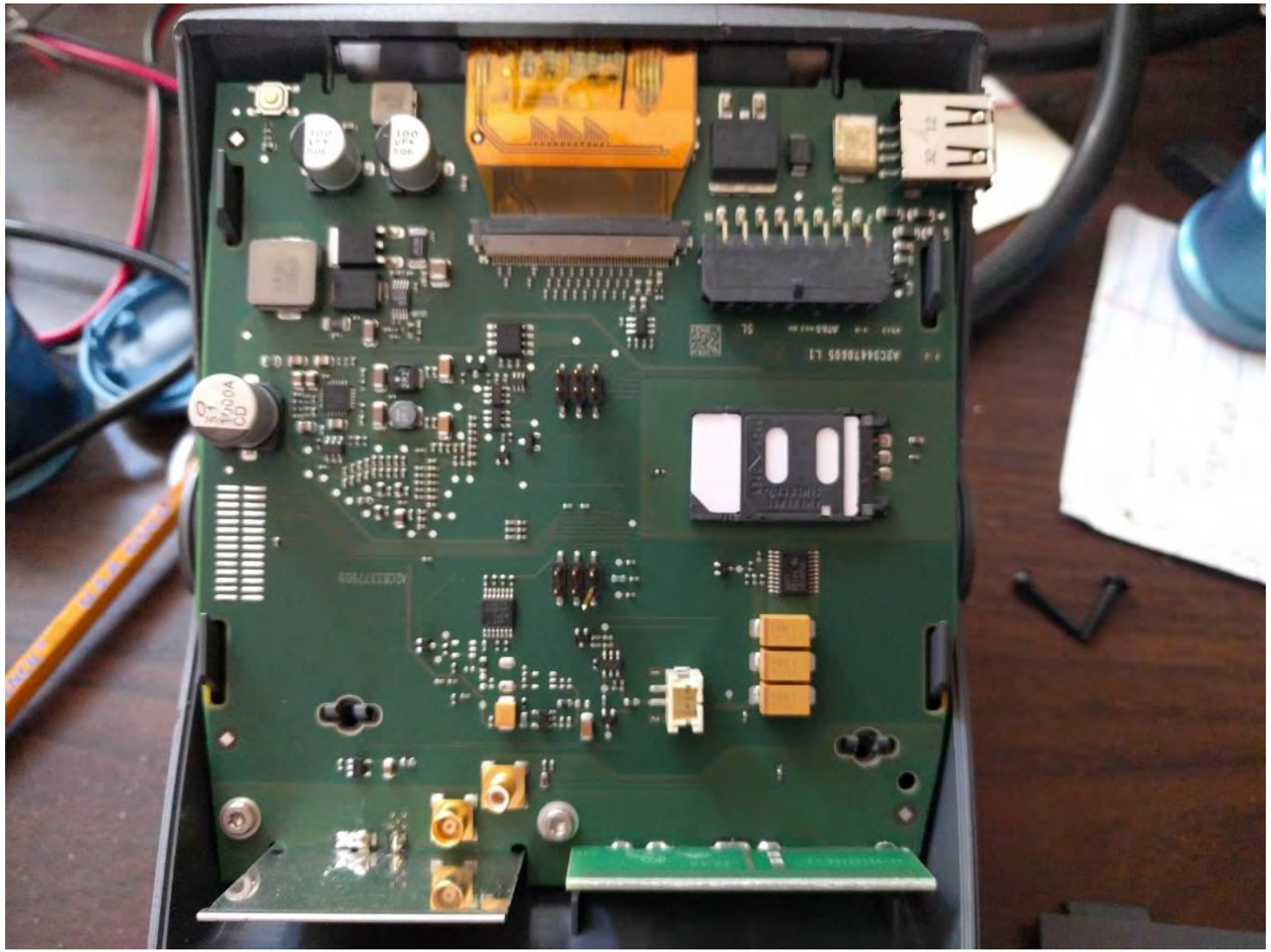



ARM
STM32F103
25FD64B
SMT
MCP2562T
SMT


TP22
TP20
TP21
P1
TP1
TP2
TP19
TP18
221675
POE 94V-0
U6
U7
U4
U2
U1
U3
U5
U20
U19
U18
U17
U16
U15
U14
U13
U12
U11
U10
U9
U8
U7
U6
U5
U4
U3
U2
U1
Y1
Y2
Y3
Y4
Y5
Y6
Y7
Y8
Y9
Y10
Y11
Y12
Y13
Y14
Y15
Y16
Y17
Y18
Y19
Y20
Y21
Y22
Y23
Y24
Y25
Y26
Y27
Y28
Y29
Y30
Y31
Y32
Y33
Y34
Y35
Y36
Y37
Y38
Y39
Y40
Y41
Y42
Y43
Y44
Y45
Y46
Y47
Y48
Y49
Y50
Y51
Y52
Y53
Y54
Y55
Y56
Y57
Y58
Y59
Y60
Y61
Y62
Y63
Y64
Y65
Y66
Y67
Y68
Y69
Y70
Y71
Y72
Y73
Y74
Y75
Y76
Y77
Y78
Y79
Y80
Y81
Y82
Y83
Y84
Y85
Y86
Y87
Y88
Y89
Y90
Y91
Y92
Y93
Y94
Y95
Y96
Y97
Y98
Y99
Y100
Y101
Y102
Y103
Y104
Y105
Y106
Y107
Y108
Y109
Y110
Y111
Y112
Y113
Y114
Y115
Y116
Y117
Y118
Y119
Y120
Y121
Y122
Y123
Y124
Y125
Y126
Y127
Y128
Y129
Y130
Y131
Y132
Y133
Y134
Y135
Y136
Y137
Y138
Y139
Y140
Y141
Y142
Y143
Y144
Y145
Y146
Y147
Y148
Y149
Y150
Y151
Y152
Y153
Y154
Y155
Y156
Y157
Y158
Y159
Y160
Y161
Y162
Y163
Y164
Y165
Y166
Y167
Y168
Y169
Y170
Y171
Y172
Y173
Y174
Y175
Y176
Y177
Y178
Y179
Y180
Y181
Y182
Y183
Y184
Y185
Y186
Y187
Y188
Y189
Y190
Y191
Y192
Y193
Y194
Y195
Y196
Y197
Y198
Y199
Y200
Y201
Y202
Y203
Y204
Y205
Y206
Y207
Y208
Y209
Y210
Y211
Y212
Y213
Y214
Y215
Y216
Y217
Y218
Y219
Y220
Y221
Y222
Y223
Y224
Y225
Y226
Y227
Y228
Y229
Y230
Y231
Y232
Y233
Y234
Y235
Y236
Y237
Y238
Y239
Y240
Y241
Y242
Y243
Y244
Y245
Y246
Y247
Y248
Y249
Y250
Y251
Y252
Y253
Y254
Y255
Y256
Y257
Y258
Y259
Y260
Y261
Y262
Y263
Y264
Y265
Y266
Y267
Y268
Y269
Y270
Y271
Y272
Y273
Y274
Y275
Y276
Y277
Y278
Y279
Y280
Y281
Y282
Y283
Y284
Y285
Y286
Y287
Y288
Y289
Y290
Y291
Y292
Y293
Y294
Y295
Y296
Y297
Y298
Y299
Y300
Y301
Y302
Y303
Y304
Y305
Y306
Y307
Y308
Y309
Y310
Y311
Y312
Y313
Y314
Y315
Y316
Y317
Y318
Y319
Y320
Y321
Y322
Y323
Y324
Y325
Y326
Y327
Y328
Y329
Y330
Y331
Y332
Y333
Y334
Y335
Y336
Y337
Y338
Y339
Y340
Y341
Y342
Y343
Y344
Y345
Y346
Y347
Y348
Y349
Y350
Y351
Y352
Y353
Y354
Y355
Y356
Y357
Y358
Y359
Y360
Y361
Y362
Y363
Y364
Y365
Y366
Y367
Y368
Y369
Y370
Y371
Y372
Y373
Y374
Y375
Y376
Y377
Y378
Y379
Y380
Y381
Y382
Y383
Y384
Y385
Y386
Y387
Y388
Y389
Y390
Y391
Y392
Y393
Y394
Y395
Y396
Y397
Y398
Y399
Y400
Y401
Y402
Y403
Y404
Y405
Y406
Y407
Y408
Y409
Y410
Y411
Y412
Y413
Y414
Y415
Y416
Y417
Y418
Y419
Y420
Y421
Y422
Y423
Y424
Y425
Y426
Y427
Y428
Y429
Y430
Y431
Y432
Y433
Y434
Y435
Y436
Y437
Y438
Y439
Y440
Y441
Y442
Y443
Y444
Y445
Y446
Y447
Y448
Y449
Y450
Y451
Y452
Y453
Y454
Y455
Y456
Y457
Y458
Y459
Y460
Y461
Y462
Y463
Y464
Y465
Y466
Y467
Y468
Y469
Y470
Y471
Y472
Y473
Y474
Y475
Y476
Y477
Y478
Y479
Y480
Y481
Y482
Y483
Y484
Y485
Y486
Y487
Y488
Y489
Y490
Y491
Y492
Y493
Y494
Y495
Y496
Y497
Y498
Y499
Y500
Y501
Y502
Y503
Y504
Y505
Y506
Y507
Y508
Y509
Y510
Y511
Y512
Y513
Y514
Y515
Y516
Y517
Y518
Y519
Y520
Y521
Y522
Y523
Y524
Y525
Y526
Y527
Y528
Y529
Y530
Y531
Y532
Y533
Y534
Y535
Y536
Y537
Y538
Y539
Y540
Y541
Y542
Y543
Y544
Y545
Y546
Y547
Y548
Y549
Y550
Y551
Y552
Y553
Y554
Y555
Y556
Y557
Y558
Y559
Y560
Y561
Y562
Y563
Y564
Y565
Y566
Y567
Y568
Y569
Y570
Y571
Y572
Y573
Y574
Y575
Y576
Y577
Y578
Y579
Y580
Y581
Y582
Y583
Y584
Y585
Y586
Y587
Y588
Y589
Y590
Y591
Y592
Y593
Y594
Y595
Y596
Y597
Y598
Y599
Y600
Y601
Y602
Y603
Y604
Y605
Y606
Y607
Y608
Y609
Y610
Y611
Y612
Y613
Y614
Y615
Y616
Y617
Y618
Y619
Y620
Y621
Y622
Y623
Y624
Y625
Y626
Y627
Y628
Y629
Y630
Y631
Y632
Y633
Y634
Y635
Y636
Y637
Y638
Y639
Y640
Y641
Y642
Y643
Y644
Y645
Y646
Y647
Y648
Y649
Y650
Y651
Y652
Y653
Y654
Y655
Y656
Y657
Y658
Y659
Y660
Y661
Y662
Y663
Y664
Y665
Y666
Y667
Y668
Y669
Y670
Y671
Y672
Y673
Y674
Y675
Y676
Y677
Y678
Y679
Y680
Y681
Y682
Y683
Y684
Y685
Y686
Y687
Y688
Y689
Y690
Y691
Y692
Y693
Y694
Y695
Y696
Y697
Y698
Y699
Y700
Y701
Y702
Y703
Y704
Y705
Y706
Y707
Y708
Y709
Y710
Y711
Y712
Y713
Y714
Y715
Y716
Y717
Y718
Y719
Y720
Y721
Y722
Y723
Y724
Y725
Y726
Y727
Y728
Y729
Y730
Y731
Y732
Y733
Y734
Y735
Y736
Y737
Y738
Y739
Y740
Y741
Y742
Y743
Y744
Y745
Y746
Y747
Y748
Y749
Y750
Y751
Y752
Y753
Y754
Y755
Y756
Y757
Y758
Y759
Y760
Y761
Y762
Y763
Y764
Y765
Y766
Y767
Y768
Y769
Y770
Y771
Y772
Y773
Y774
Y775
Y776
Y777
Y778
Y779
Y780
Y781
Y782
Y783
Y784
Y785
Y786
Y787
Y788
Y789
Y790
Y791
Y792
Y793
Y794
Y795
Y796
Y797
Y798
Y799
Y800
Y801
Y802
Y803
Y804
Y805
Y806
Y807
Y808
Y809
Y810
Y811
Y812
Y813
Y814
Y815
Y816
Y817
Y818
Y819
Y820
Y821
Y822
Y823
Y824
Y825
Y826
Y827
Y828
Y829
Y830
Y831
Y832
Y833
Y834
Y835
Y836
Y837
Y838
Y839
Y840
Y841
Y842
Y843
Y844
Y845
Y846
Y847
Y848
Y849
Y850
Y851
Y852
Y853
Y854
Y855
Y856
Y857
Y858
Y859
Y860
Y861
Y862
Y863
Y864
Y865
Y866
Y867
Y868
Y869
Y870
Y871
Y872
Y873
Y874
Y875
Y876
Y877
Y878
Y879
Y880
Y881
Y882
Y883
Y884
Y885
Y886
Y887
Y888
Y889
Y890
Y891
Y892
Y893
Y894
Y895
Y896
Y897
Y898
Y899
Y900
Y901
Y902
Y903
Y904
Y905
Y906
Y907
Y908
Y909
Y910
Y911
Y912
Y913
Y914
Y915
Y916
Y917
Y918
Y919
Y920
Y921
Y922
Y923
Y924
Y925
Y926
Y927
Y928
Y929
Y930
Y931
Y932
Y933
Y934
Y935
Y936
Y937
Y938
Y939
Y940
Y941
Y942
Y943
Y944
Y945
Y946
Y947
Y948
Y949
Y950
Y951
Y952
Y953
Y954
Y955
Y956
Y957
Y958
Y959
Y960
Y961
Y962
Y963
Y964
Y965
Y966
Y967
Y968
Y969
Y970
Y971
Y972
Y973
Y974
Y975
Y976
Y977
Y978
Y979
Y980
Y981
Y982
Y983
Y984
Y985
Y986
Y987
Y988
Y989
Y990
Y991
Y992
Y993
Y994
Y995
Y996
Y997
Y998
Y999
Y1000


taoglas
CGGP.25.4.A.02
A28LF-1862-2.1
MADE IN CANADA
Turbo v2.1
©2017
BigRoad Inc.


A2C34170605 L10
CINTERION
CE 0682



Software Analysis

IOActive®

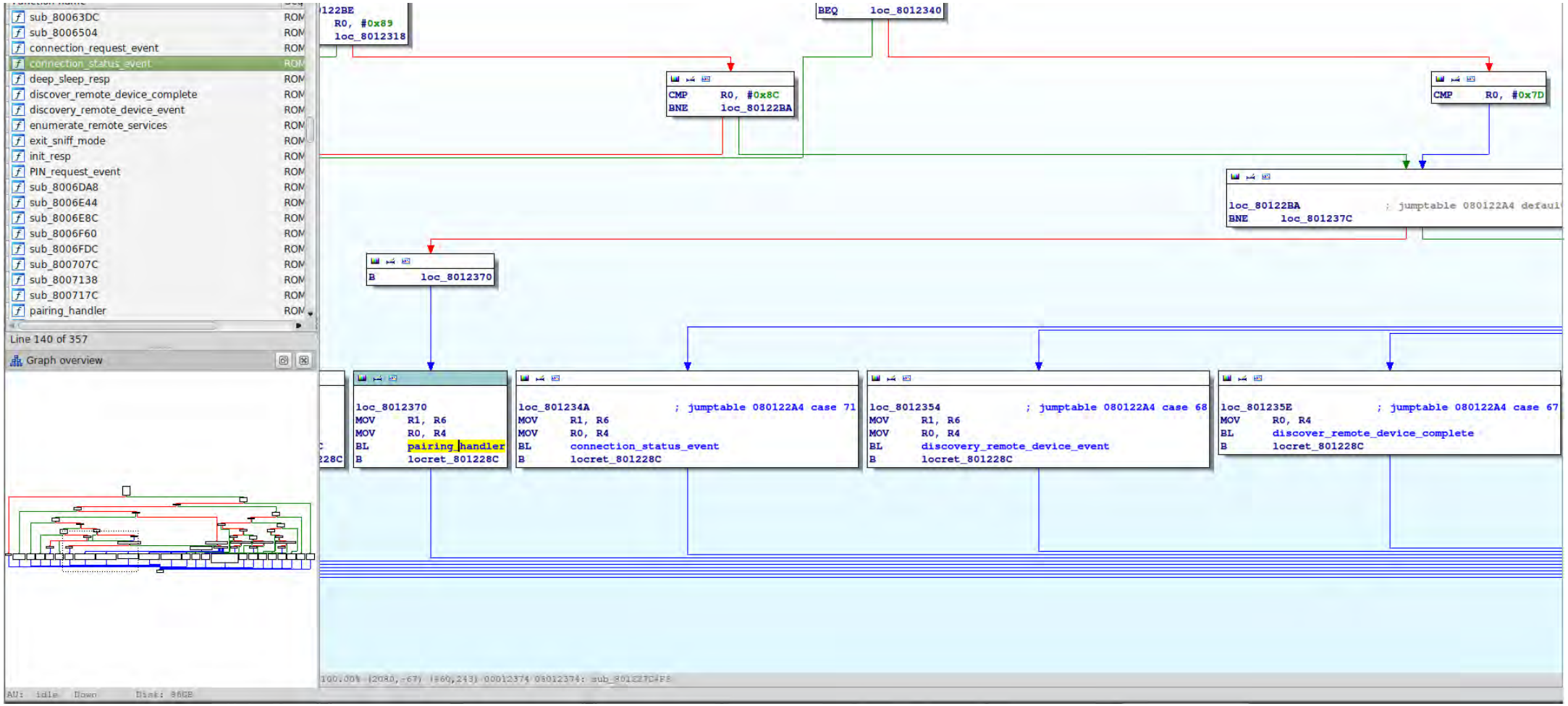
Software Analysis - Firmware

```
Terminal
Playing HOS Buffering (Long) Tone...
Playing HOS Buffer Near Full Tone...
Playing HOS Buffer Full Tone...
Playing Bluetooth Connect Tone...
Playing Bluetooth Disconnect Tone...
Invalid Command!
Buzzer Off
Buzzer Commands:
        z?      This screen
        zf      Set buzzer frequency (Hz)  (e.g: zf440)
        zh0     Play HOS Buffering Tone
        zh1     Play HOS Buffering (Long) Tone
        zh2     Play HOS Buffer Near Full Tone
        zh3     Play HOS Buffer Full Tone
        zh4     Play Bluetooth Connect Tone
        zh5     Play Bluetooth Disconnect Tone
        zp0     Buzzer off
        zp1     Buzzer on
J1939 Reset Off
J1939 Reset On
Invalid Command!
INDEX   PGN     SPN
---------------------
J1939 Bus Test:
J1939 Commands:
        c?      This screen
        cr0     J1939 Reset Line Off
        cr1     J1939 Reset Line On
        co      Output J1939 Data
        cf      Display J1939 Allowed PIDs
        ct      Perform J1939 Bus Test
 J1939: xQueueReceive() #0 failed
J1939 Length too short! len = %u
J1939: Failed to get byte %i of %i
Ayaq!H!I        x
 hci_receive_response() failed
parse_hci_m2_xet_event() failed
unexpected command 0x%02x
unexpected information_id 0x%02x
unexpected command_result 0x%02x
Total Tasks Running: %u
Total Run Time: %u
%s      %u      %u      %c      %u      %u              %u%%
%s      %u      %u      %c      %u      %u              <1%%
Clear record table.
Ticks == 0!
h@i 0&I hHa$H
 Record Data is empty!
record checksum mismatch! rec.crc8=%02X, crc=%02X
Record Data is now empty!
address = %u, crc8 = %02X, temp_rec.crc8 = %02X
data_read_record_table
pApp->record_table_head         = %u
pApp->record_table_sequence     = %u
pApp->record_data_start_address = %u
pApp->record_data_next_address  = %u
pApp->record_count              = %u
:
```

```
Terminal
FInitializing odometer at %d
Fwrite %x(%d)
Fverify failed @%x
/var/lib/jenkins/jobs/TurboFirmware_Release_14/workspace/src/firmware/turbo/common/flash.c
flash id failed
mfgId: %x deviceId: %x
Detected %s
Not detected
FInit complete
(addr % flashGetSectorSize()) == 0
_receiveEvent
_requestMailbox
Short packet
 pGTransport Error: %d for PID 0x%x
FFF too large: %d
FFF response failed
SF dropped
CF message dropped
CF overflow
CF seq: got %d expected %d
ppGgot fix
FUsing Simulated GPS Source
Simulated time set %u
Error: sim message bad sig
Error: sim message size (%d)
FTime set %d/%d/%d %d:%02d:%02d %d
NAV-PVT short
Resetting GPS Source to UART
Can't create HWI
../sensor.c
hpGaccel int0
No accel detected
FLIS3DH detected
LIS331DLH detected
I2C bus fault
FInit complete
FWrite failed: %d
FErase failed: %d
FEEPROM size
/var/lib/jenkins/jobs/TurboFirmware_Release_14/workspace/src/firmware/turbo/common/nvram.c
blockLength: %d; dataLength: %d
Offset: %d
No valid data
EEPROMInit failed
FNo valid data; erasing...
sizeof(NvData_t) % eepromBlockSize == 0
Init complete
Init complete
Reset Request Throttled
Reset Requested
Unhandled message 0x%x
Sending loopback %d
Message response failed: %d
Bad id 0x%x
Bad length
out of buffers
../j1708.c
:
```


IOActive

Software Analysis - RE



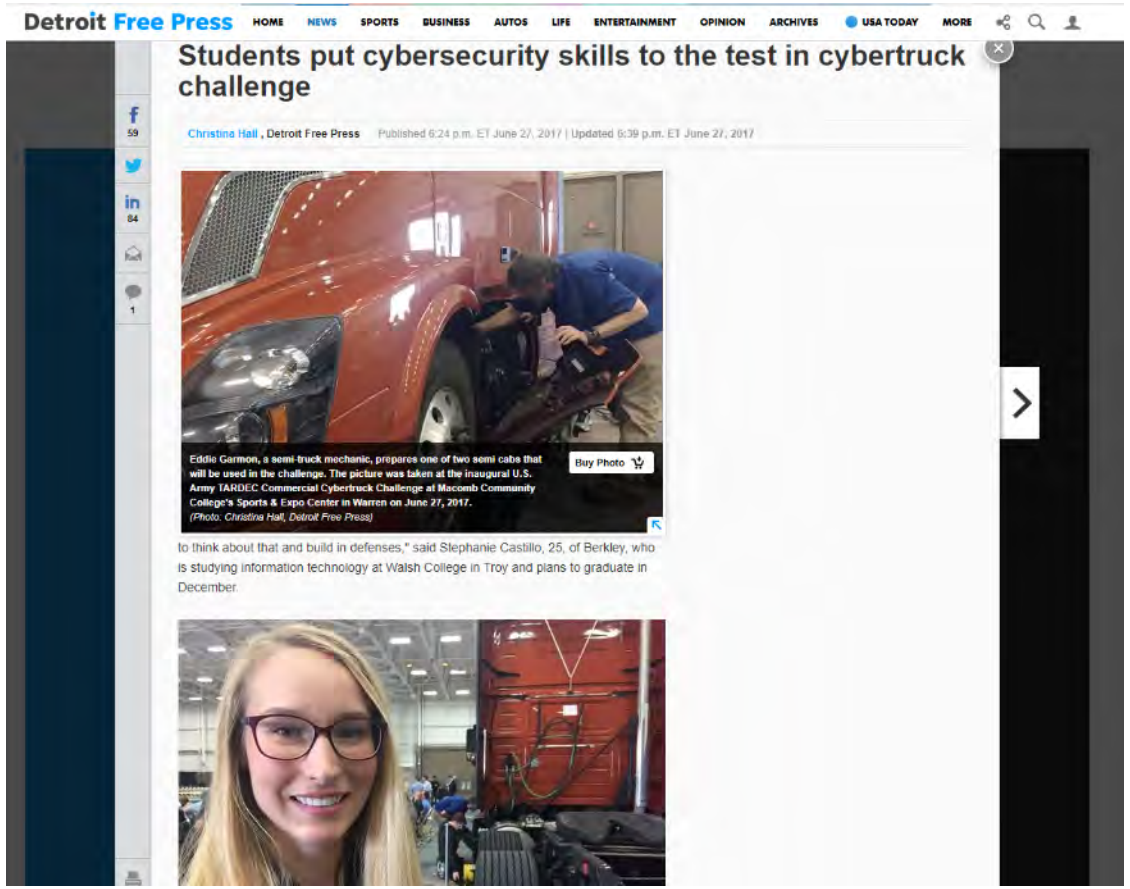
IOActive

Don’t Just Take My Word For It

IOActive®

Cybertruck Challenge

- Students from multiple universities and community colleges
- 2 days class, 2 days hands-on
- No previous exposure or experience



Detroit Free Press HOME NEWS SPORTS BUSINESS AUTOS LIFE ENTERTAINMENT OPINION ARCHIVES USA TODAY MORE

Students put cybersecurity skills to the test in cybertruck challenge

Christina Hall , Detroit Free Press Published 6:24 p.m. ET June 27, 2017 | Updated 6:39 p.m. ET June 27, 2017

Eddie Garmon, a semi-truck mechanic, prepares one of two semi cabs that will be used in the challenge. The picture was taken at the inaugural U.S. Army TARDEC Commercial Cybertruck Challenge at Macomb Community College's Sports & Expo Center in Warren on June 27, 2017. (Photo: Christina Hall, Detroit Free Press)

Buy Photo

to think about that and build in defenses," said Stephanie Castillo, 25, of Berkley, who is studying information technology at Walsh College in Troy and plans to graduate in December.

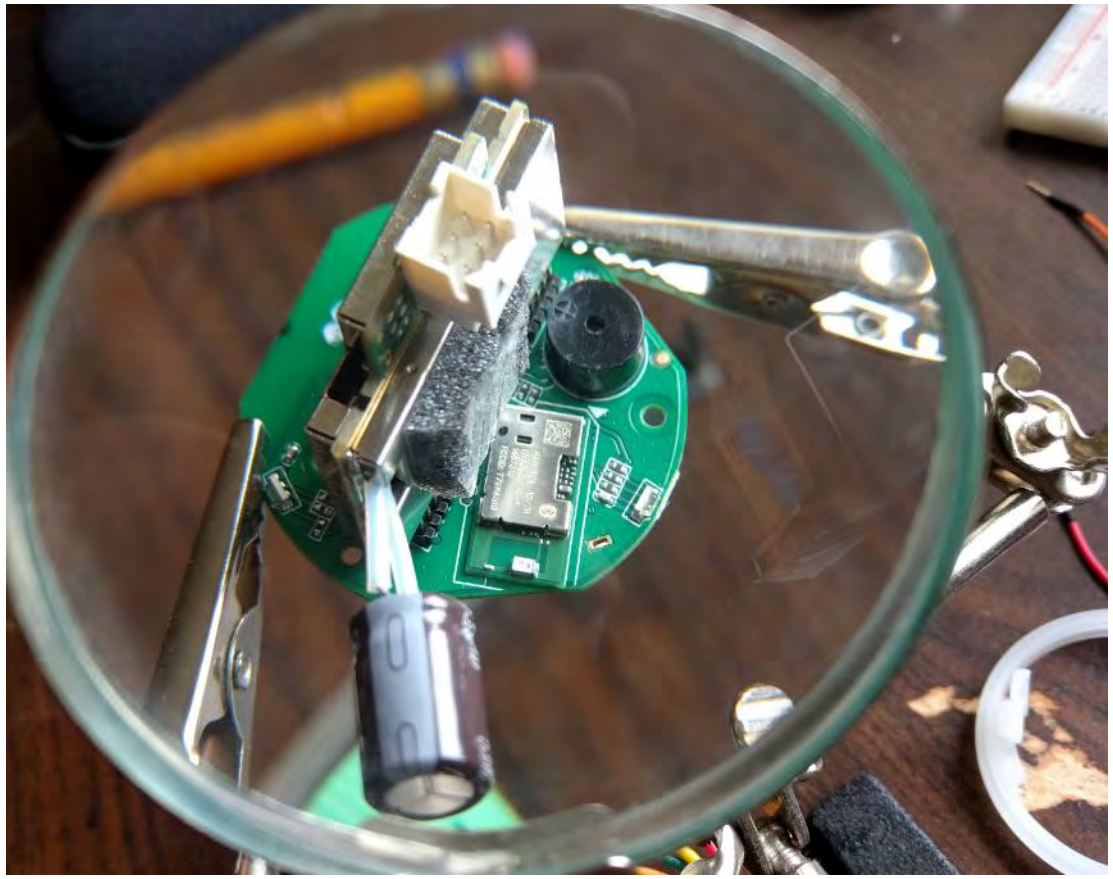
IOActive.

Student Results

- Extracted firmware over SWD
- Identified lack of encryption
- Basic Dynamic analysis with GDB

Student opinion of device security:

Low to non-existent



IOActive

Conclusions

IOActive®

Security Overview

- Devices shipped with debug enabled
- Firmware easily accessible for analysis
  - Development strings present
  - Use of banned functions
- Lack of secureboot
- Lack of encryption for communications

Basically a general failure to follow cybersecurity best practices

Potential Impact

- Heavy Trucking is critical infrastructure
- What happens if the device is locally vulnerable?
- What happens if the device is remotely vulnerable?
- What about backend infrastructure?

Potential Impact

- Daniel Suarez – “The Daemon” is not that far out there
- A problem in Denver can affect trucks on the East coast
- ELDs are arguably easier to spoof than logbooks

Someday This Will Be Me

IOActive IOAsis at Black Hat Flashcard

- Electronic Logging Devices that replace driver logbooks are mandated by US Government
- These devices are heavily commoditized and fail to follow almost all cybersecurity best practices
- The impact to US critical infrastructure is real and remote connectivity without cybersecurity considerations is a threat

Heavy Trucks and Electronic Logging Devices: What Could Go Wrong?

Corey Thuen

@CoreyThuen

IOActive