RUHR UNIVERSITÄT BOCHUM RUB

hgi SysSec

Automotive Defeat Devices

HackPra

January 24, 2018

Moritz Contag

@dwuid
https://dwuid.com

$ whoami

RUHR UNIVERSITÄT BOCHUM RUB

hgi SysSec

- **2011** – B. Sc. and M. Sc. at RUB
- IT Security/Information Engineering

- **2015** – PhD Candidate
- Chair for Systems Security
- Prof. Thorsten Holz

$ whoarewe

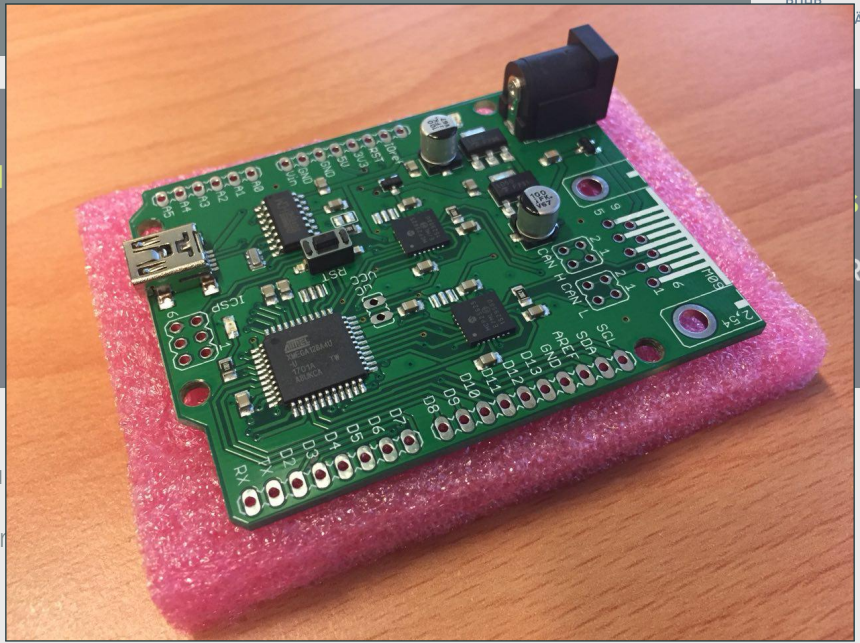
RUHR UNIVERSITÄT BOCHUM RUB

- Capture-the-Flag team at RUB
- Annual **hack.lu** CTF (since 2010)
- Hack with us!

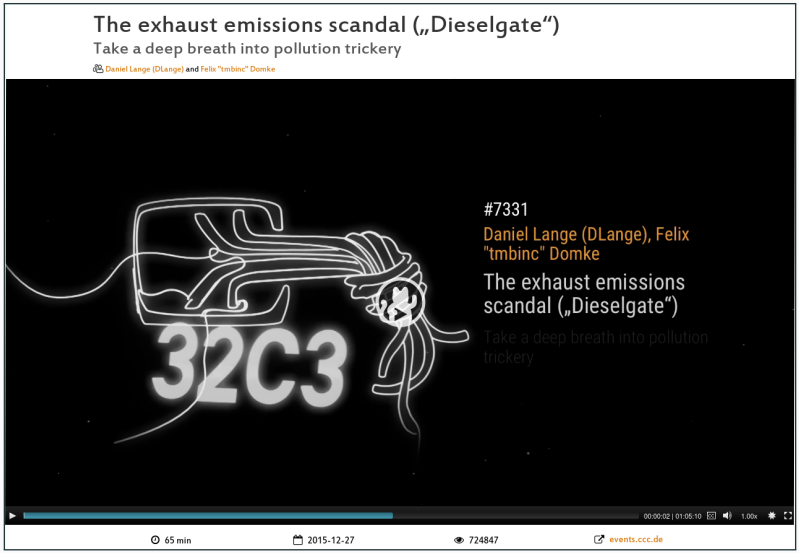
https://fluxfingers.net/contact

CTF meets Automotive Security

- Capture-the-Flag competition
- Riscure and Argus Cyber Security
- Automotive focus
- Hardware-based



- Captu
- Riscur


The exhaust emissions scandal („Dieselgate“)
Take a deep breath into pollution trickery
Daniel Lange (DLange) and Felix "tmbinc" Domke
32C3
#7331
Daniel Lange (DLange), Felix "tmbinc" Domke
The exhaust emissions scandal („Dieselgate“)
Take a deep breath into pollution trickery
00:00:02 | 01:05:10
1.00x
65 min
2015-12-27
724847
events.ccc.de

How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles

Moritz Contag*, Guo Li†, Andre Pawlowski*, Felix Domke‡,
Kirill Levchenko†, Thorsten Holz*, and Stefan Savage†

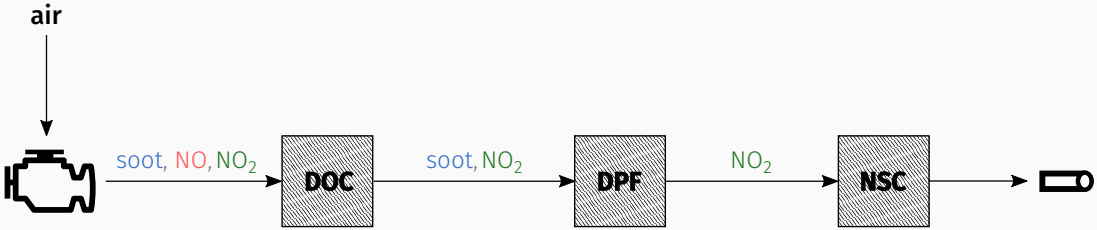
* Ruhr-Universität Bochum, Germany, {moritz.contag, andre.pawlowski, thorsten.holz}@rub.de
† University of California, San Diego, {gul027, klevchen, savage}@cs.ucsd.edu
‡ tmbinc@elitedvb.net

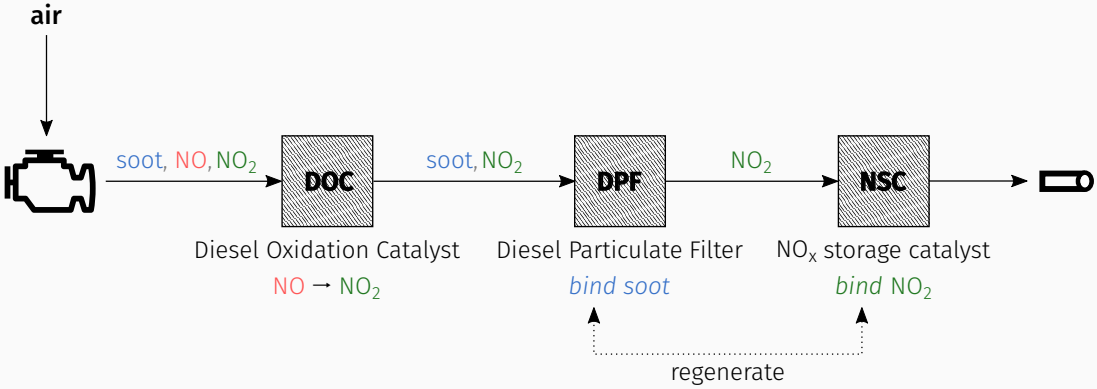
***Abstract*—Modern vehicles are required to comply with a range of environmental regulations limiting the level of emissions for various greenhouse gases, toxins and particulate matter. To ensure compliance, regulators test vehicles in controlled settings and empirically measure their emissions at the tailpipe. However, the black box nature of this testing and the standardization of its forms have created an opportunity for evasion. Using modern electronic engine controllers, manufacturers can programmatically infer when a car is undergoing an emission test and alter the behavior of the vehicle to comply with emission standards, while exceeding them during normal driving in favor of improved performance. While the use of such a defeat device**

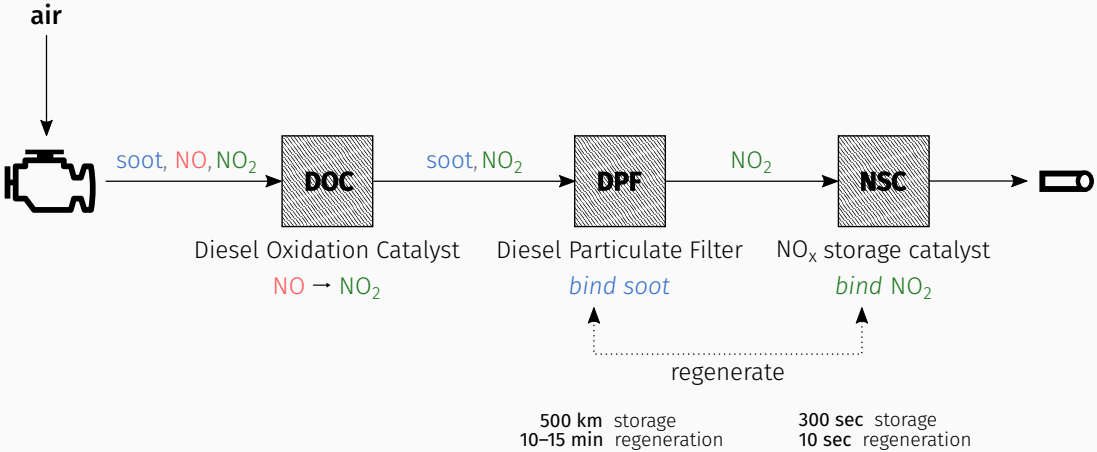
determined that the vehicle was not under test, it would disable certain emission control measures, in some cases leading the vehicle to emit up to 40 times the allowed nitrogen oxides [15].

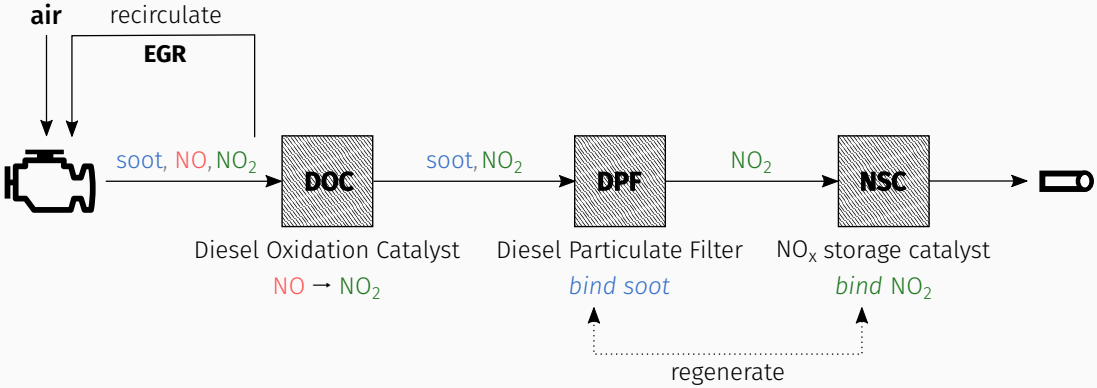
Defeat devices like Volkswagen's are possible because of how regulatory agencies test vehicles for compliance before they can be offered for sale. In most jurisdictions, including the US and Europe, emissions tests are performed on a chassis dynamometer, a fixture that holds the vehicle in place while allowing its tires to rotate freely. During the test, a vehicle is made to follow a precisely defined speed profile (i.e.,

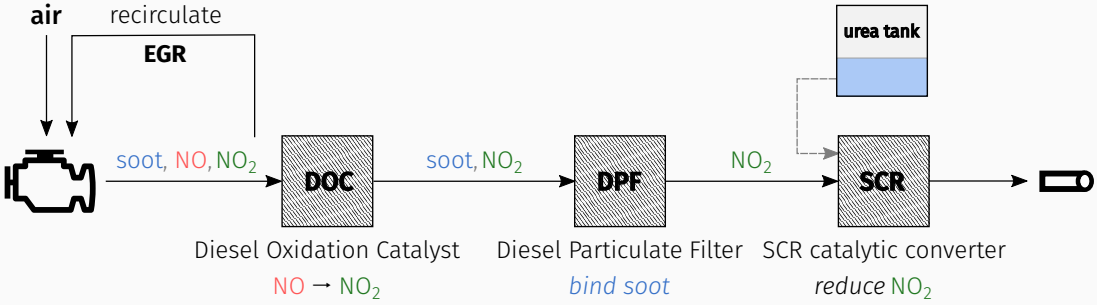
Exhaust Aftertreatment Systems

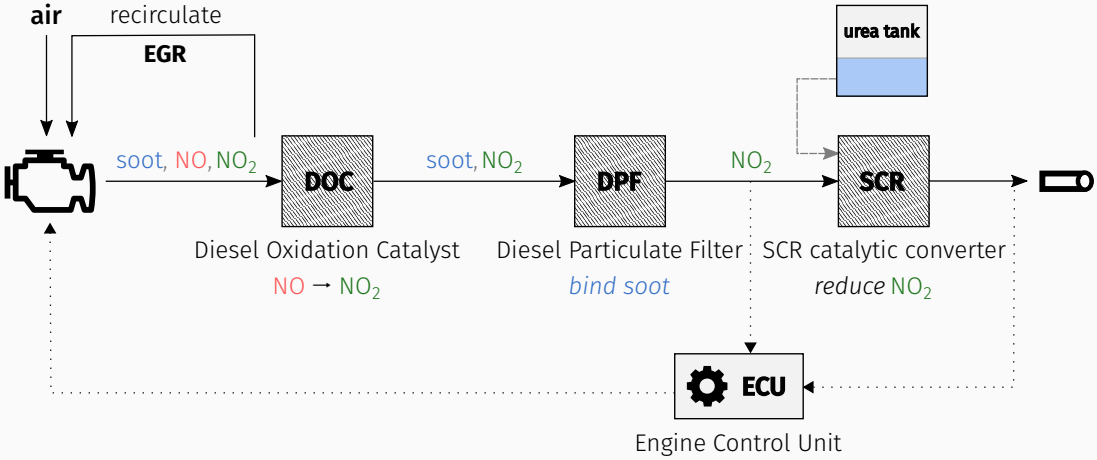

air
soot, NO, NO2
DOC
soot, NO2
DPF
NO2
NSC
Diesel Oxidation Catalyst
NO → NO2
Diesel Particulate Filter
bind soot
NOx storage catalyst
bind NO2

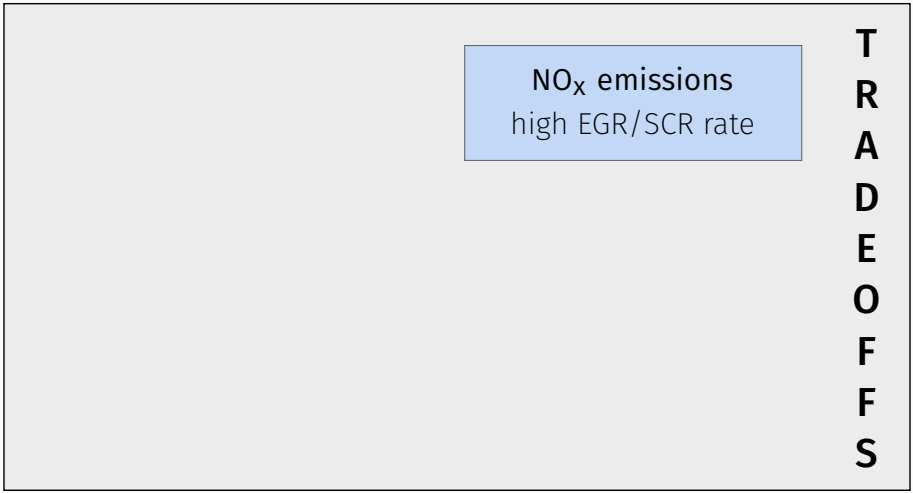

air
soot, NO, NO2
DOC
soot, NO2
DPF
NO2
NSC
Diesel Oxidation Catalyst
NO → NO2
Diesel Particulate Filter
bind soot
NOx storage catalyst
bind NO2
regenerate

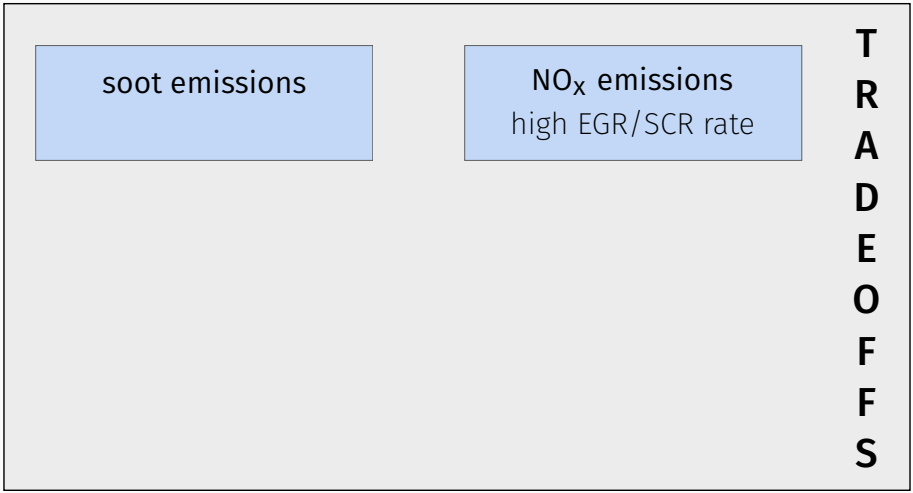

air
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
NSC
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
NO_x storage catalyst
bind NO_2
regenerate
500 km storage
10–15 min regeneration
300 sec storage
10 sec regeneration

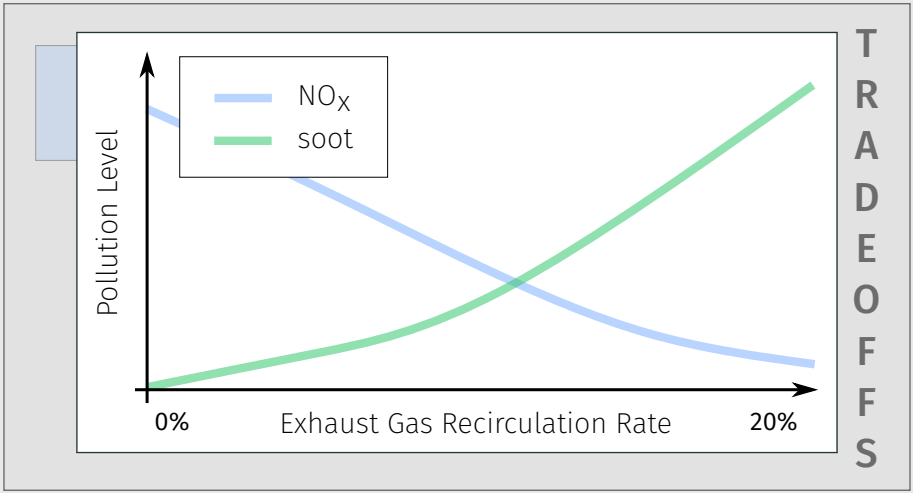

air
recirculate
EGR
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
NSC
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
NO_x storage catalyst
bind NO_2
regenerate

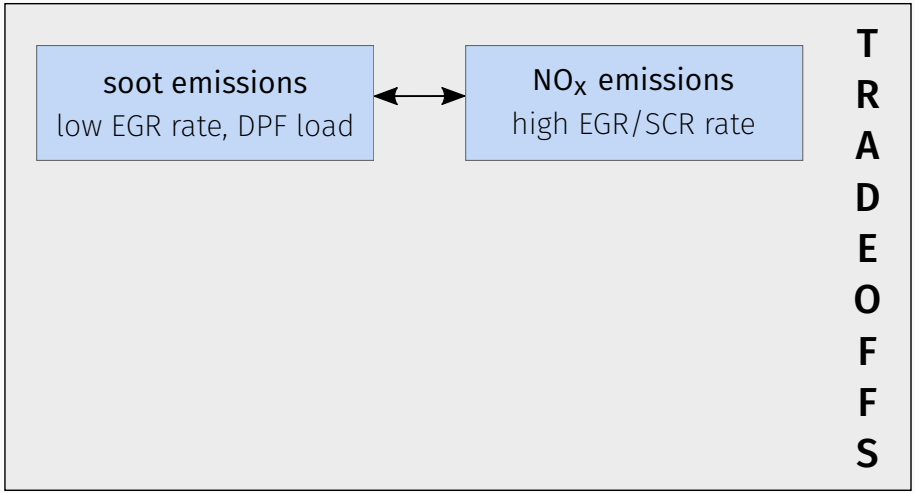

air
recirculate
EGR
urea tank
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
SCR
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
SCR catalytic converter
reduce NO_2

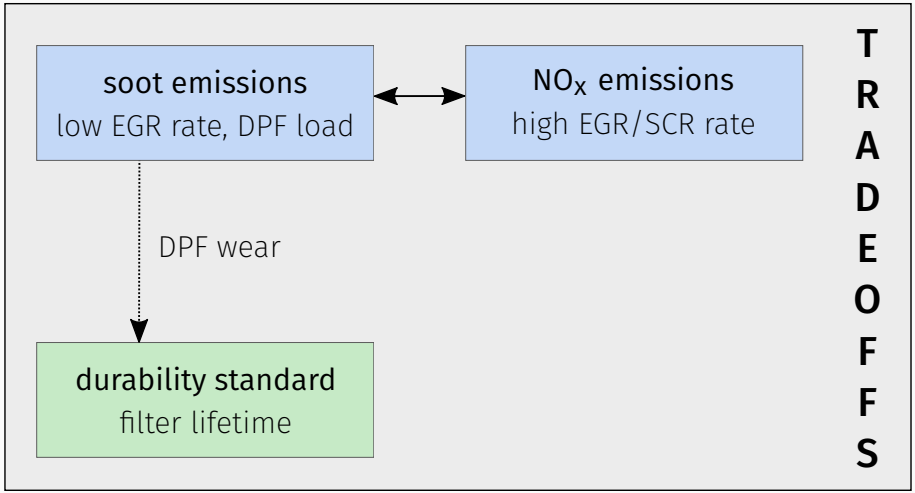

air
recirculate
EGR
urea tank
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
SCR
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
SCR catalytic converter
reduce NO_2
ECU
Engine Control Unit

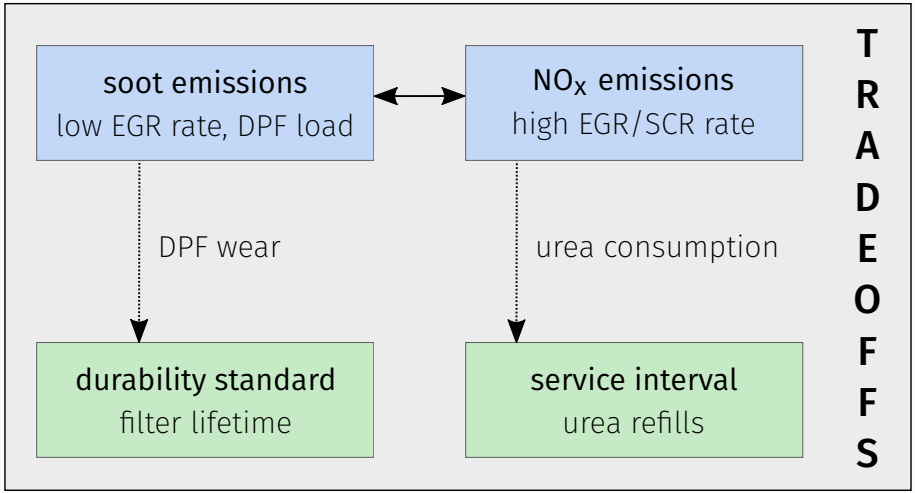

NO_X emissions
high EGR/SCR rate
TRADEOFFS


soot emissions
NO_X emissions
high EGR/SCR rate
TRADEOFFS

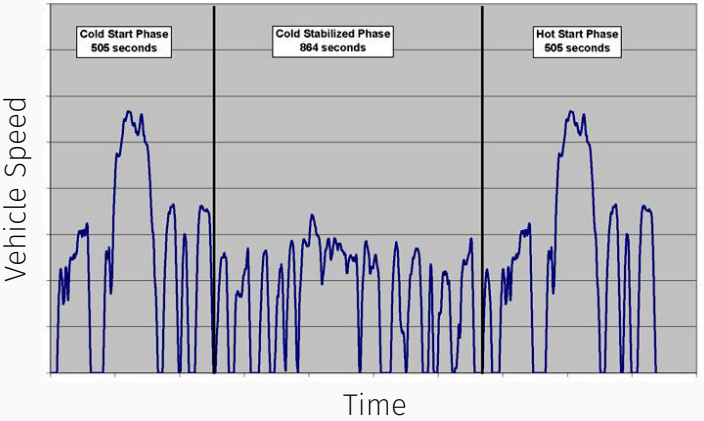

NOX
soot
Pollution Level
0%
Exhaust Gas Recirculation Rate
20%
TRADEOFFS


soot emissions
low EGR rate, DPF load
NOx emissions
high EGR/SCR rate
TRADEOFFS

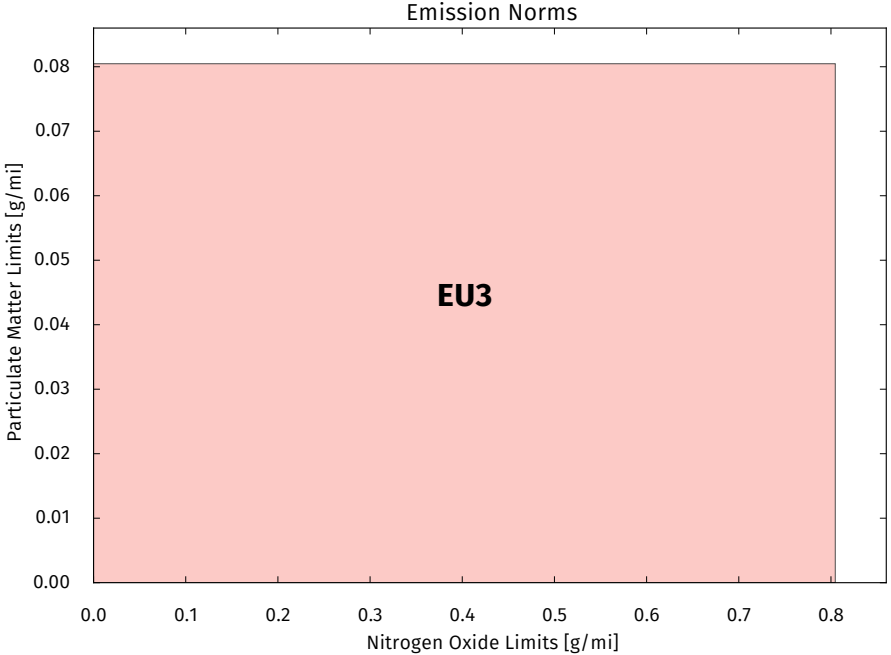

soot emissions
low EGR rate, DPF load
NOx emissions
high EGR/SCR rate
DPF wear
durability standard
filter lifetime
TRADEOFFS

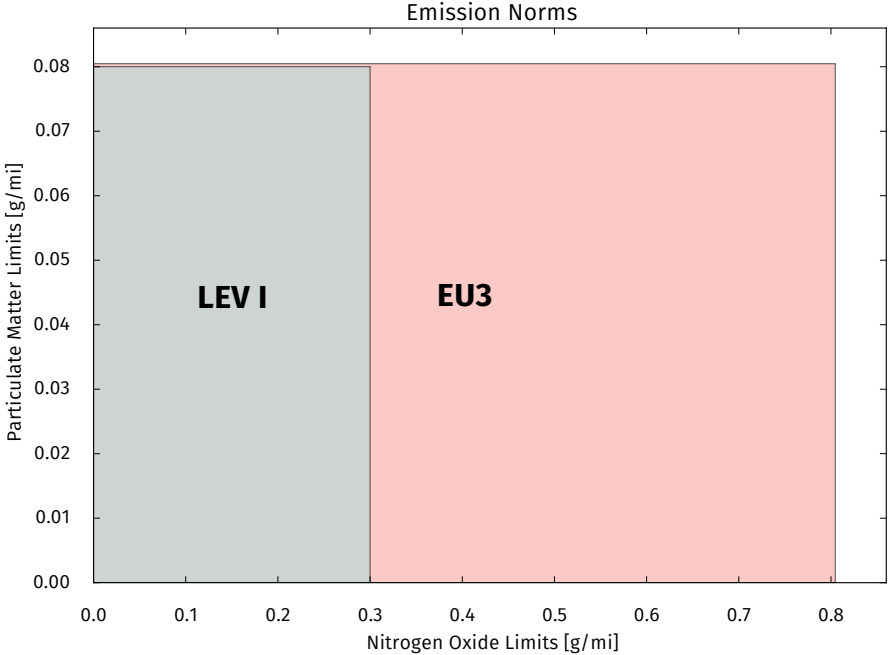

soot emissions
low EGR rate, DPF load
NOx emissions
high EGR/SCR rate
DPF wear
urea consumption
durability standard
filter lifetime
service interval
urea refills
TRADEOFFS

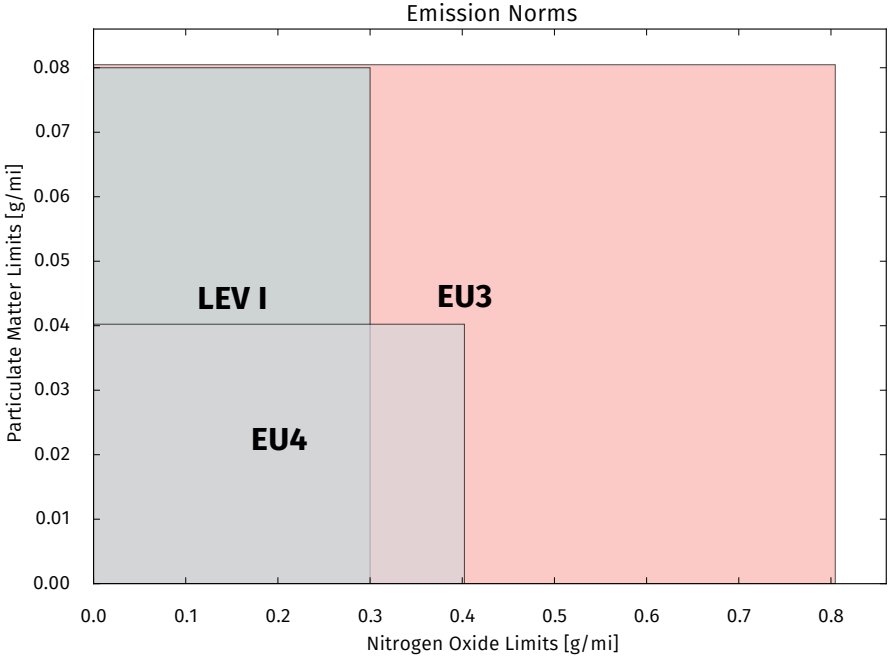
Federal Test Procedure

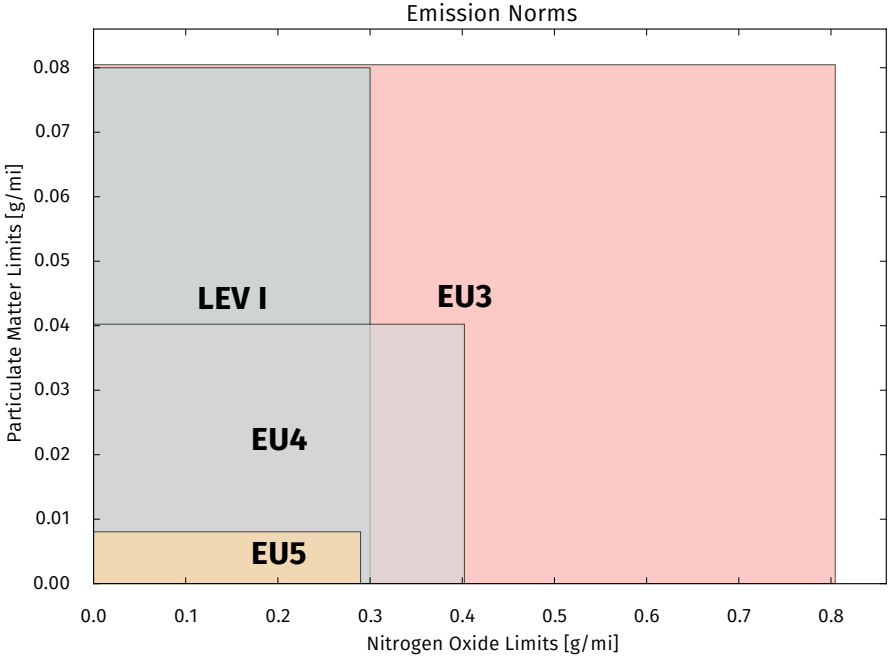


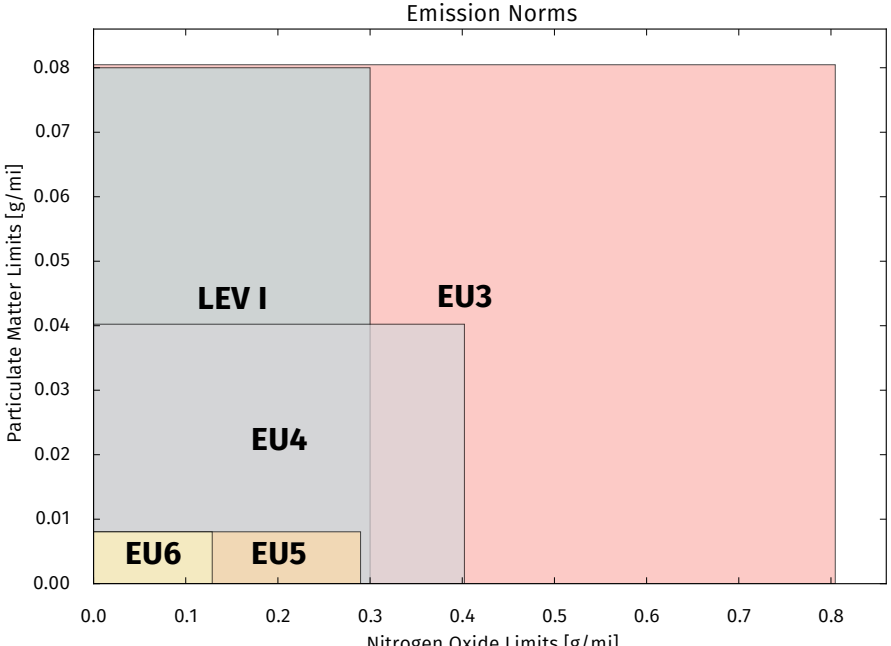
- Specify **time** – **vehicle speed**.
- Different tests per jurisdiction (EPA, CARB, EU).
- **Standardized** tests, publicly available.
- Runtime about **20–30 minutes**.

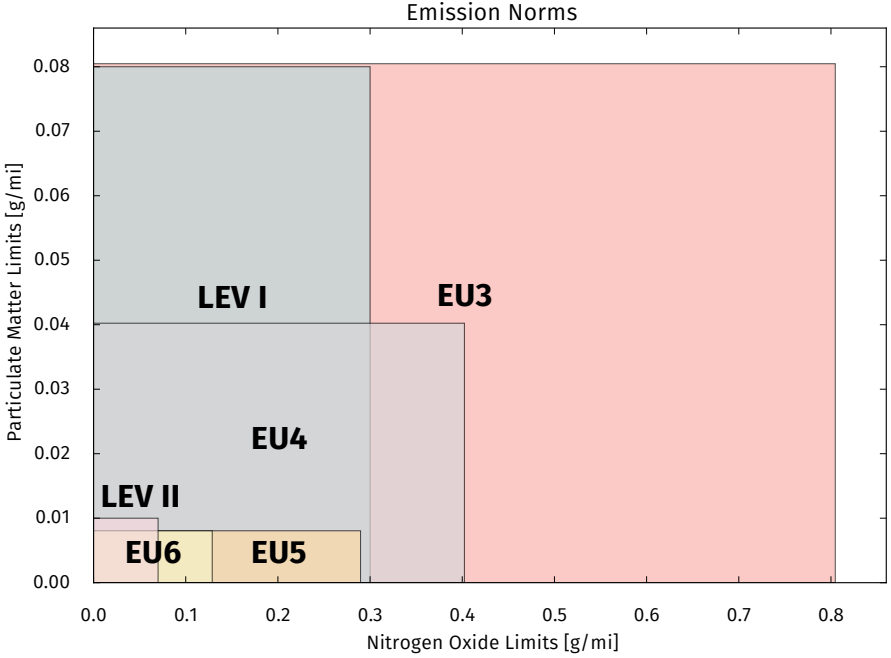

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
EU3
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]

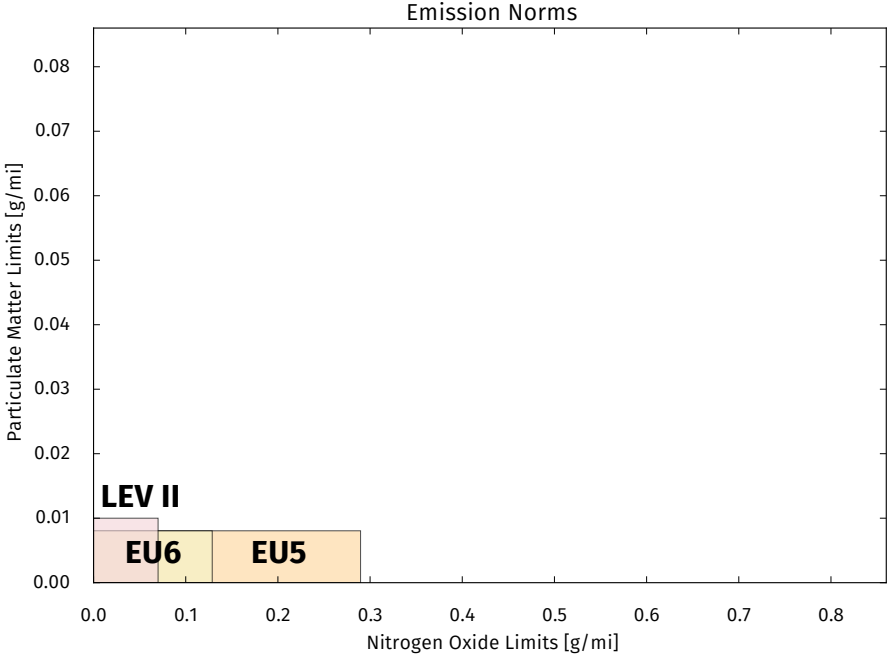

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]

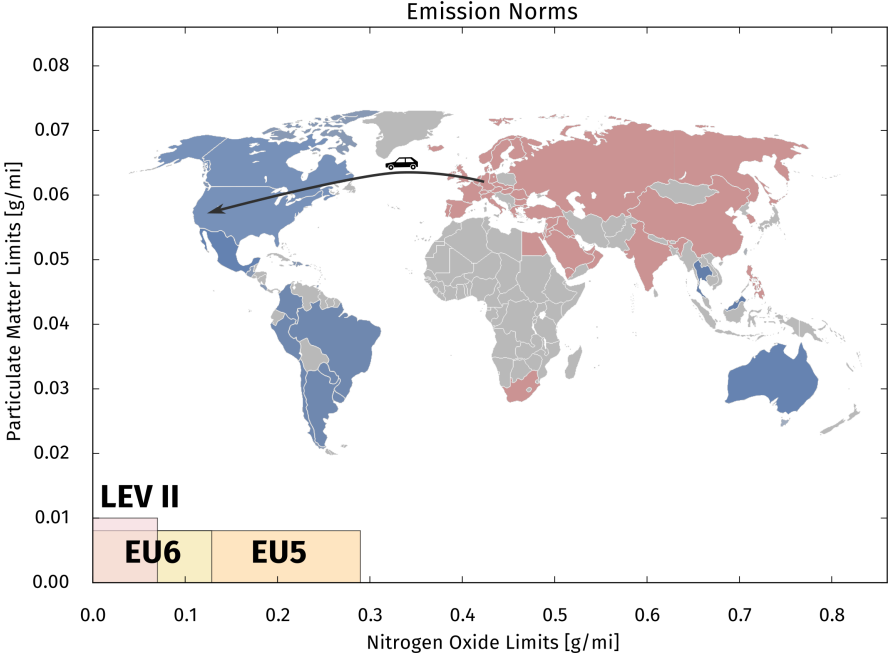

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
EU4
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
EU4
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
EU4
EU6
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
EU4
LEV II
EU6
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV II
EU6
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV II
EU6
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]

Defeat Devices

Regulations – §86.1803-01, United States

RUHR UNIVERSITÄT BOCHUM RUB

Auxiliary Emission Control Device (AECD) means any element of design which senses

- temperature,
- vehicle speed,
- engine RPM,
- transmission gear,
- manifold vacuum,

or any other parameter for the purpose of **activating**, **modulating**, **delaying**, or **deactivating** the operation of any part of the emission control system.

Regulations – §86.1803-01, United States

RUHR UNIVERSITÄT BOCHUM RUB

Defeat device means an auxiliary emission control device (AECD) that reduces the effectiveness of the emission control system under conditions which may reasonably be expected to be encountered in normal vehicle operation and use, **unless**:

1. Such conditions are substantially included in the Federal emission test procedure;
2. The need for the AECD is justified in terms of protecting the vehicle against damage or accident;
3. The AECD does not go beyond the requirements of engine starting; or
4. The AECD applies only for emergency vehicles [...]

Defeat Devices

RUHR UNIVERSITÄT BOCHUM RUB

Two essential components of a defeat device:

1. **Detect** an ongoing emissions test, and
2. **react** to it by modifying emission-related subsystems.

Defeat Devices

RUHR UNIVERSITÄT BOCHUM RUB

Two essential components of a defeat device:

1. Detect an ongoing emissions test, and
2. react to it by modifying emission-related subsystems.

We mostly focus on the first part in our talk.

Emissions test detection can be of varying complexity. Distinguish two flavors:

Passive — Targeting **environmental parameters** (e. g., altitude, temperature).

Defeat Devices

RUHR UNIVERSITÄT BOCHUM RUB

Emissions test detection can be of varying complexity. Distinguish two flavors:

Passive — Targeting **environmental parameters** (e. g., altitude, temperature).

Active — Specifically targeting characteristic **vehicle behavior**.

Defeat Devices

RUHR UNIVERSITÄT BOCHUM RUB

Emissions test detection can be of varying complexity. Distinguish two flavors:

Passive — Targeting environmental parameters (e. g., altitude, temperature).

Active — Specifically targeting characteristic **vehicle behavior**.

Examples

- Some Cadillacs stopped clean driving when turning on heating or air conditioning.

Defeat Devices

Emissions test detection can be of varying complexity. Distinguish two flavors:

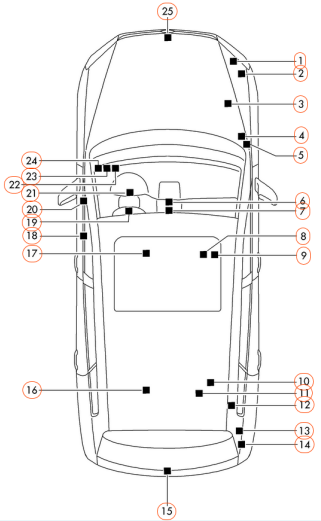
Passive — Targeting **environmental parameters** (e. g., altitude, temperature).

Active — Specifically targeting characteristic vehicle behavior.

Examples

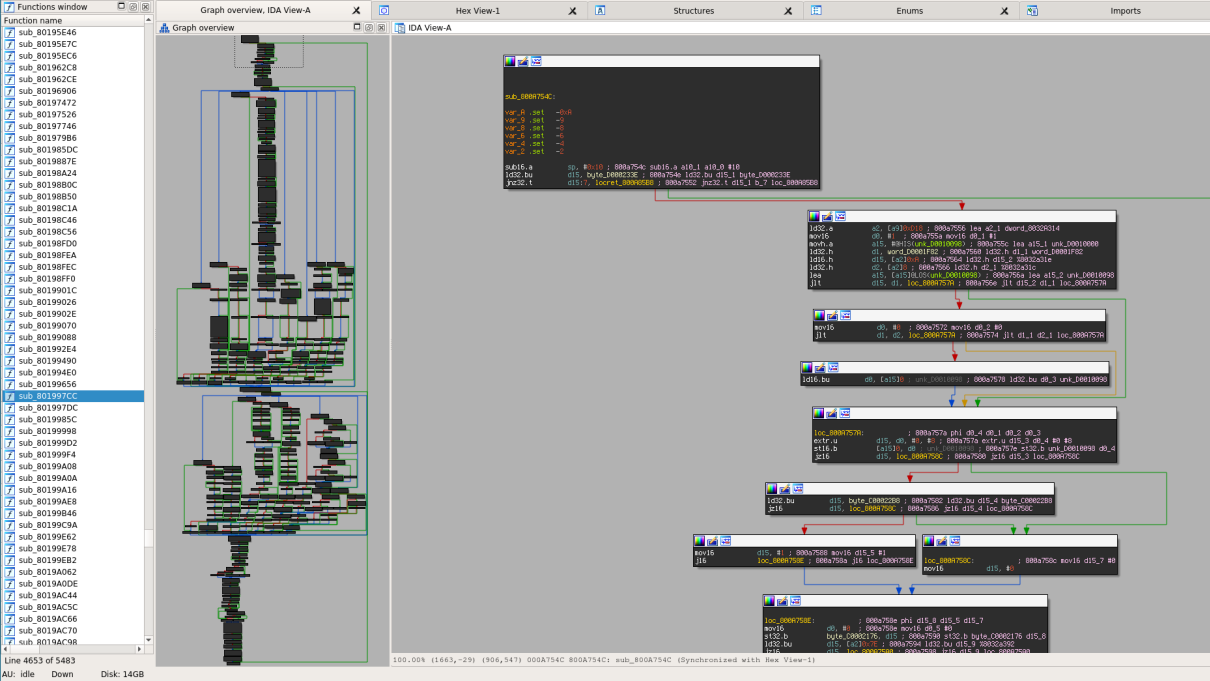
- Some Cadillacs stopped clean driving when turning on heating or air conditioning.
- The Opel Zafira can detect test cycles using rpm–torque operating points.

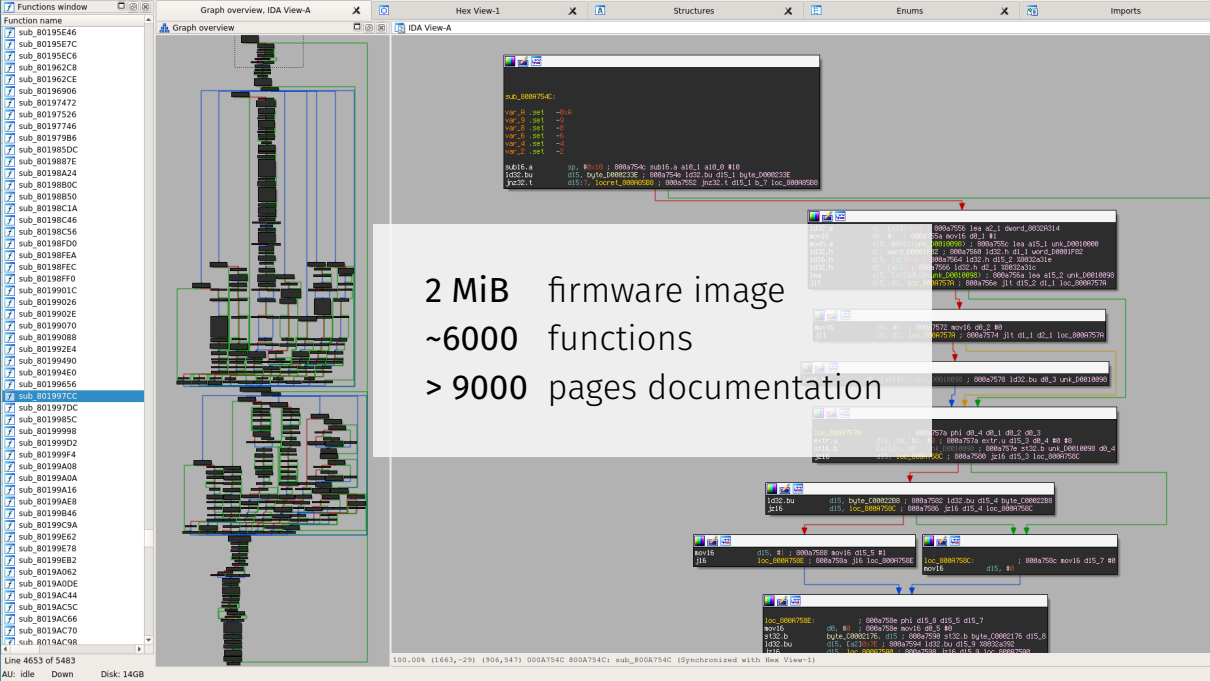
Engine Control Unit Firmware

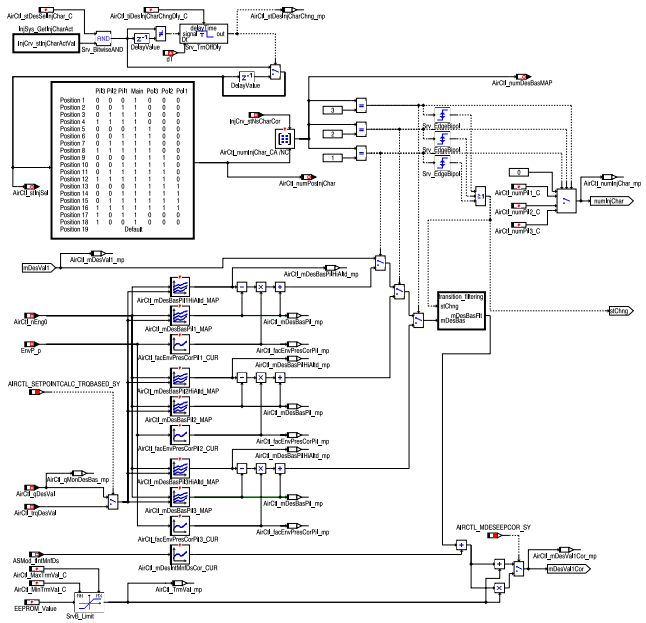


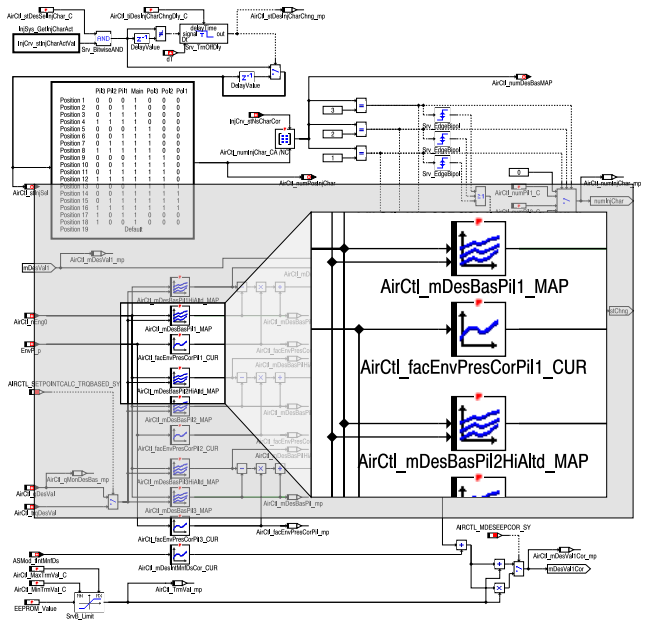
Note: Click red circle on image to select the meaning in table

#	Code	Title	Note
4		control unit for diesel engine see illustration, item:	906-20,1
(4)		control unit for petrol engine see illustration, item:	906-22,1
5		control unit for electric ancillary hydraulic pump for gear oil see illustration, item:	927-45,7 **Model data:** *PR-7L7,7L8*
6		control unit for airbag see illustration, item:	959-30,1
7		power module for cornering light see illustration, item:	941-10,4 **Model data:** *PR-8IM*
(7)		power module for cornering light see illustration, item:	941-20,4 **Model data:** *PR-8IP*
8		control unit for differential lock see illustration, item:	927-45,5 **Model data:** *PR-FN4*
9		control unit for 8-speed automatic gearbox see illustration, item:	927-45,1 **Model data:** *PR-G1G*
10		control unit for backrest release see illustration, item:	959-47,5 **Model data:** *PR-UK2*
11		control unit for fuel pump see illustration, item:	919-30,10
12		control unit for electro-mechanical parking brake see illustration, item:	907-05,8
13		control unit for differential locks see illustration, item:	927-45,3 **Model data:** *PR-1Y1*


Functions window
Function name
sub_80195E46
sub_80195E7C
sub_80195EC6
sub_801962C8
sub_801962CE
sub_80196906
sub_80197472
sub_80197526
sub_80197746
sub_801979B6
sub_80198SDC
sub_8019887E
sub_80198A24
sub_80198B0C
sub_80198B50
sub_80198C1A
sub_80198C46
sub_80198C56
sub_80198FD0
sub_80198FEA
sub_80198FEC
sub_80198FF0
sub_80199010
sub_80199026
sub_8019902E
sub_80199070
sub_801990B8
sub_80199EE4
sub_80199490
sub_801994E0
sub_80199656
sub_801997CC
sub_80197DC
sub_8019985C
sub_8019999B
sub_80199D2
sub_80199F4
sub_80199A08
sub_80199A0A
sub_80199A16
sub_80199AE8
sub_80199B46
sub_80199C9A
sub_80199E62
sub_80199E78
sub_80199EB2
sub_8019A062
sub_8019A0DE
sub_8019AC44
sub_8019AC5C
sub_8019AC66
sub_8019AC70
sub_8019AC98
Line 4653 of 5483
AU: idle Down Disk: 14GB
Graph overview, IDA View-A
Hex View-1
Structures
Enums
Imports
Graph overview
IDA View-A
sub_800A754C:
var_0 .set -0x0
var_9 .set -9
var_8 .set -8
var_6 .set -6
var_4 .set -4
var_2 .set -2
sub5.a sp, #0x10 ; 800a754c sub15.a a10_1 a10_0 #10
ld32.bu d15, byte_D000233E ; 800a754e ld32.bu d15_1 byte_D000233E
jnz32.t d15:7, !ocret_800A85B8 ; 800a7552 jnz32.t d15_1 b_7 loc_800A85B8
ld32.a a2, [a3]0x010 ; 800a7556 lea a2_1 dword_8032A314
mov16 d0, #1 ; 800a755a mov16 d0_1 #1
movh.a a15, #0x15<unk_D0010000> ; 800a755c lea a15_1 unk_D0010000
ld32.h d1, word_D001F02 ; 800a7560 ld32.h d1_1 word_D001F02
ld16.h d15, [a2]0x0 ; 800a7564 ld32.h d15_2 32032a3e
ld32.h d2, [a3]0 ; 800a7566 ld32.h d2_1 32032a3c
lea a15, [a15]0,05<unk_D0010090> ; 800a756a lea a15_2 unk_D0010090
jlt d15, d1, loc_800A757A ; 800a756e jlt d15_2 d1_1 loc_800A757A
mov16 d0, #0 ; 800a7572 mov16 d0_2 #0
jlt d1, d2, loc_800A757A ; 800a757A jlt d1_1 d2_1 loc_800A757A
ld16.bu d0, [a15]0 ; unk_D0010090 ; 800a7578 ld32.bu d0_3 unk_D0010090
loc_800A757A: ; 800a757a phi d0_4 d0_1 d0_2 d0_3
extr.u d15, d0, #0, #8 ; 800a757a extr.u d15_3 d0_4 #0 #8
st16.b [a15]0, d0 ; unk_D0010090 ; 800a757e st32.b unk_D0010090 d0_4
jz16 d15, loc_800A750C ; 800a7580 jz16 d15_3 loc_800A750C
ld32.bu d15, byte_C0002DB8 ; 800a7582 ld32.bu d15_4 byte_C0002DB8
jz16 d15, loc_800A750C ; 800a7586 jz16 d15_4 loc_800A750C
mov16 d15, #1 ; 800a7588 mov16 d15_5 #1
j16 loc_800A750E ; 800a758a j16 loc_800A750E
loc_800A750C: ; 800a758c mov16 d15_7 #0
mov16 d15, #0
loc_800A750E: ; 800a758e phi d15_8 d15_5 d15_7
mov16 d0, #1 ; 800a750e mov16 d0_5 #0
st32.b byte_C0002176, d15 ; 800a7590 st32.b byte_C0002176 d15_8
ld32.bu d15, [a2]0 ; 800a7594 ld32.bu d15_9 30032a98
jnz16 d15, loc_800A759A ; 800a7598 jnz16 d15_9 loc_800A759A
100.00% (1663,-29) (906,547) 000A754C 800A754C: sub_800A754C (Synchronized with Hex View-1)


Functions window
Function name
sub_80195E46
sub_80195E7C
sub_80195EC6
sub_801962C8
sub_801962CE
sub_80196906
sub_80197472
sub_80197526
sub_80197746
sub_801979B6
sub_801985DC
sub_8019887E
sub_80198A24
sub_80198B0C
sub_80198B50
sub_80198C1A
sub_80198C46
sub_80198C56
sub_80198FD0
sub_80198FEA
sub_80198FEC
sub_80198FF0
sub_8019901C
sub_80199026
sub_8019902E
sub_80199070
sub_801990B8
sub_80199204
sub_80199490
sub_80199490
sub_801994E0
sub_80199656
sub_801997CC
sub_80199DC
sub_8019985C
sub_8019999B
sub_80199902
sub_80199F4
sub_80199A08
sub_80199A0A
sub_80199A16
sub_80199AE8
sub_80199B46
sub_80199C9A
sub_80199E62
sub_80199E78
sub_80199EB2
sub_80199A062
sub_8019A0DE
sub_8019AC44
sub_8019AC5C
sub_8019AC66
sub_8019AC70
sub_8019AC98
Line 4653 of 5483
AU: idle
Down
Disk: 14GB
Graph overview, IDA View-A
Hex View-1
Structures
Enums
Imports
Graph overview
IDA View-A
2 MiB firmware image
~6000 functions
> 9000 pages documentation
100.00% (1663,-29) (906,547) 000A754C 800A754C: sub_800A754C (Synchronized with Hex View-1)





ASAM MCD-2 MC

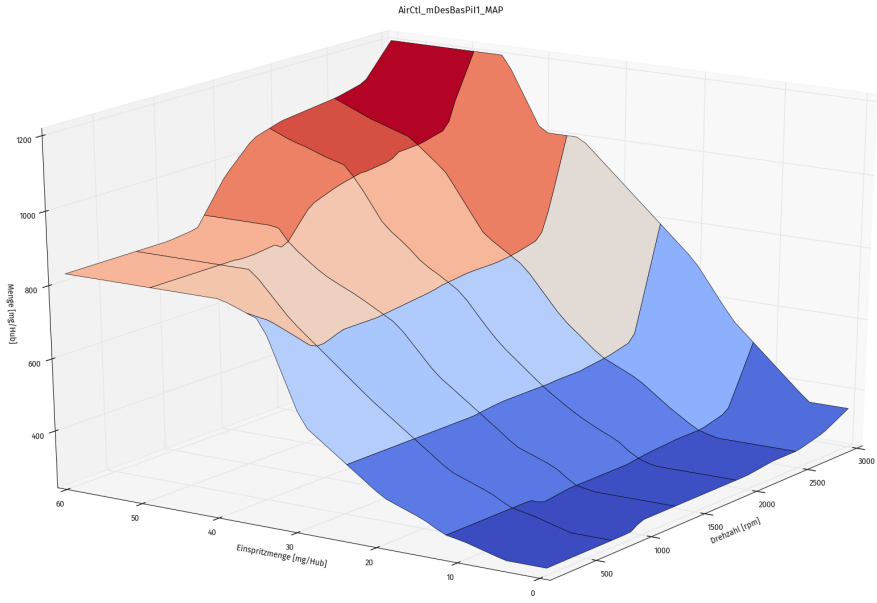
"`.a2l` files"

```
/begin MEASUREMENT
   EnvT_t
   "Umgebungslufttemperatur"

   SWORD
   Temp_Cels
   1
   100
   -3549.940
   3003.560

   FORMAT "%8.3"

   ECU_ADDRESS 0xD0000AA6
/end MEASUREMENT
```

```
/begin COMPU_METHOD
   Temp_Cels
   ""
   RAT_FUNC
   "%6.1"
   "deg C"

   COEFFS 0 10 2731.4 0 0 1
/end COMPU_METHOD
```

```
/begin CHARACTERISTIC
   AirCtl_mDesBasPiI1_MAP
   "Grundkennfeld Luftmassensollwert"

   MAP
   0x8037CE3A
   Map_Xs16Ys16Ws16

   1500.000
   AirMassPerCyl
   0.00
   1500.000

   FORMAT "%8.3"
   EXTENDED_LIMITS -3276.800 3276.700
```

```
/begin AXIS_DESCR
   STD_AXIS
   AirCtl_nEng0
   EngN
   16
   ...
/end AXIS_DESCR

/begin AXIS_DESCR
   STD_AXIS
   AirCtl_qMonDesBas_mp
   InjMass
   16
   ...
/end AXIS_DESCR
/end CHARACTERISTIC
```


AirCtl_mDesBasPil1_MAP
1200
1000
800
600
400
mAirPc [mg/Hub]
60
50
40
30
20
10
0
Einspritzmenge [mg/Hub]
500
1000
1500
2000
2500
3000
Drehzahl [rpm]

“Curve Function” – `SrvX_IpoCurveS16`

RUHR UNIVERSITÄT BOCHUM RUB

- Core function provided by the base system.
  - Unlikely to change across firmware versions.
  - Easy to detect in stripped images.
- Used to query **characteristic curves** specifying physical processes.

“Curve Function” – SrvX_IpoCurveS16

RUHR UNIVERSITÄT BOCHUM RUB

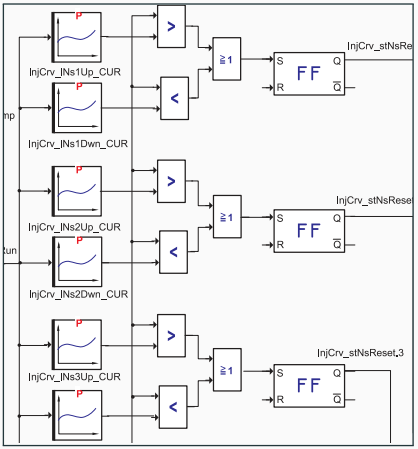
- Core function provided by the base system.
  - Unlikely to change across firmware versions.
  - Easy to detect in stripped images.
- Used to query **characteristic curves** specifying physical processes.

Point Queries

$$y \leftarrow \texttt{SrvX\_IpoCurveS16}(\mathit{curve}, x)$$

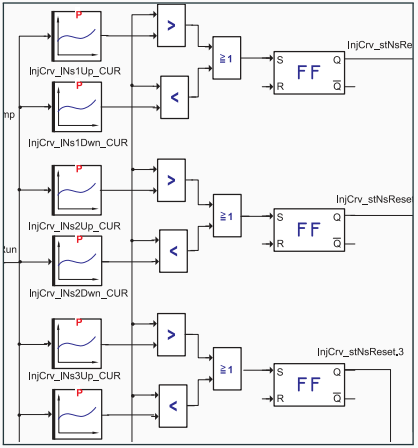
Volkswagen AG

Volkswagen AG Defeat Device



Vendor-specific “Acoustic Function”

$$y_0 \leftarrow \texttt{SrvX\_IpoCurveS16}(curve_{\perp}, \texttt{x})$$
$$y_1 \leftarrow \texttt{SrvX\_IpoCurveS16}(curve_{\top}, \texttt{x})$$



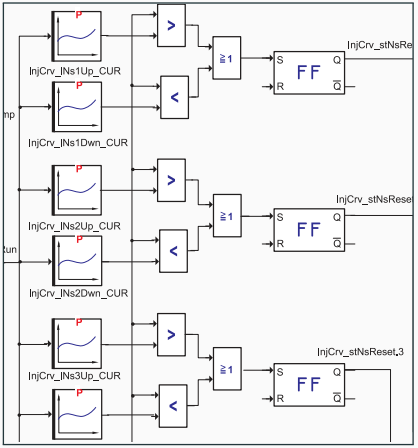
Vendor-specific “Acoustic Function”

$$y_0 \leftarrow \texttt{SrvX\_IpoCurveS16}(\mathit{curve}_{\perp}, \mathbf{x})$$
$$y_1 \leftarrow \texttt{SrvX\_IpoCurveS16}(\mathit{curve}_{\top}, \mathbf{x})$$

$$y_0 \leq \mathbf{y} \leq y_1$$

$$\Longleftrightarrow$$

“Profile matches”



Vendor-specific “Acoustic Function”

$$y_0 \leftarrow \texttt{SrvX\_IpoCurveS16}(\mathit{curve}_{\perp}, \mathbf{x})$$
$$y_1 \leftarrow \texttt{SrvX\_IpoCurveS16}(\mathit{curve}_{\top}, \mathbf{x})$$

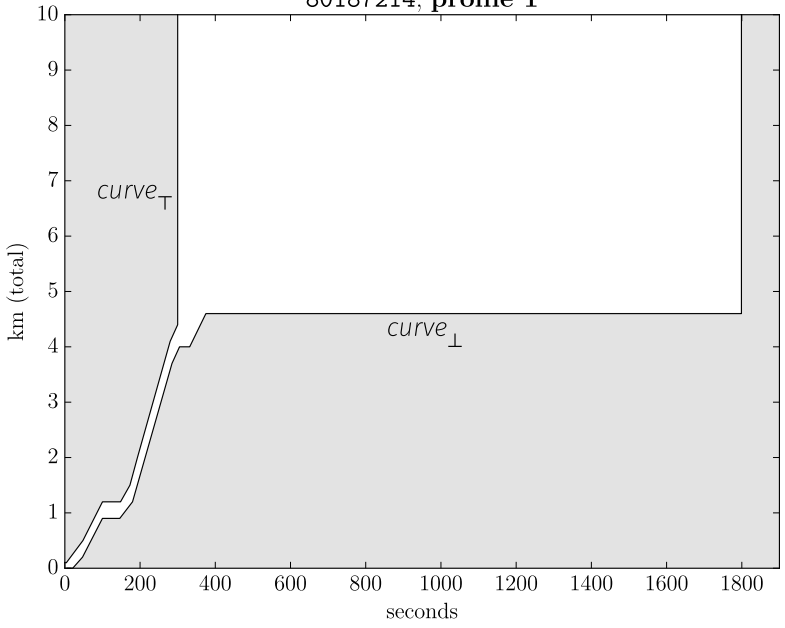
$$y_0 \leq \mathbf{y} \leq y_1$$

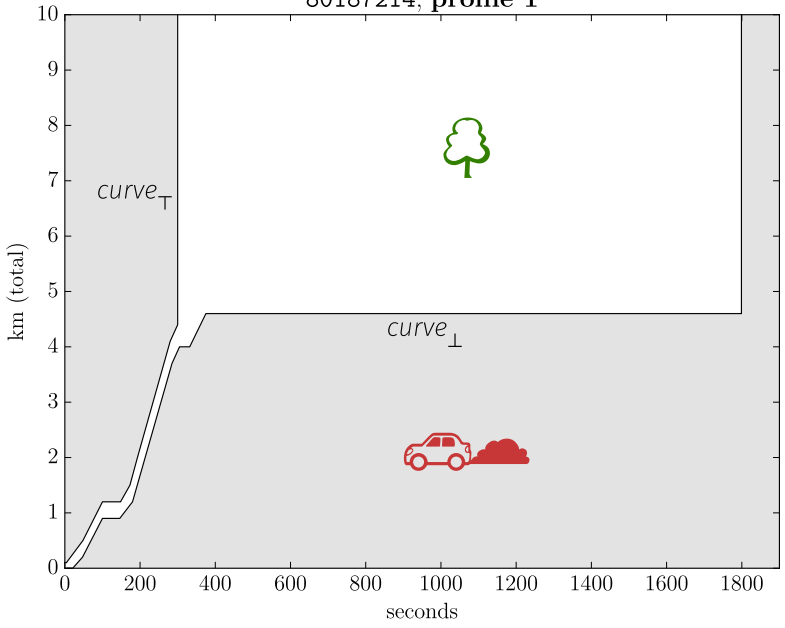
$$\Longleftrightarrow$$

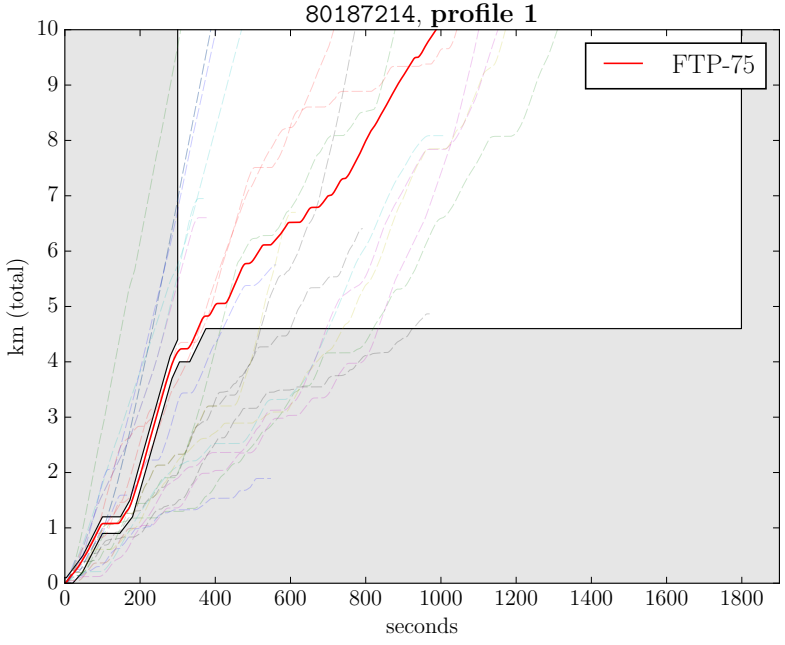
“Profile matches”

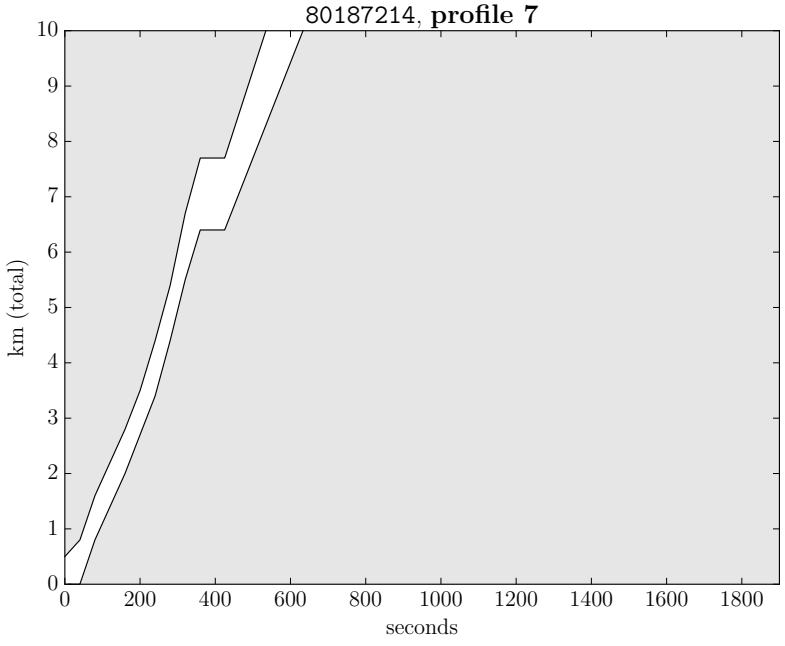
$\mathbf{x} \coloneqq$ “time since engine start”

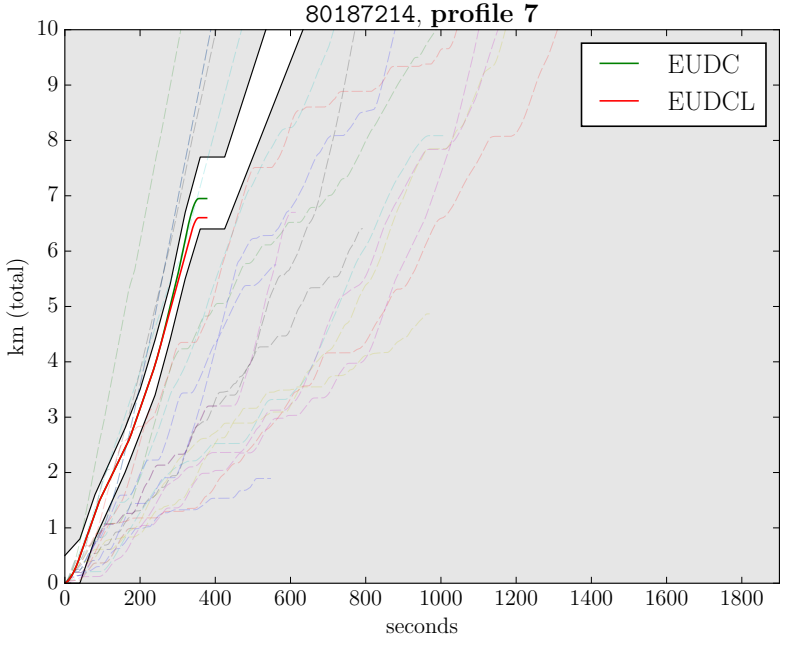
$\mathbf{y} \coloneqq$ “distance covered”

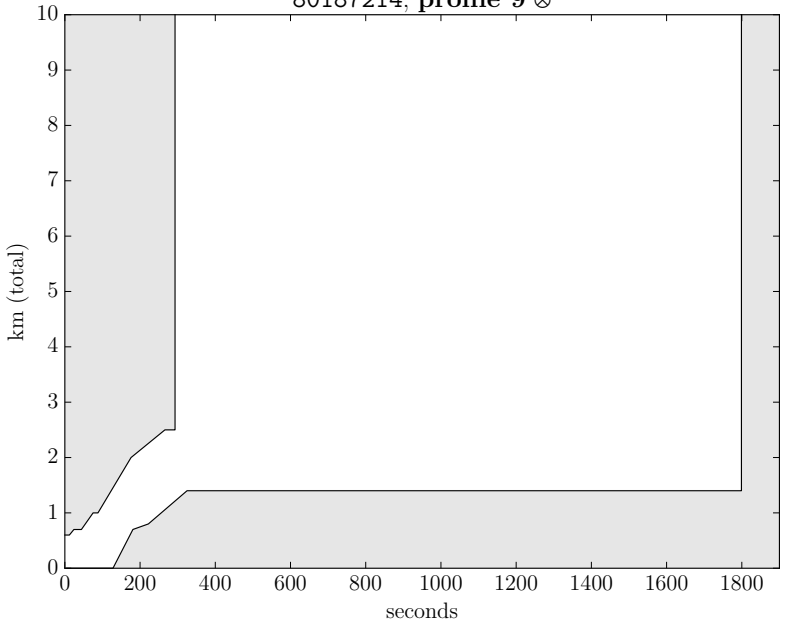

80187214, profile 1
curve⊤
curve⊥
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

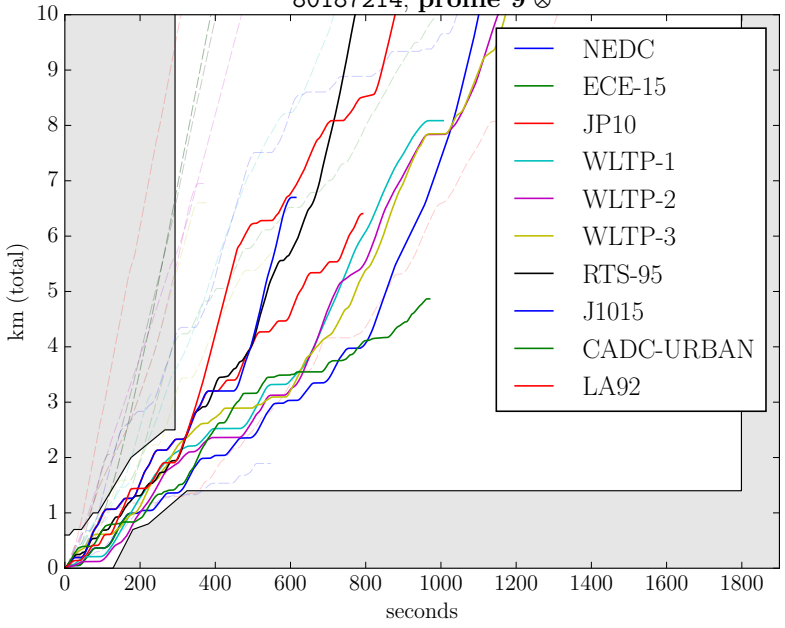

80187214, profile 1
km (total)
seconds
curve⊤
curve⊥
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

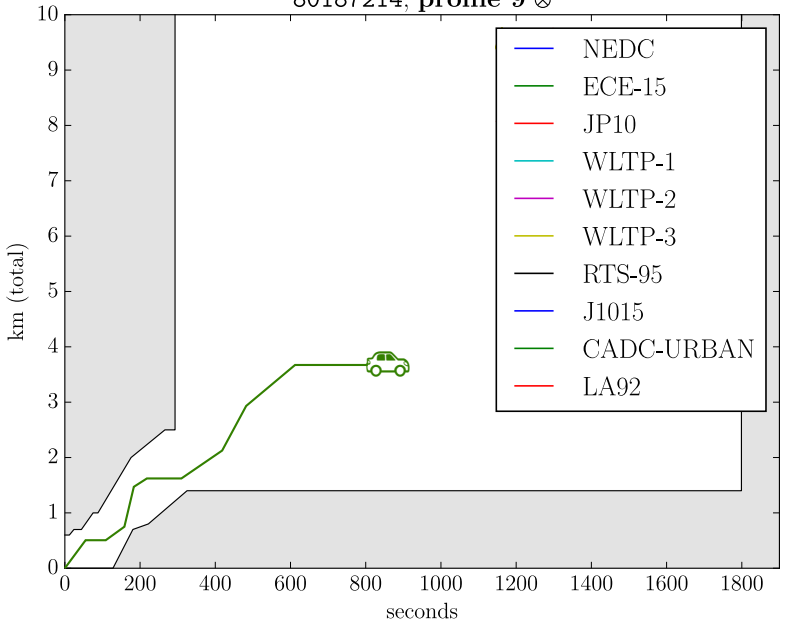

80187214, profile 1
FTP-75
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

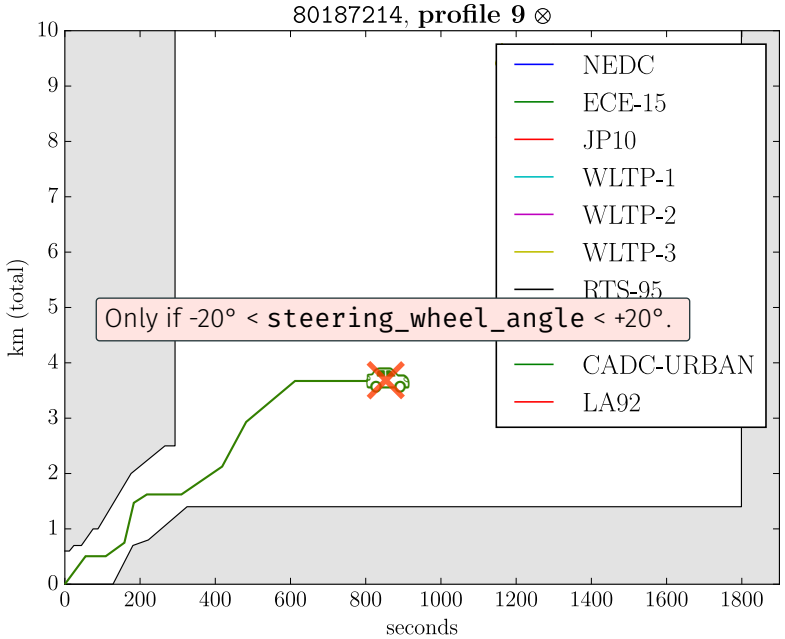

80187214, profile 7
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800


80187214, profile 7
EUDC
EUDCL
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800


80187214, profile 9 ⊗
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800


80187214, profile 9 ⊗
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800
NEDC
ECE-15
JP10
WLTP-1
WLTP-2
WLTP-3
RTS-95
J1015
CADC-URBAN
LA92


80187214, profile 9 ⊗
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800
NEDC
ECE-15
JP10
WLTP-1
WLTP-2
WLTP-3
RTS-95
J1015
CADC-URBAN
LA92


80187214, profile 9 ⊗
NEDC
ECE-15
JP10
WLTP-1
WLTP-2
WLTP-3
RTS-95
CADC-URBAN
LA92
Only if -20° < steering_wheel_angle < +20°.
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

RUHR UNIVERSITÄT BOCHUM RUB

CurveDiff automatically analyzes ECU firmware.

- Based on PyPy 2.7 and IDA Pro 6.x.

```
[17905: 0 - 18:17:12] Analyzing FL_03L906012___7444.
[17905: 0 - 18:17:12] Pre-processing database...
[17905: 1 - 18:17:51] Exporting functions...
[17905: 2 - 18:18:46] Analyzing functions...
[17905: 3 - 18:19:17] Exporting curves...
[17905: 4 - 18:19:42] Analyzing curves...

Function 80187214 matches the following test cycles:
- (802f6f70, 802f6fae): FTP-75
- (802f6fec, 802f702a): LA92
- (802f7068, 802f70a6): US06
- (802f70e4, 802f7122): SC03
- (802f7160, 802f719e): HWFET
- (802f71dc, 802f721a): ECE-15
- (802f7258, 802f7296): EUDC EUDCL
- (802f72d4, 802f7312): FTP-75 CADC-RURAL IM240
- (802f7350, 802f738e): NEDC ECE-15 JP10 WLTP-1…
- (802f6ef4, 802f6f32): CADC-RURAL SC03

[17905: 5 - 18:19:43] Success.
```

RUHR UNIVERSITÄT BOCHUM RUB

CurveDiff automatically analyzes ECU firmware.

- Based on **PyPy 2.7** and **IDA Pro 6.x**.
- Electronic Diesel Control **EDC17** by Bosch.

```
[17905: 0 - 18:17:12] Analyzing FL_03L906012___7444.
[17905: 0 - 18:17:12] Pre-processing database...
[17905: 1 - 18:17:51] Exporting functions...
[17905: 2 - 18:18:46] Analyzing functions...
[17905: 3 - 18:19:17] Exporting curves...
[17905: 4 - 18:19:42] Analyzing curves...

Function 80187214 matches the following test cycles:
- (802f6f70, 802f6fae): FTP-75
- (802f6fec, 802f702a): LA92
- (802f7068, 802f70a6): US06
- (802f70e4, 802f7122): SC03
- (802f7160, 802f719e): HWFET
- (802f71dc, 802f721a): ECE-15
- (802f7258, 802f7296): EUDC EUDCL
- (802f72d4, 802f7312): FTP-75 CADC-RURAL IM240
- (802f7350, 802f738e): NEDC ECE-15 JP10 WLTP-1…
- (802f6ef4, 802f6f32): CADC-RURAL SC03

[17905: 5 - 18:19:43] Success.
```

CurveDiff automatically analyzes ECU firmware.

- Based on **PyPy 2.7** and **IDA Pro 6.x**.
- Electronic Diesel Control **EDC17** by Bosch.
- Infineon **TriCore 179x** processor.

```
[17905: 0 - 18:17:12] Analyzing FL_03L906012___7444.
[17905: 0 - 18:17:12] Pre-processing database...
[17905: 1 - 18:17:51] Exporting functions...
[17905: 2 - 18:18:46] Analyzing functions...
[17905: 3 - 18:19:17] Exporting curves...
[17905: 4 - 18:19:42] Analyzing curves...

Function 80187214 matches the following test cycles:
- (802f6f70, 802f6fae): FTP-75
- (802f6fec, 802f702a): LA92
- (802f7068, 802f70a6): US06
- (802f70e4, 802f7122): SC03
- (802f7160, 802f719e): HWFET
- (802f71dc, 802f721a): ECE-15
- (802f7258, 802f7296): EUDC EUDCL
- (802f72d4, 802f7312): FTP-75 CADC-RURAL IM240
- (802f7350, 802f738e): NEDC ECE-15 JP10 WLTP-1…
- (802f6ef4, 802f6f32): CADC-RURAL SC03

[17905: 5 - 18:19:43] Success.
```

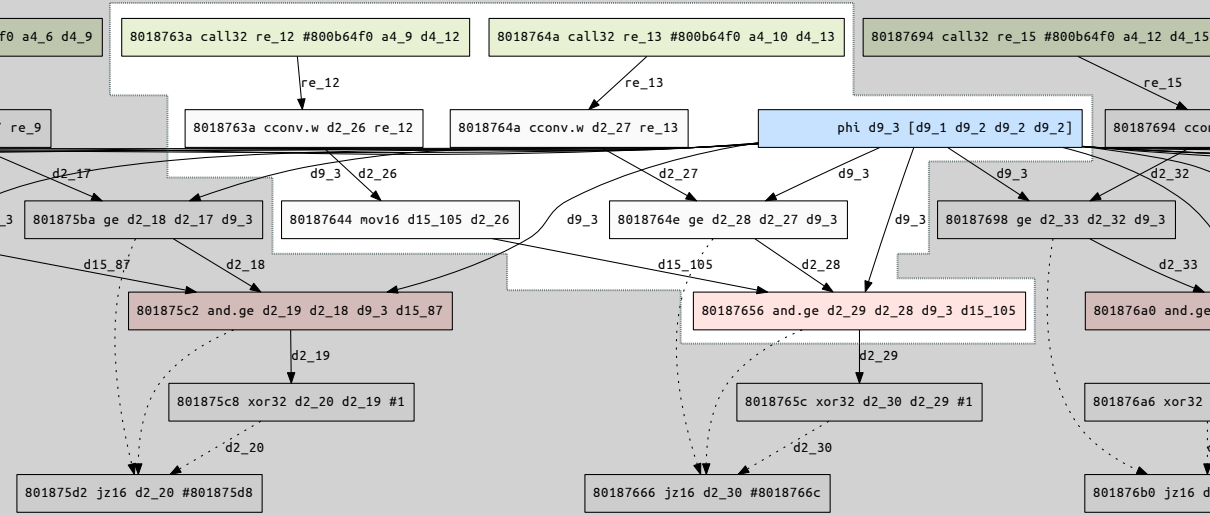
CurveDiff Framework

RUHR UNIVERSITÄT BOCHUM RUB

CurveDiff automatically analyzes ECU firmware.

- Based on **PyPy 2.7** and **IDA Pro 6.x**.
- Electronic Diesel Control **EDC17** by Bosch.
- Infineon **TriCore 179x** processor.
- Lift to **Static Single Assignment** form, compiler optimizations.

```
[17905: 0 - 18:17:12] Analyzing FL_03L906012___7444.
[17905: 0 - 18:17:12] Pre-processing database...
[17905: 1 - 18:17:51] Exporting functions...
[17905: 2 - 18:18:46] Analyzing functions...
[17905: 3 - 18:19:17] Exporting curves...
[17905: 4 - 18:19:42] Analyzing curves...

Function 80187214 matches the following test cycles:
- (802f6f70, 802f6fae): FTP-75
- (802f6fec, 802f702a): LA92
- (802f7068, 802f70a6): US06
- (802f70e4, 802f7122): SC03
- (802f7160, 802f719e): HWFET
- (802f71dc, 802f721a): ECE-15
- (802f7258, 802f7296): EUDC EUDCL
- (802f72d4, 802f7312): FTP-75 CADC-RURAL IM240
- (802f7350, 802f738e): NEDC ECE-15 JP10 WLTP-1…
- (802f6ef4, 802f6f32): CADC-RURAL SC03

[17905: 5 - 18:19:43] Success.
```


f0 a4_6 d4_9
8018763a call32 re_12 #800b64f0 a4_9 d4_12
8018764a call32 re_13 #800b64f0 a4_10 d4_13
80187694 call32 re_15 #800b64f0 a4_12 d4_15
re_12
re_13
re_15
re_9
8018763a cconv.w d2_26 re_12
8018764a cconv.w d2_27 re_13
phi d9_3 [d9_1 d9_2 d9_2 d9_2]
80187694 ccon
d2_17
d9_3
d2_26
d2_27
d9_3
d9_3
d2_32
_3
801875ba ge d2_18 d2_17 d9_3
80187644 mov16 d15_105 d2_26
d9_3
8018764e ge d2_28 d2_27 d9_3
d9_3
80187698 ge d2_33 d2_32 d9_3
d15_87
d2_18
d15_105
d2_28
d2_33
801875c2 and.ge d2_19 d2_18 d9_3 d15_87
80187656 and.ge d2_29 d2_28 d9_3 d15_105
801876a0 and.ge
d2_19
d2_29
801875c8 xor32 d2_20 d2_19 #1
8018765c xor32 d2_30 d2_29 #1
801876a6 xor32
d2_20
d2_30
801875d2 jz16 d2_20 #801875d8
80187666 jz16 d2_30 #8018766c
801876b0 jz16 d

Potential Defeat Devices

RUHR UNIVERSITÄT BOCHUM RUB

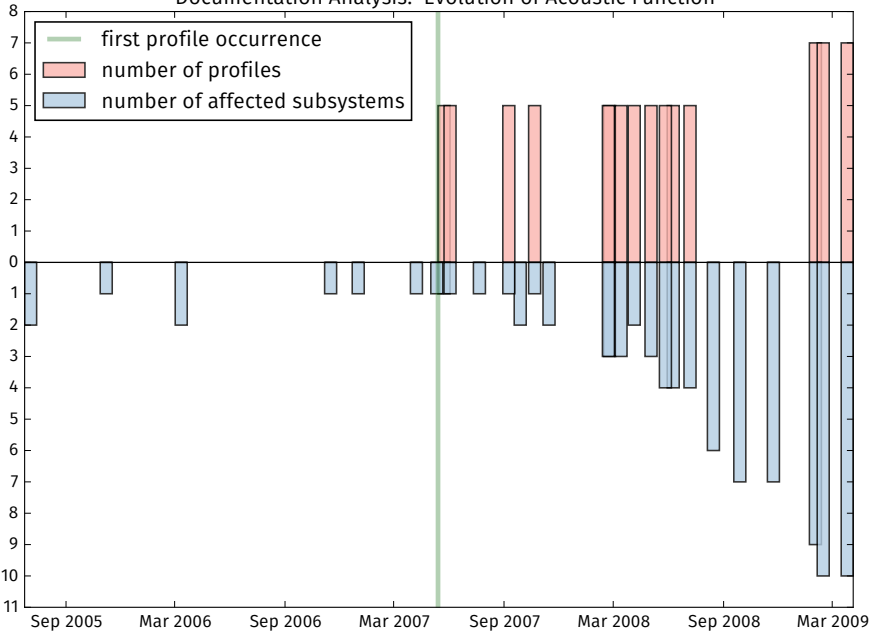
Analyzed **926** firmware images spanning **eight** years,
333 try to detect at least one emission test cycle.

2009-01	Golf, Passat (2)
2009-07	A3
2009-08	Passat Blue Motion
2009-09	Golf (2), Passat (3)
2009-10	Golf+, Passat
2009-11	A3 (8), Golf Blue Motion, Golf (2), Passat
2009-12	A3 (5), Golf Variant (2), Golf+ (2), Golf (7), Jetta (3), Passat (4)
2010-01	Jetta, Passat (2)
2010-03	A3 (2), Golf (3), Jetta, Passat (3), Q5 (4)
2010-04	Jetta (2), Passat, Passat Coupe (4), Q5
2012-05	A3 (19), A4, A6, Alhambra (4), Altea, Eos (2), Golf, Ibiza (4), Leon, Octavia (6), Q5 (2), Superb (2), TT, Tiguan, Yeti (4)
2012-06	Amarok (8), CC, Eos (2), Golf (2), Jetta (2), Octavia (3), Q5 (2), Sharan (7), Tiguan, Touran (2)
2012-07	A1 (3), Alhambra (4), Caddy (2), Sharan (8)
2012-09	Golf (2), Passat, Yeti (6)
2012-10	A3, Alhambra (2), Tiguan, Yeti
2012-12	Eos (2), Golf Cabriolet, Tiguan (7), Touran, Yeti
2013-01	Leon, Passat
2013-05	Amarok (4)
2013-06	Amarok (5), Superb (3), Tiguan
2013-07	Octavia
2013-08	Yeti (3)
2013-11	Superb (3)
2013-12	Superb (2), Yeti (4)
2014-03	Amarok (16), Eos, Tiguan, Yeti
2014-04	Q5, Superb (2)
2014-06	Amarok (6), Tiguan (4)
2014-09	Alhambra
2014-10	Sharan
2014-12	A4 (3), A6, **Passat** (4) ⊗
2015-01	Superb
2015-02	A3 (3)
2015-03	Alhambra (2)
2015-05	Alhambra (6), Sharan (6)
2015-07	Q3 (2)
2015-10	Altea (2), Yeti (3)
2015-11	Superb
2016-02	Altea
2016-03	A4, Exeo (4)
2016-04	A6, Exeo, Q3
2016-06	Altea (3), CC (3), Jetta, Leon (2), Superb, Tiguan (2)
2016-07	Amarok, CC, Golf, Superb
2016-08	CC (3), Golf Cabriolet, Golf (2), Passat (2), Scirocco, Touran (3)
2016-09	CC (14), Octavia (2), Passat (2), Tiguan (7)
2016-10	Eos

Affected Subsystems

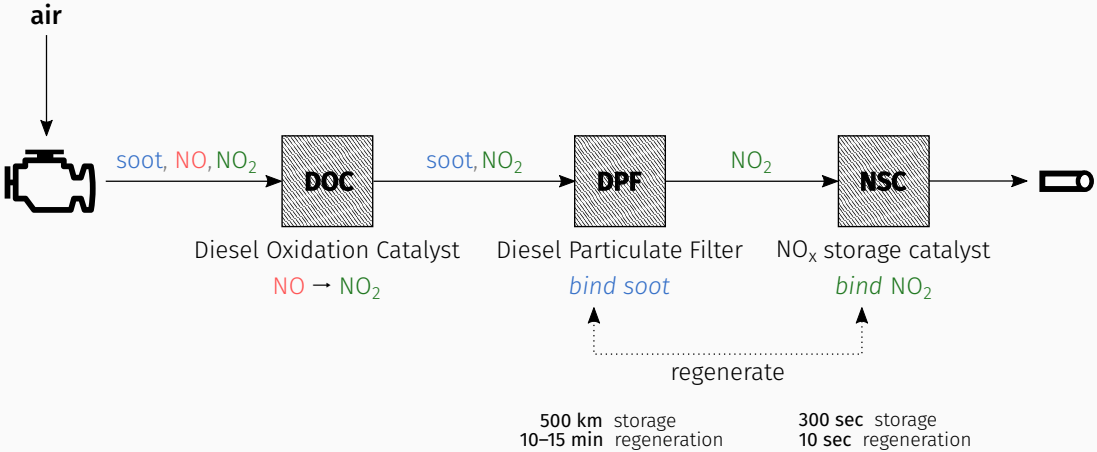
- **InjCrv** – injection pattern, injection timing
- **Rail, PCR** – manifold pressure

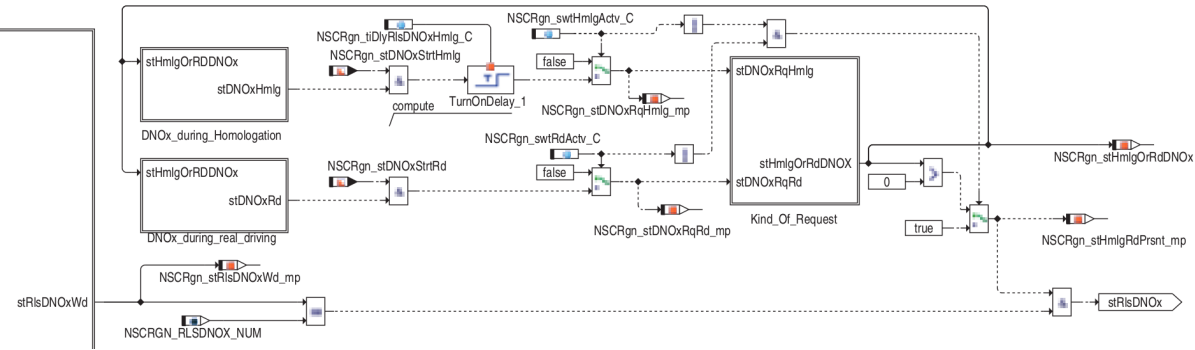
- **SmkLim** – smoke limitation
- **AFS, AirCtl** – desired air mass EGR
- **PFlt** – soot mass simulation
- **ASMod** – desired soot mass DPF
- **SCRFFC** – desired reducing agent SCR

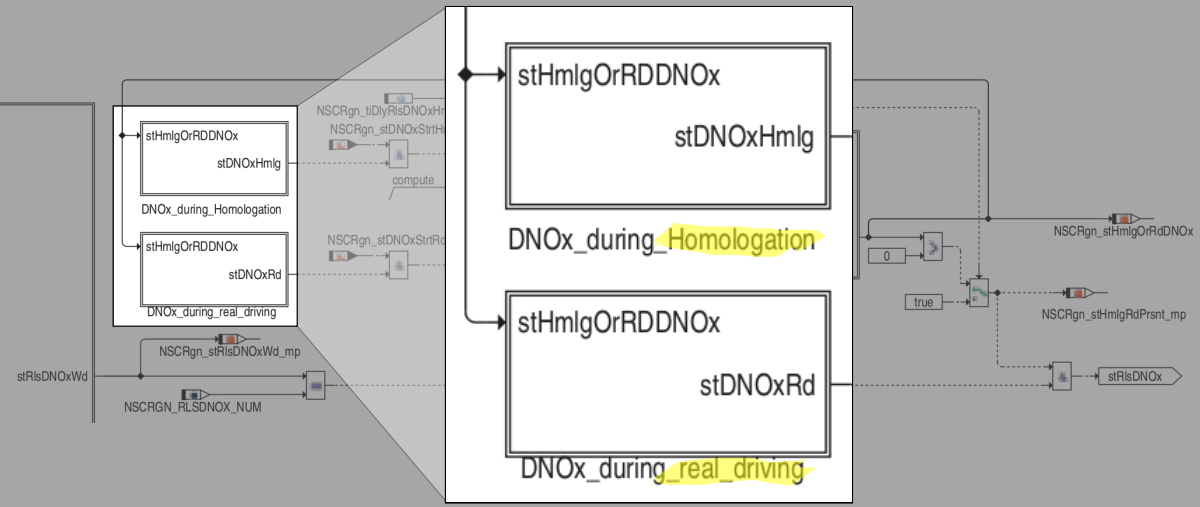

Documentation Analysis: Evolution of Acoustic Function
first profile occurrence
number of profiles
number of affected subsystems
8
7
6
5
4
3
2
1
0
1
2
3
4
5
6
7
8
9
10
11
Sep 2005
Mar 2006
Sep 2006
Mar 2007
Sep 2007
Mar 2008
Sep 2008
Mar 2009

Fiat Chrysler Automobiles

Image by Herranderssvensson


air
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
NSC
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
NO_x storage catalyst
bind NO_2
regenerate
500 km storage
10–15 min regeneration
300 sec storage
10 sec regeneration

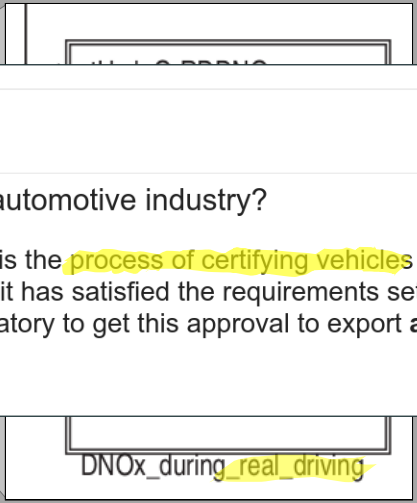


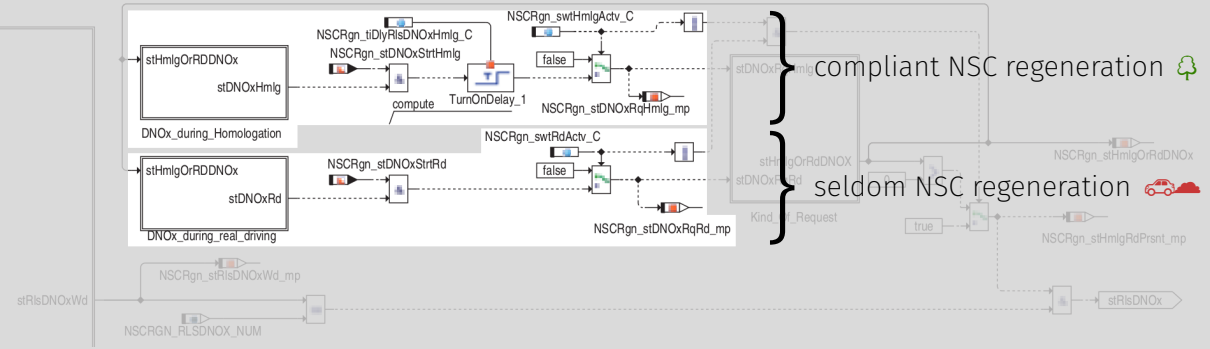


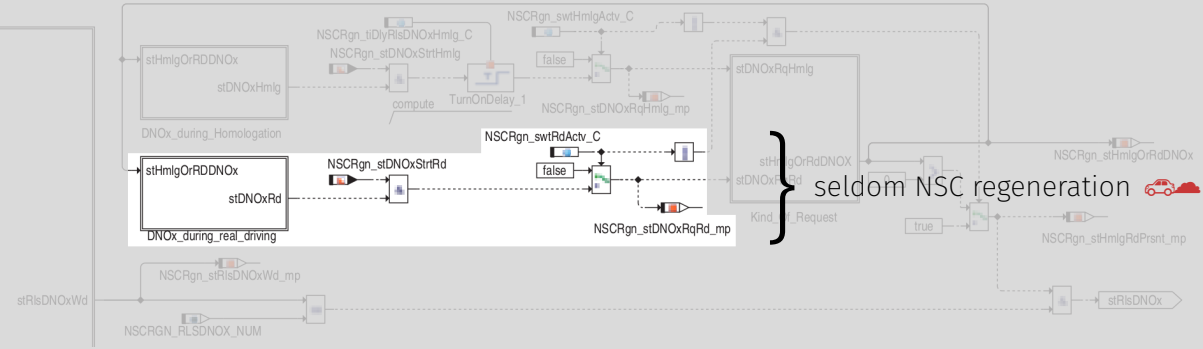
People also ask

What is homologation in automotive industry?

Automotive homologation is the process of certifying vehicles or a particular component in a **vehicle** that it has satisfied the requirements set by various statutory regulatory bodies. It is mandatory to get this approval to export **automobile** products or components.







after 1600 seconds

California found a new cheat device in Audi transmissions: report

Viknesh Vijayenthiran Nov 7, 2016 Follow Viknesh

RELATED ARTICLES

Attribution

- Pumpe-Düse-Einspritzung
- Konventionelle Einspritzung
- Motorsteuerung
- Glühkerzen
- Abgasnachbehandlung
- Vakuumpumpe
- Lambdasonde
- Luftmassenmesser
- Weitere Sensoren
- Großdiesel

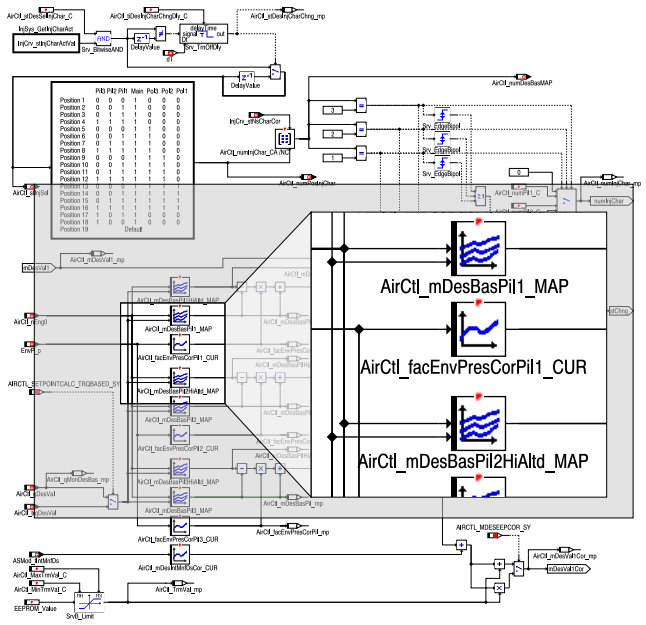
Produktinformation

Motorsteuerung: Motorfunktionen perfekt geregelt

Die EDC (Electronic Diesel Control) ist die Motorsteuerung beim Diesel. Sie regelt die Funktionen des Einspritzsystems und sorgt dafür, dass der Motor das angeforderte Motordrehmoment bereitstellt. Die Einspritzung wird dabei permanent auf den Motor und die Fahrsituation abgestimmt. Dieselmotoren mit Bosch-Motorsteuerung überzeugen durch hohe Dynamik bei geringem Kraftstoffverbrauch und optimierte Motorleistung.

Vorteile

- Sparsamer Betrieb durch schnelle Anpassung aller Einspritzparameter



Supplied Fixes

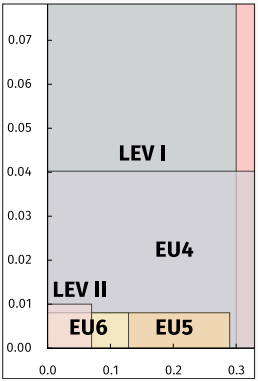
United States

				NO_x control[1]	Hardware replacement	Labor hours	Fuel economy loss	Diesel Exhaust Fluid increase
Gen 1	2009	VW Jetta, Beetle, Golf	2.0L	LNT EGR	Lean-NO_x trap Particulate filter Glow plug module	6	Up to 2 mpg[3]	N/A
Gen 1	2010–2014	Audi A3 VW Jetta, Beetle, Golf	2.0L	LNT EGR	Lean-NO_x trap	2.5 - 3	Up to 2 mpg[3]	N/A
Gen 2	2012–2014	VW Passat[2]	2.0L	SCR EGR	Software only	1	Up to 1 mpg[4]	50% - 130%
Gen 3	2015	Audi A3 VW Jetta, Beetle, Golf, Passat	2.0L	SCR EGR	SCR catalyst Particulate filter Oxidation catalyst 2nd NO_x sensor	9	None	1% - 14%
Gen 1	2009–2012	VW Touareg	3.0L	SCR EGR	No fix – vehicles will be scrapped			
Gen 2.1	2013–2014	VW Touareg Porsche Cayenne Audi Q7	3.0L	SCR EGR	SCR catalyst Cyl. pressure sensor Particulate sensor	3	Up to 1 mpg[5]	About 40%
Gen 2.1	2015	Audi Q7	3.0L	SCR EGR	SCR catalyst Particulate sensor	3	Up to 1 mpg[4]	About 40%
Gen 2.2	2015–2016	VW Touareg Porsche Cayenne	3.0L	SCR EGR	Software only	1	Up to 1 mpg[4]	About 40%
Gen 2	2014–2016	Audi A6, A7, A8, Q5	3.0L	SCR EGR	Fix not yet defined			

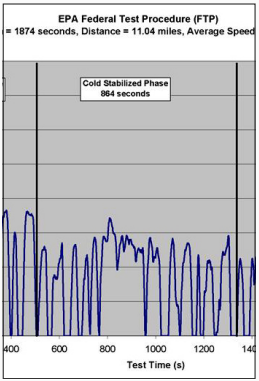
Europe

				NO_x control[1]	Hardware replacement	Labor hours	Fuel economy loss	Diesel Exhaust Fluid increase
Euro5	2009–2014	Audi A1, A3, A4, A5, A6, Q3, Q5, TT	1.2L	EGR	Software only[2]	0.5	None	N/A
		Seat Alhambra, Altea, Exeo, Ibiza, Leon, Toledo Skoda Fabia, Roomster, Rapid, Yeti, Octavia, Superb	1.6L		Flow transformer[3]	1.0	None	N/A
		VW Golf, Passat, Tiguan, Polo, Jetta, Scirocco, Caddy, Transporter	2.0L		Software only[2]	0.5	None	N/A
Euro5	2010–2013	Audi A7, A8 Porsche Cayenne	3.0L	EGR	Software only	0.5		N/A
Euro6	2014–2017	Porsche Cayenne	3.0L	SCR EGR	Software only	1.0		
Euro6	2014–2017	Audi A8	4.2L	SCR EGR	Software only			

Future of Emissions Testing

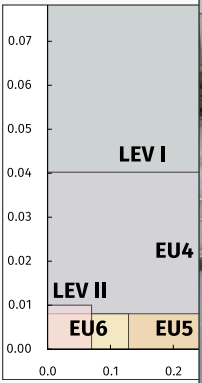


Strict Regulations



Public Test Cycles

Black Box Testing



Strict Regulations ~~Public Test Cycles~~ Black Box Testing

Portable Emissions Measurement

Resulting Challenge

RUHR UNIVERSITÄT BOCHUM RUB

Compliance testing now is a **software verification problem**.

- Easier to hide in software; black box testing alone is insufficient.
- *Portable Emissions Measurement* only side-steps the problem.
- Software analysis facilitates large-scale testing.

Conclusion

RUHR UNIVERSITÄT BOCHUM RUB

- We analyzed two **modern defeat devices** in software:
  - Volkswagen AG ..... driving profile check
  - Fiat 500X ..... timing-based check
- We performed a **large-scale study** of the VW AG defeat device.
  - Tested > 900 firmware images.
  - ~300 try to detect at least one test cycle.

- Black-box emissions testing is insufficient.
- Easy to cheat using software, high incentive to do so.
- Software verification of compliance poses a new challenge.