RUHR UNIVERSITÄT BOCHUM RUB

UC San Diego

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

IEEE Security & Privacy 2017, San Jose

May 22, 2017

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

* Ruhr-Universität Bochum † University of California, San Diego

AMERICA

'It Was Installed For This Purpose,' VW's CEO Tells Congress About Defeat Device

October 8, 2015 · 10:17 AM ET

BILL CHAPPELL

Volkswagen Says 11 Million Cars Worldw

By JACK EWING SEPT. 22, 2015

BUSINESS NEWS | Thu Jan 12, 2017 | 12:26am GMT

U.S. indicts six as Volkswagen agrees to $4.3 billion diesel settlement

SHARE

Department of Justice

Office of Public Affairs

Monday, January 4, 2016

IEDIATE RELEASE

ed States Files Complaint Against Volkswagen, Audi and Porsche for Alleged Clean Air Act Violations

partment of Justice, on behalf of the Environmental Protection Agency (EPA), today filed a civil complaint in federal

Abgasaffäre

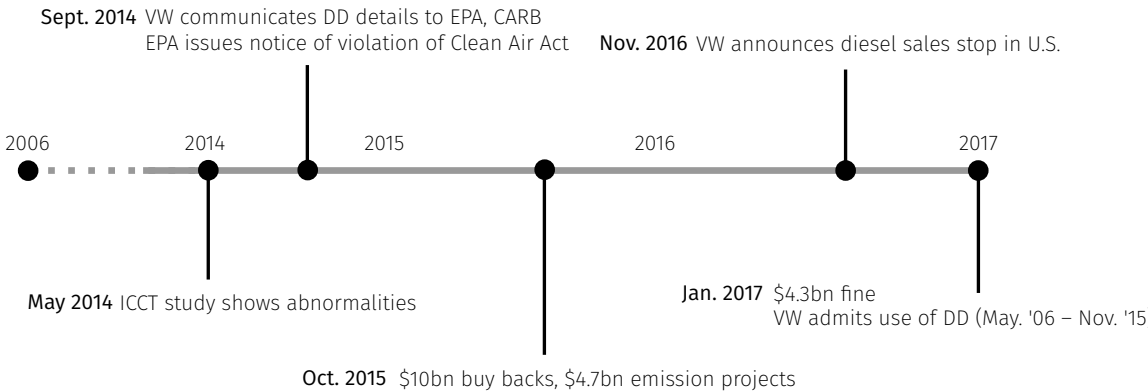
VW manipulierte offenbar während Ermittlungen weiter

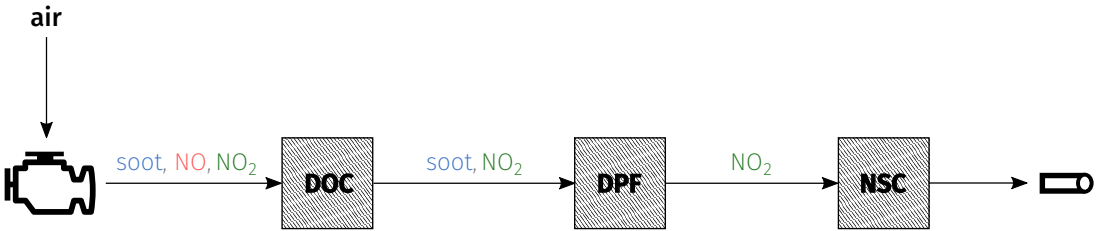
Techniker haben die Manipulationssoftware laut Medien noch verändert, als US-Behörden bereits gegen VW ermittelten. Das könnte zum Auffliegen der Affäre geführt haben.

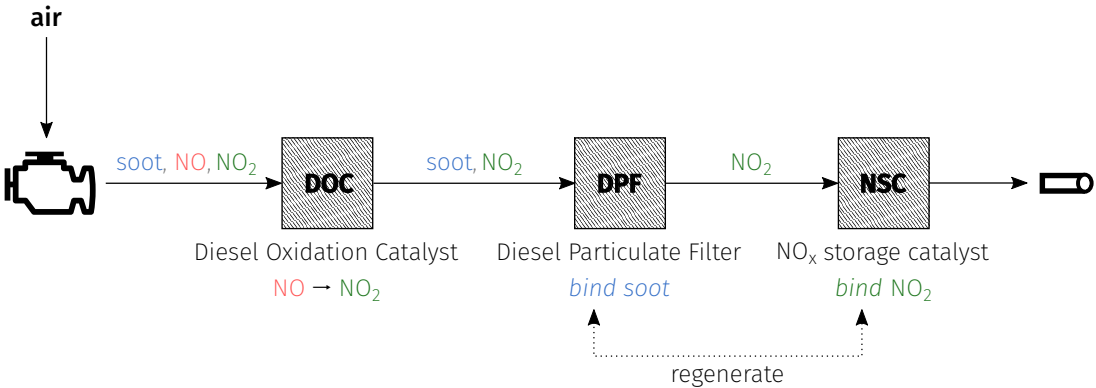
10. März 2016, 22:25 Uhr / Quelle: ZEIT ONLINE, afp, fin / 56 Kommentare

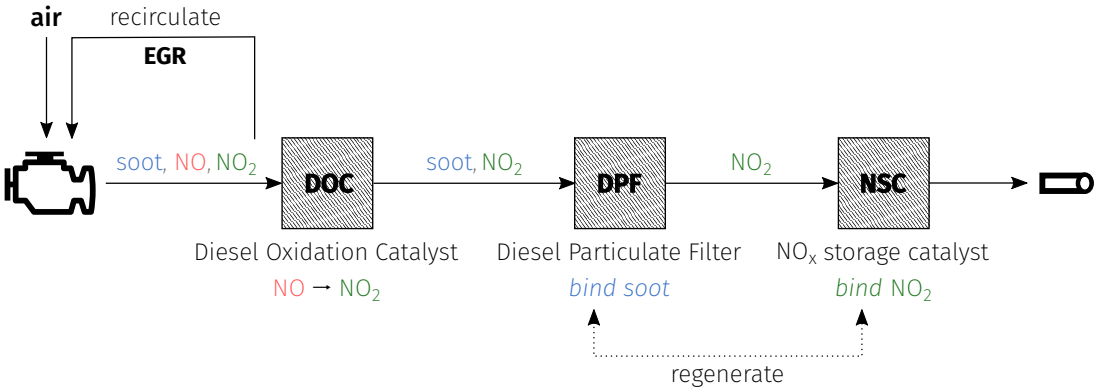
AFTER VW DIESELGATE, FIAT CHRYSLER ACCUSED OF RIGGING EMISSIONS BY US

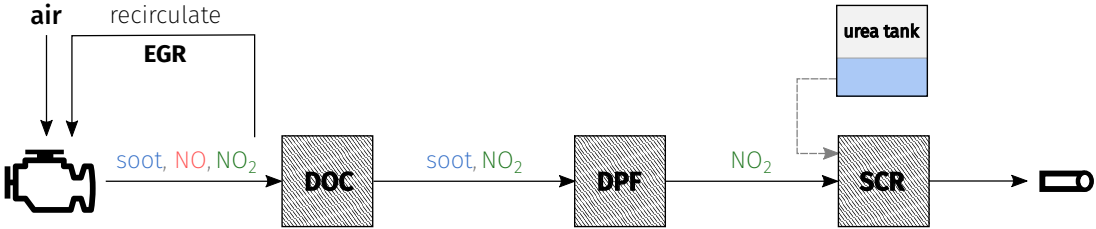
The Italian car maker is accused of installing software in Jeeps that helps them pass emission tests

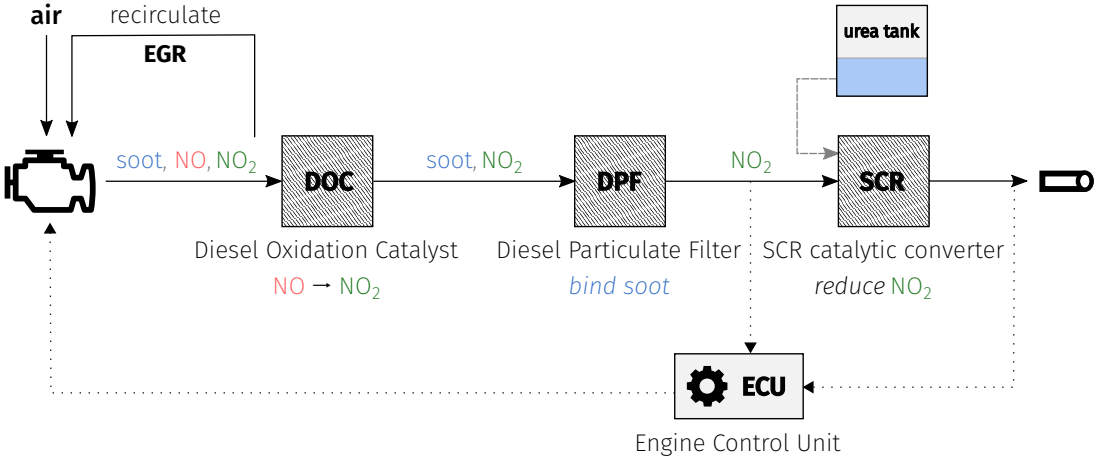

Sept. 2014 VW communicates DD details to EPA, CARB
EPA issues notice of violation of Clean Air Act
Nov. 2016 VW announces diesel sales stop in U.S.
2006
2014
2015
2016
2017
May 2014 ICCT study shows abnormalities
Jan. 2017 $4.3bn fine
VW admits use of DD (May. '06 – Nov. '15)
Oct. 2015 $10bn buy backs, $4.7bn emission projects

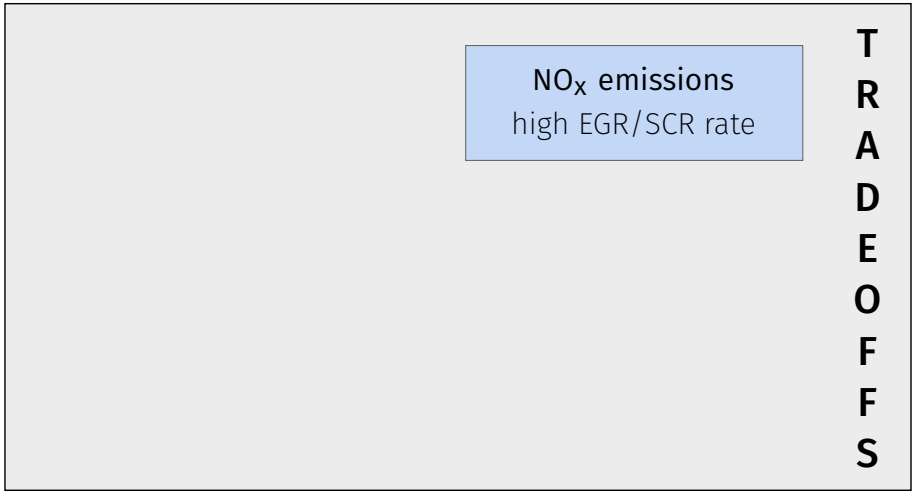

air
soot, NO, NO2
DOC
soot, NO2
DPF
NO2
NSC
Diesel Oxidation Catalyst
NO → NO2
Diesel Particulate Filter
bind soot
NOx storage catalyst
bind NO2

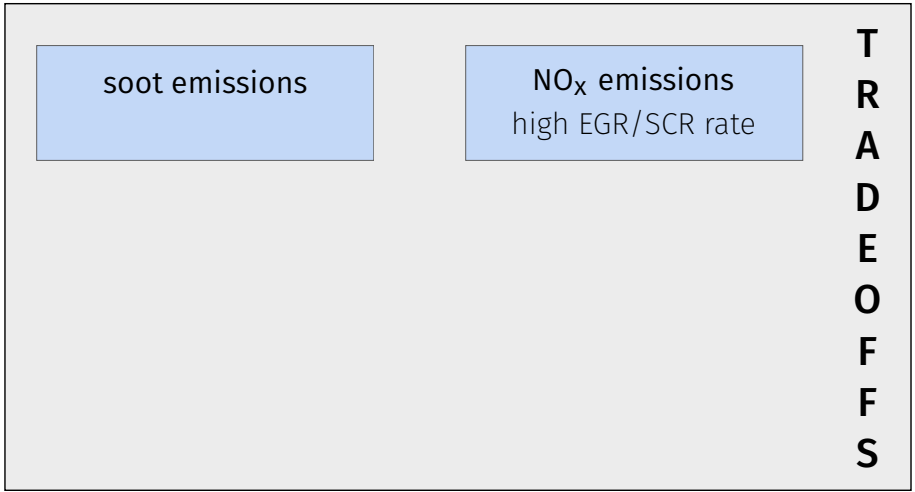

air
soot, NO, NO2
DOC
soot, NO2
DPF
NO2
NSC
Diesel Oxidation Catalyst
NO → NO2
Diesel Particulate Filter
bind soot
NOx storage catalyst
bind NO2
regenerate

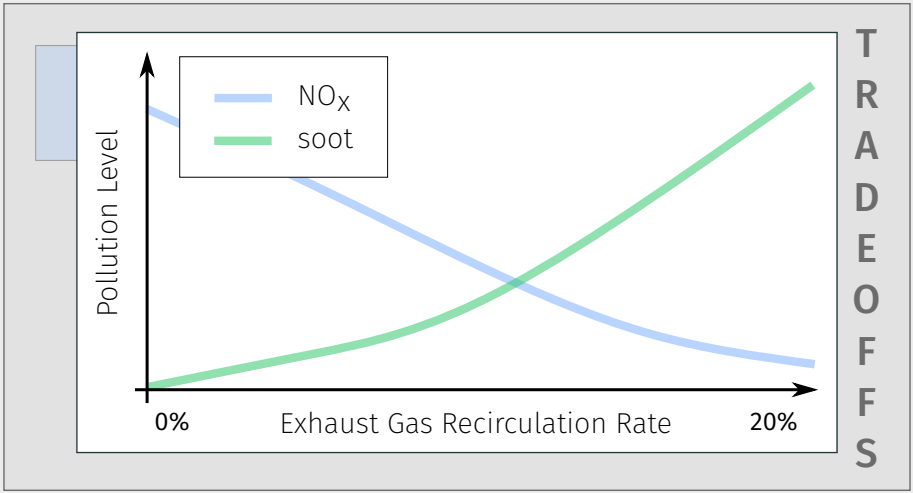

air
recirculate
EGR
soot, NO, NO2
DOC
soot, NO2
DPF
NO2
NSC
Diesel Oxidation Catalyst
NO → NO2
Diesel Particulate Filter
bind soot
NOx storage catalyst
bind NO2
regenerate

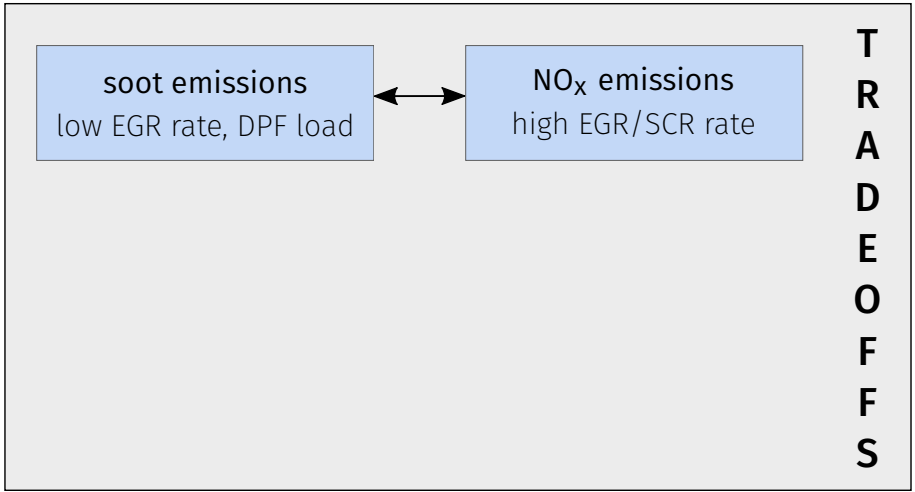

air
recirculate
EGR
urea tank
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
SCR
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
SCR catalytic converter
reduce NO_2

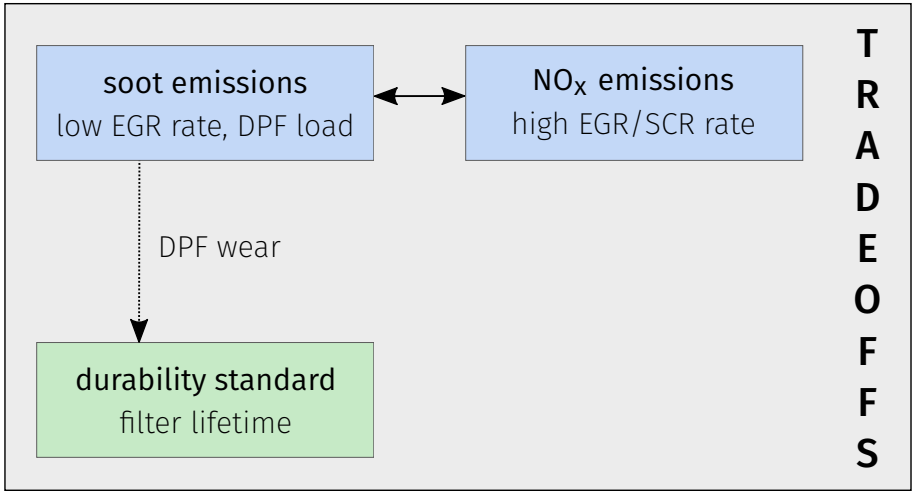

air
recirculate
EGR
urea tank
soot, NO, NO_2
DOC
soot, NO_2
DPF
NO_2
SCR
Diesel Oxidation Catalyst
NO → NO_2
Diesel Particulate Filter
bind soot
SCR catalytic converter
reduce NO_2
ECU
Engine Control Unit

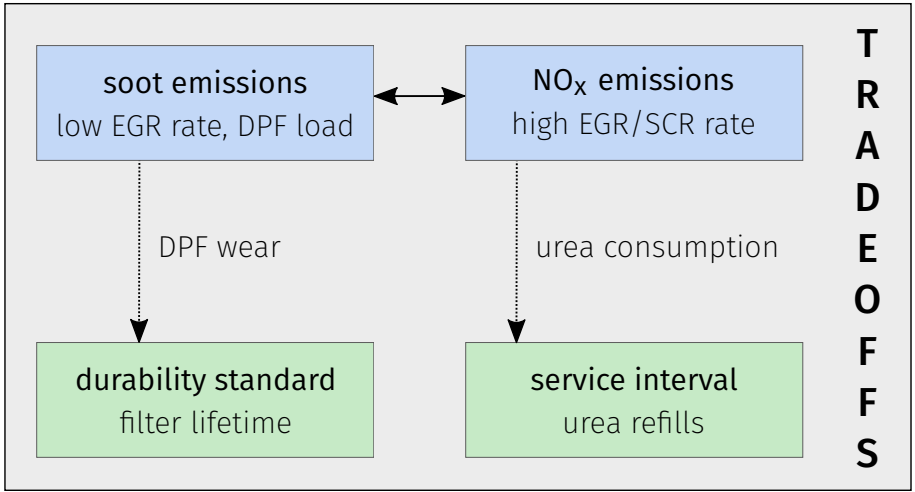

NO_X emissions
high EGR/SCR rate
TRADEOFFS


soot emissions
NO_X emissions
high EGR/SCR rate
TRADEOFFS

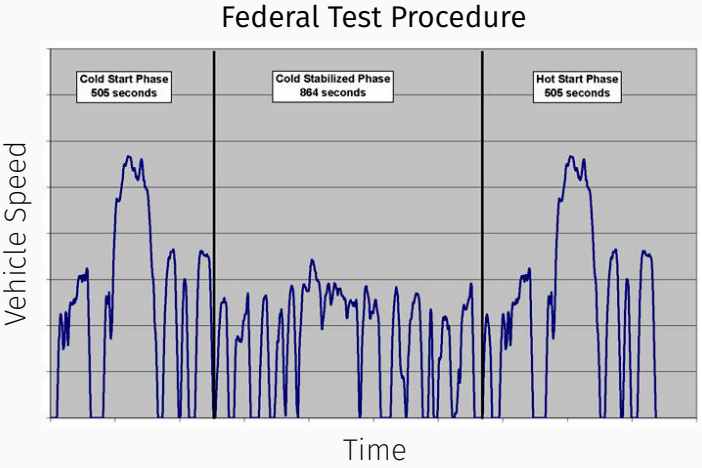

TRADEOFFS
NOX
soot
Pollution Level
0%
Exhaust Gas Recirculation Rate
20%


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

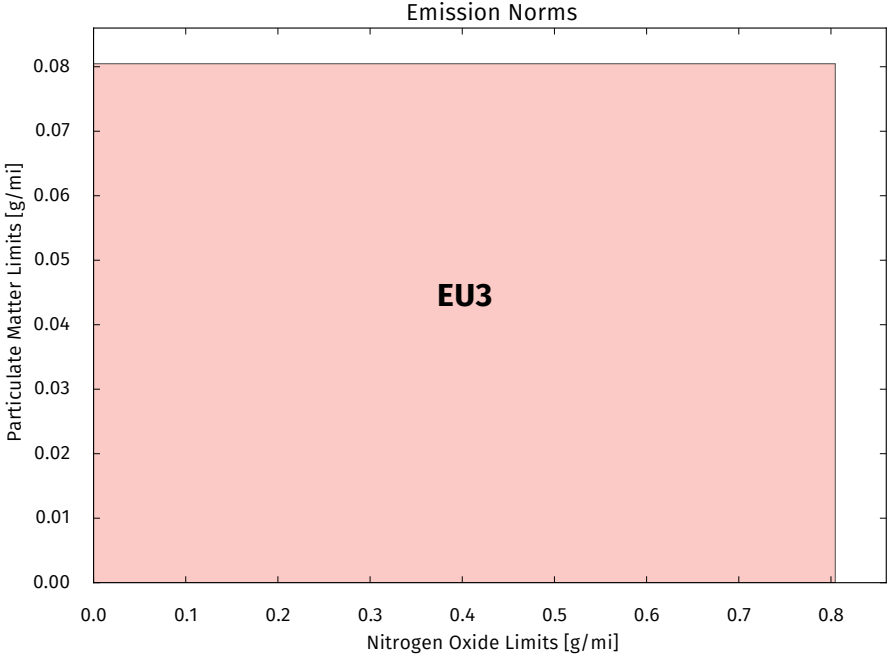

soot emissions
low EGR rate, DPF load
NO_X emissions
high EGR/SCR rate
DPF wear
durability standard
filter lifetime
TRADEOFFS

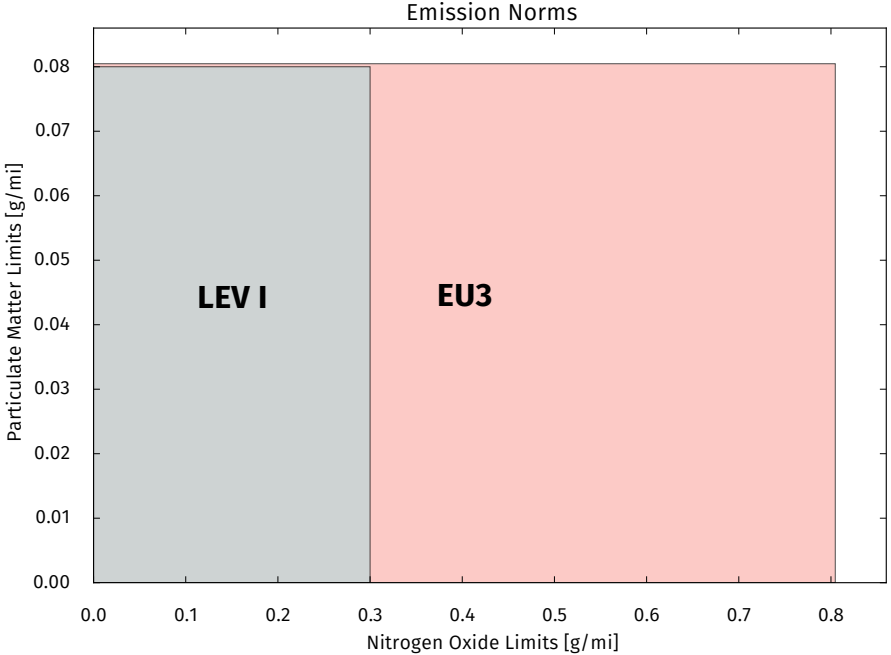

soot emissions
low EGR rate, DPF load
NO_X emissions
high EGR/SCR rate
TRADEOFFS
DPF wear
urea consumption
durability standard
filter lifetime
service interval
urea refills

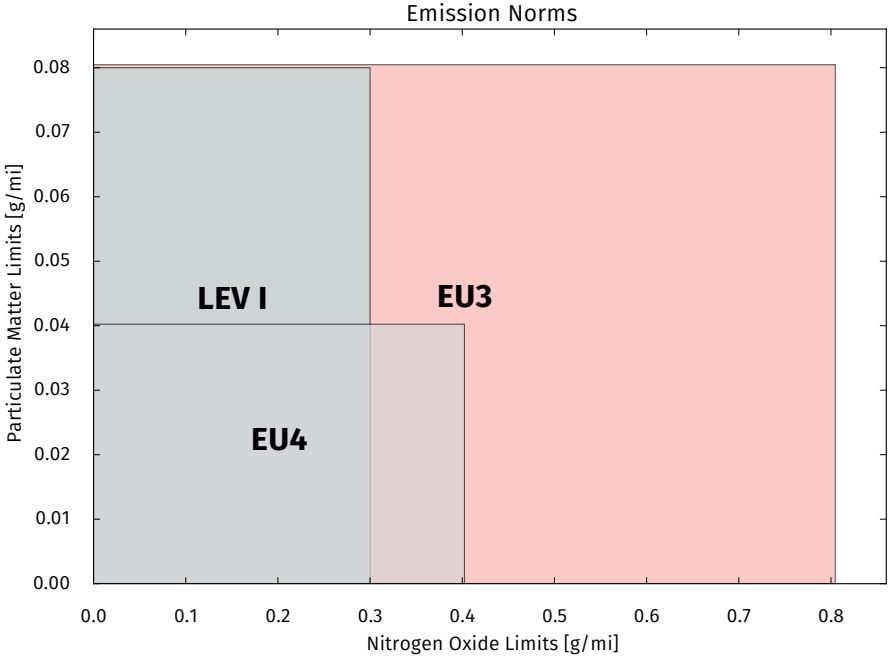
Emission Tests

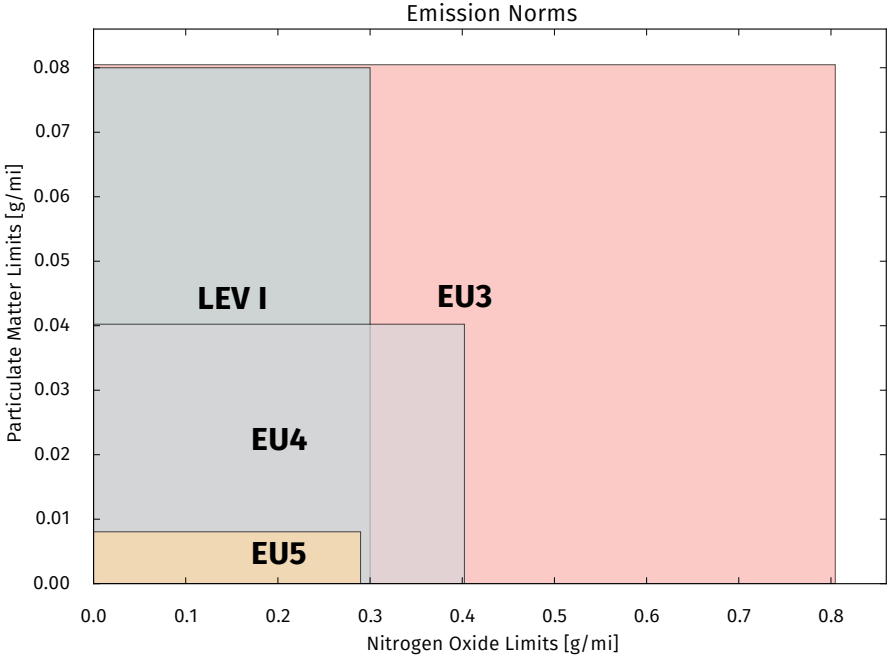


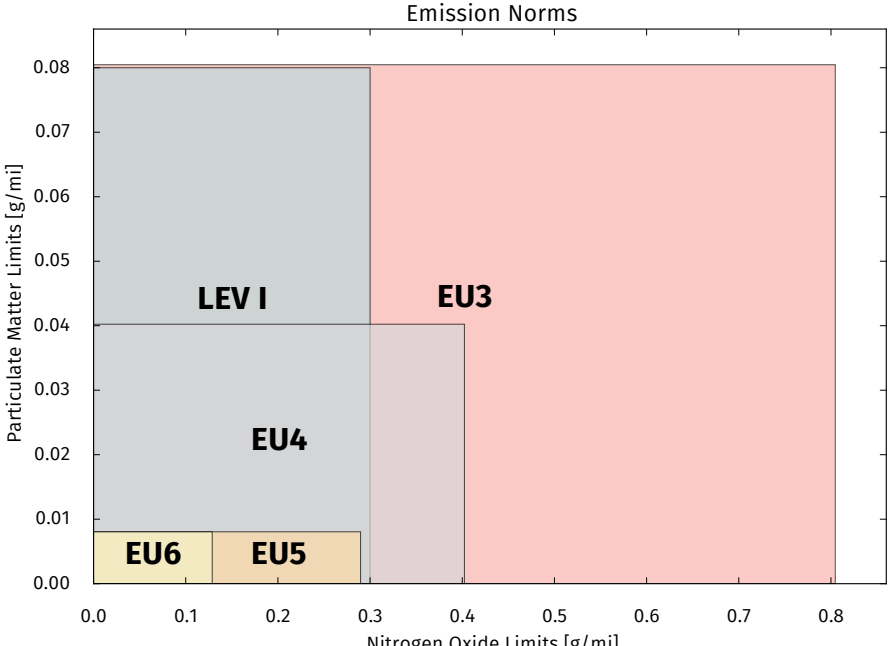
- Specify **time** – **vehicle speed**.
- Different tests per jurisdiction (EPA, CARB, EU).
- **Standardized** tests, publicly available.

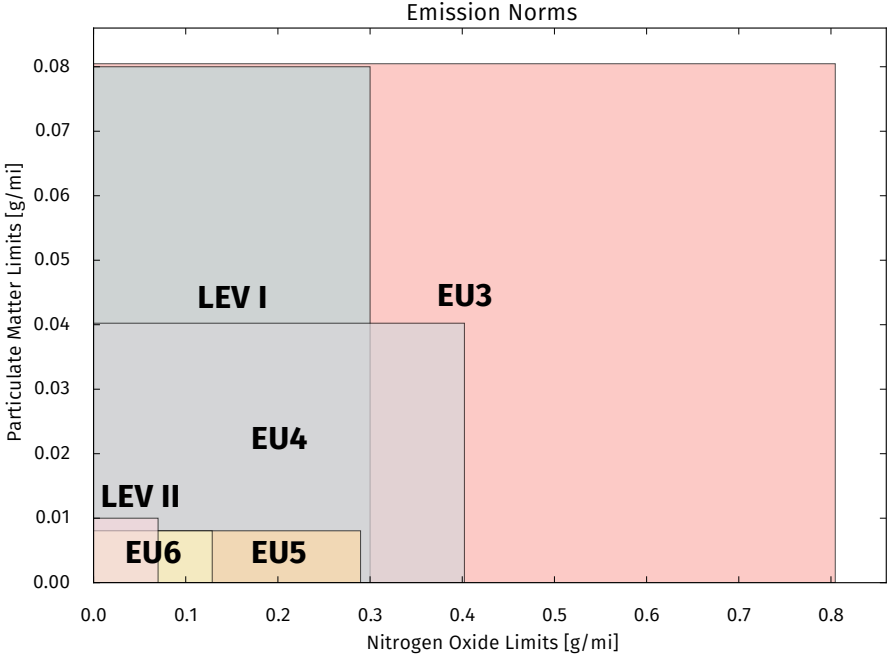

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
EU3
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]

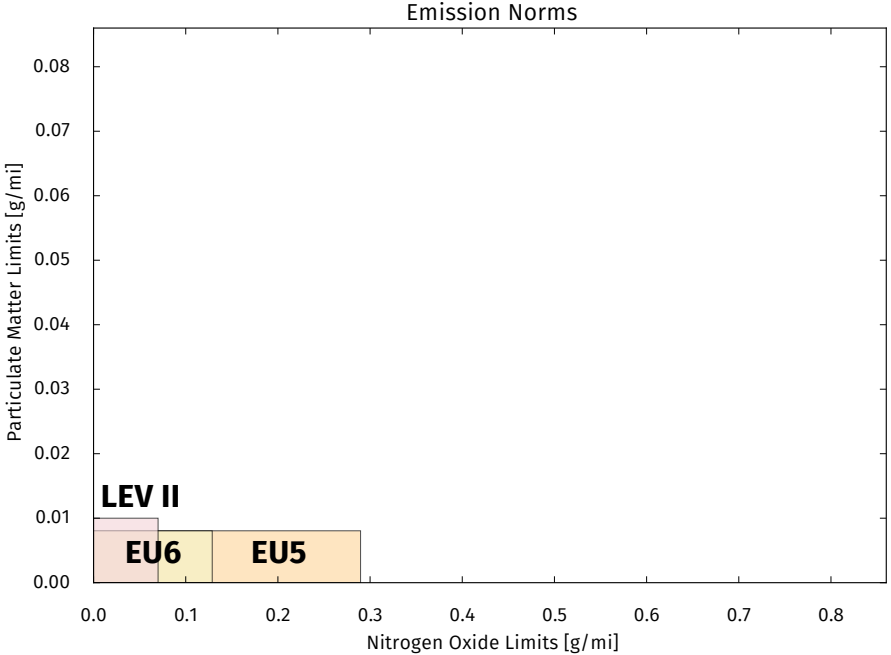

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


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]

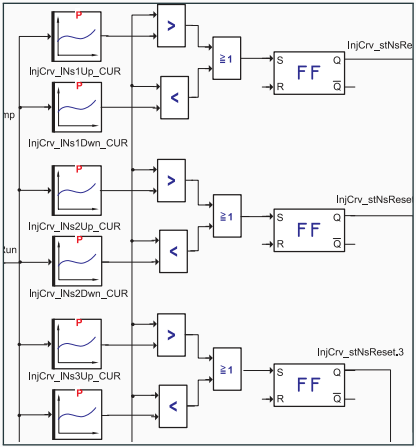

Emission Norms
Particulate Matter Limits [g/mi]
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0.00
LEV I
EU3
EU4
EU6
EU5
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
Nitrogen Oxide Limits [g/mi]


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]

Volkswagen AG Defeat Device

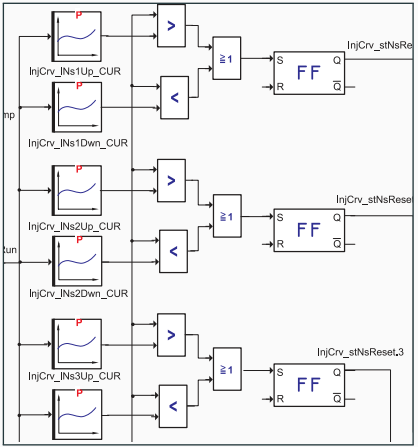
Volkswagen AG Defeat Device



Vendor-specific “Acoustic Function”

$$y_0 \leftarrow \text{query } curve_{\perp} \text{ at point } \mathbf{x}$$
$$y_1 \leftarrow \text{query } curve_{\top} \text{ at point } \mathbf{x}$$

Volkswagen AG Defeat Device



Vendor-specific “Acoustic Function”

$y_0 \leftarrow \text{query } \mathit{curve}_{\perp} \text{ at point } \mathbf{x}$

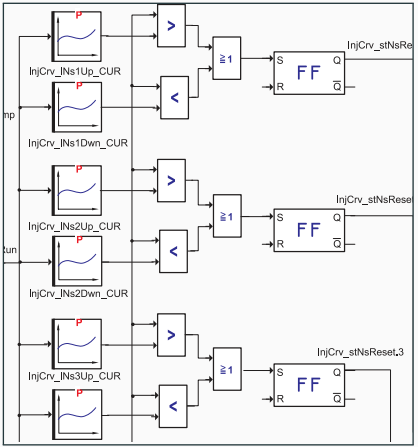
$y_1 \leftarrow \text{query } \mathit{curve}_{\top} \text{ at point } \mathbf{x}$

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

$$\Longleftrightarrow$$

“Profile matches”

Volkswagen AG Defeat Device



Vendor-specific “Acoustic Function”

$y_0 \leftarrow \text{query } \mathit{curve}_{\perp} \text{ at point } \mathbf{x}$

$y_1 \leftarrow \text{query } \mathit{curve}_{\top} \text{ at point } \mathbf{x}$

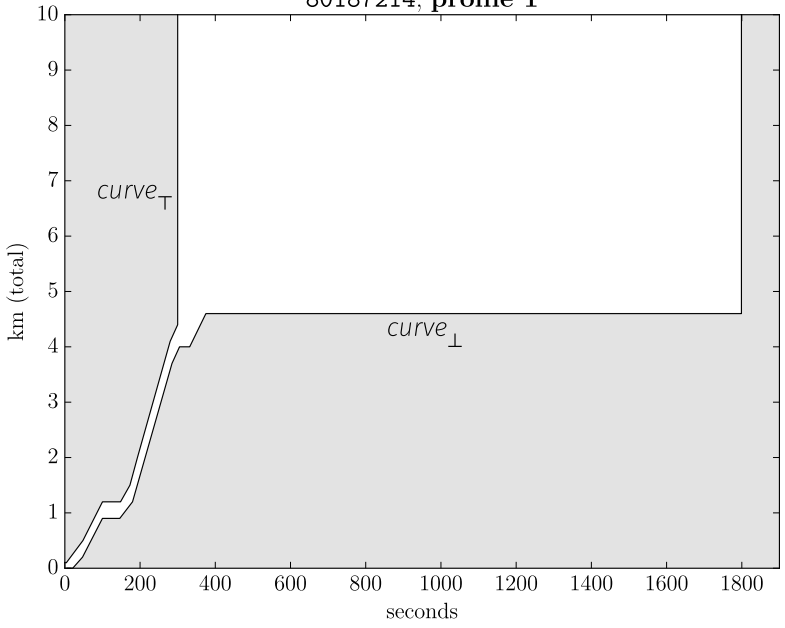
$$y_0 \leq \mathbf{y} \leq y_1$$

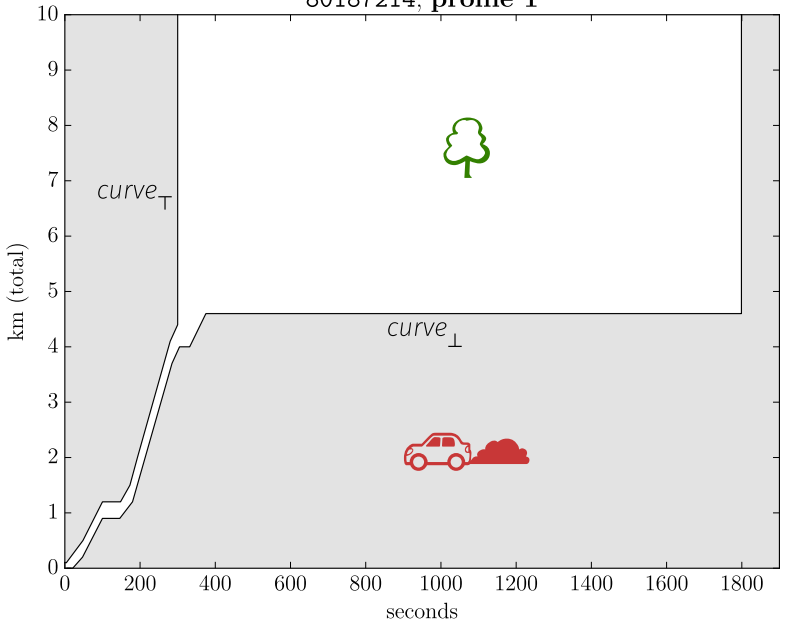
$$\Longleftrightarrow$$

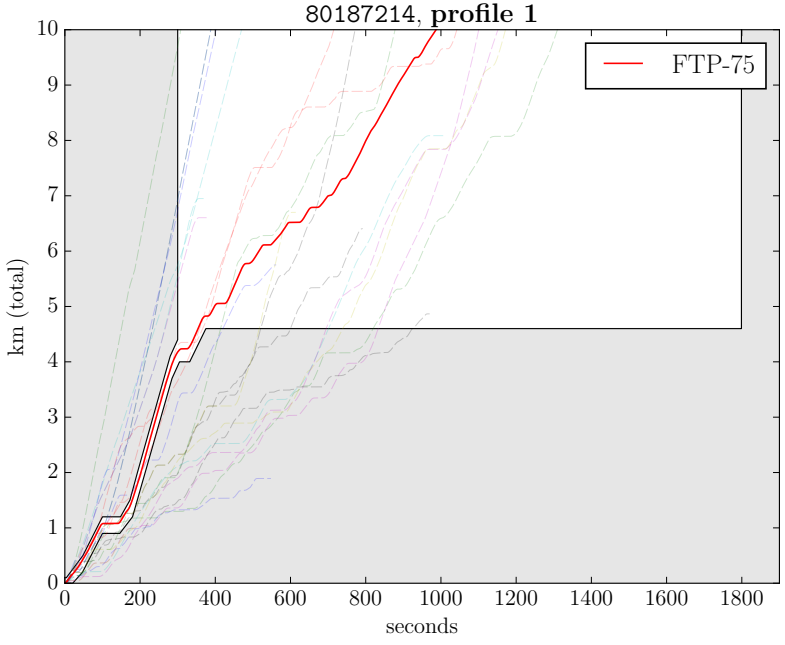
“Profile matches”

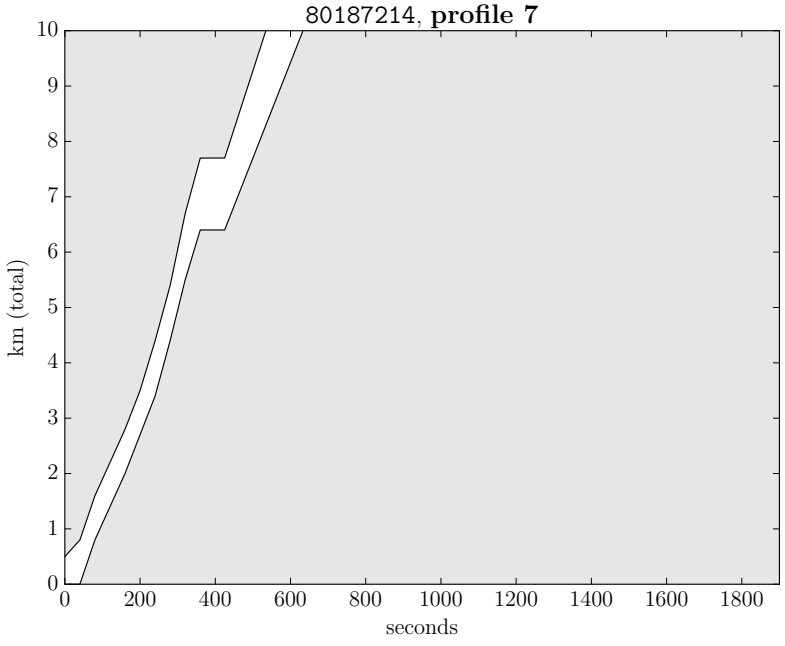
$\mathbf{x} :=$ “time since engine start”

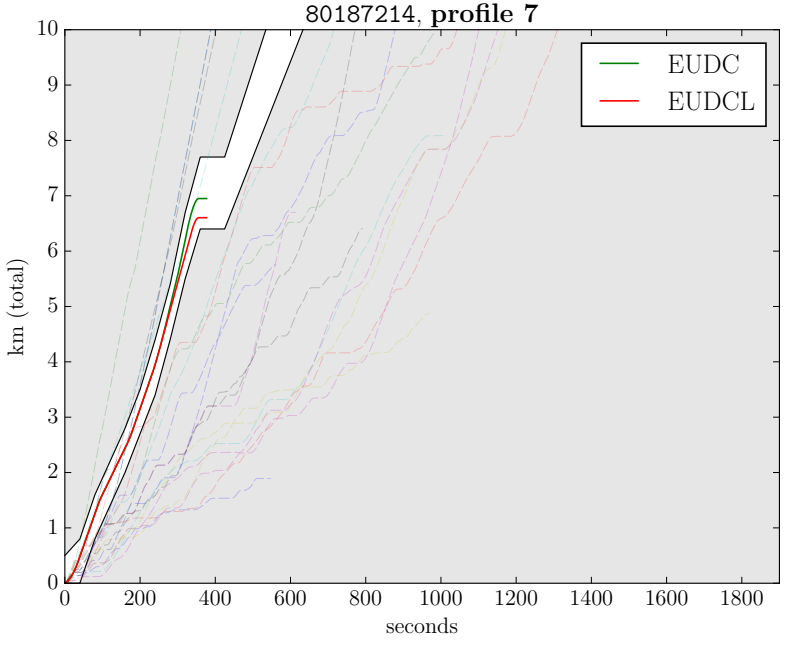
$\mathbf{y} :=$ “distance covered”

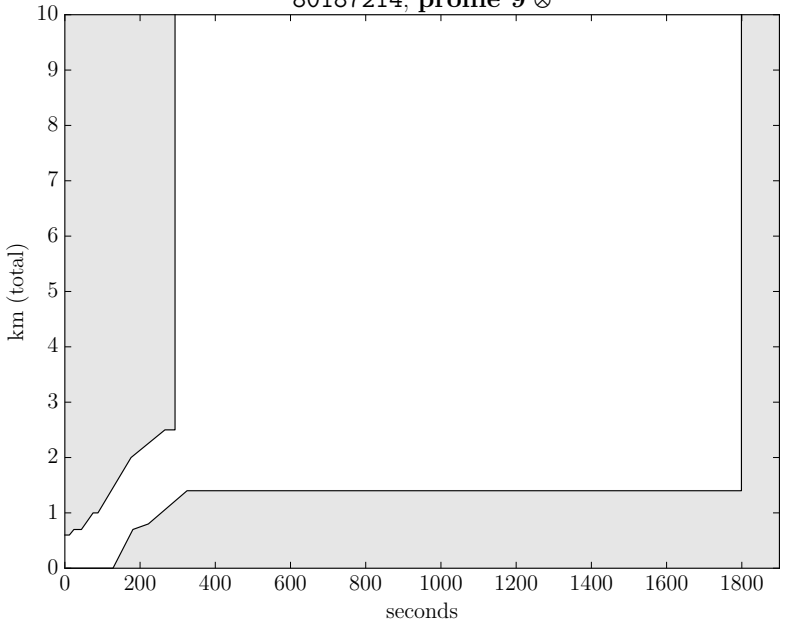

80187214, profile 1
curve⊤
curve⊥
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

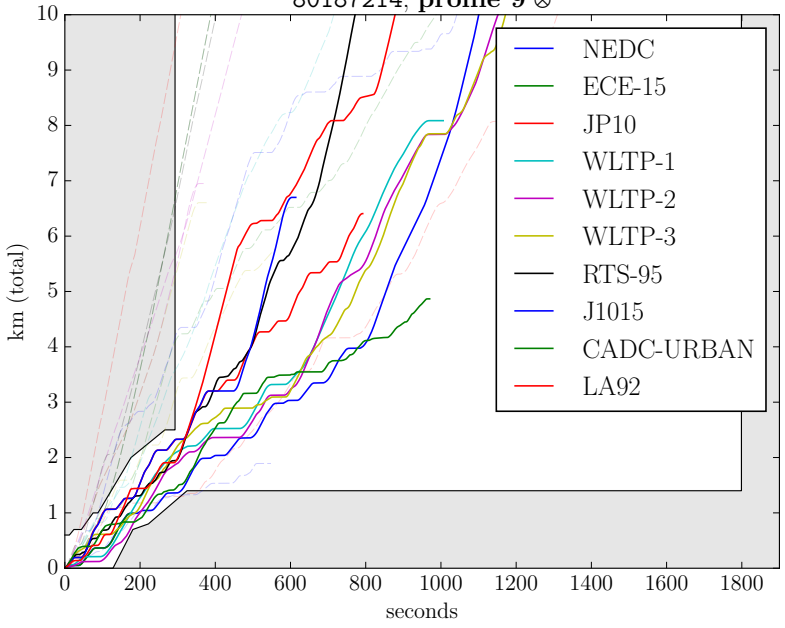

80187214, profile 1
km (total)
seconds
curve⊤
curve⊥
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

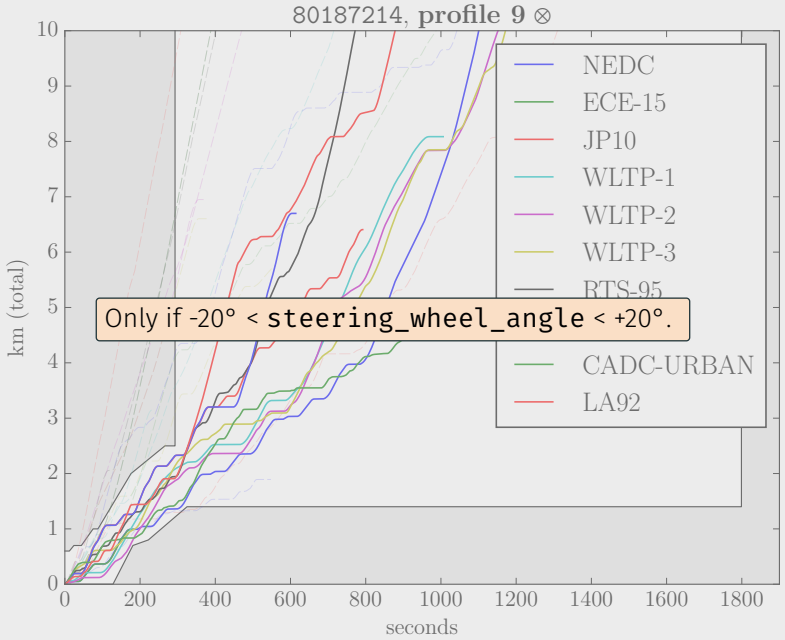

80187214, profile 1
FTP-75
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800

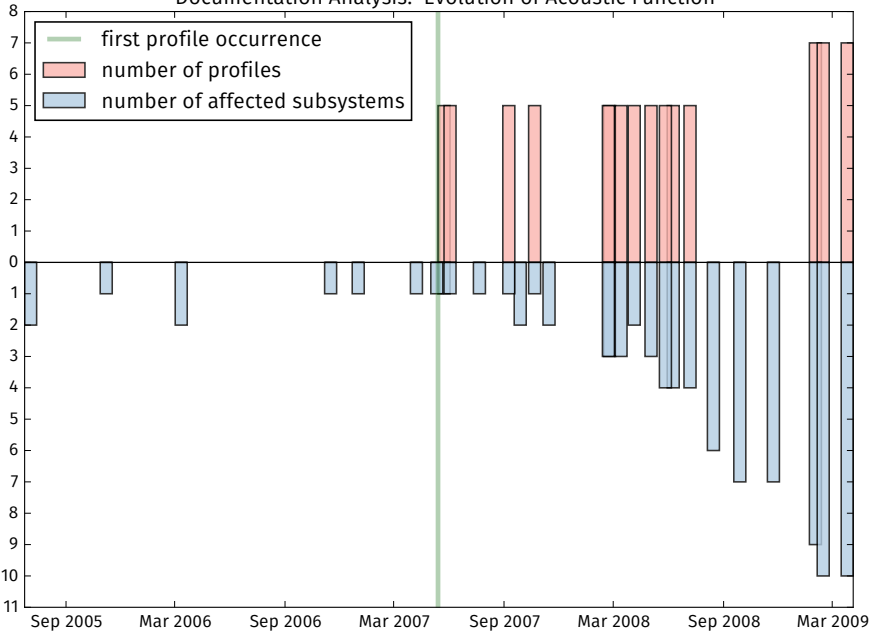

80187214, profile 7
km (total)
seconds
0
1
2
3
4
5
6
7
8
9
10
0
200
400
600
800
1000
1200
1400
1600
1800


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
CADC-URBAN
LA92
Only if -20° < steering_wheel_angle < +20°.


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

CurveDiff Framework

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.

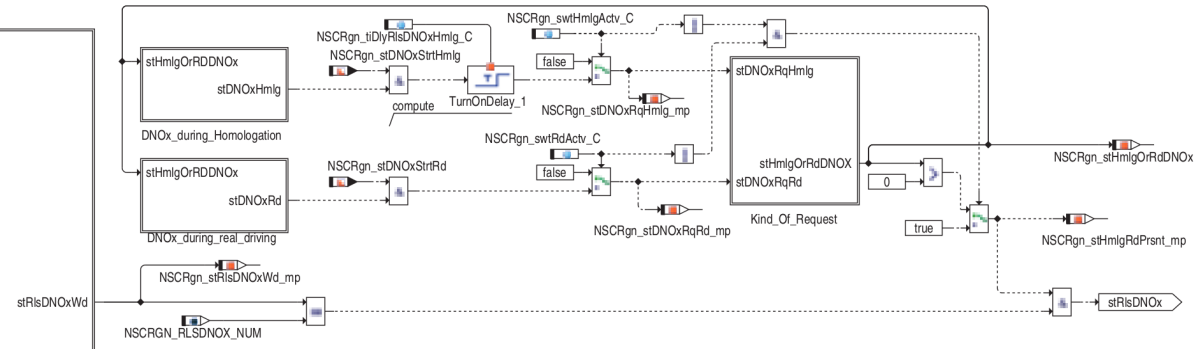
```
[17905: 0 - 18:17:12] Analyzing FL_03L906012___7444.
[17905: 0 - 18:17:12] Pre-processing database...
[17905: 1 - 18:17:51] Exporting functions...
[17905: 2 - 18:18:46] Analyzing functions...
[17905: 3 - 18:19:17] Exporting curves...
[17905: 4 - 18:19:42] Analyzing curves...

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.
```

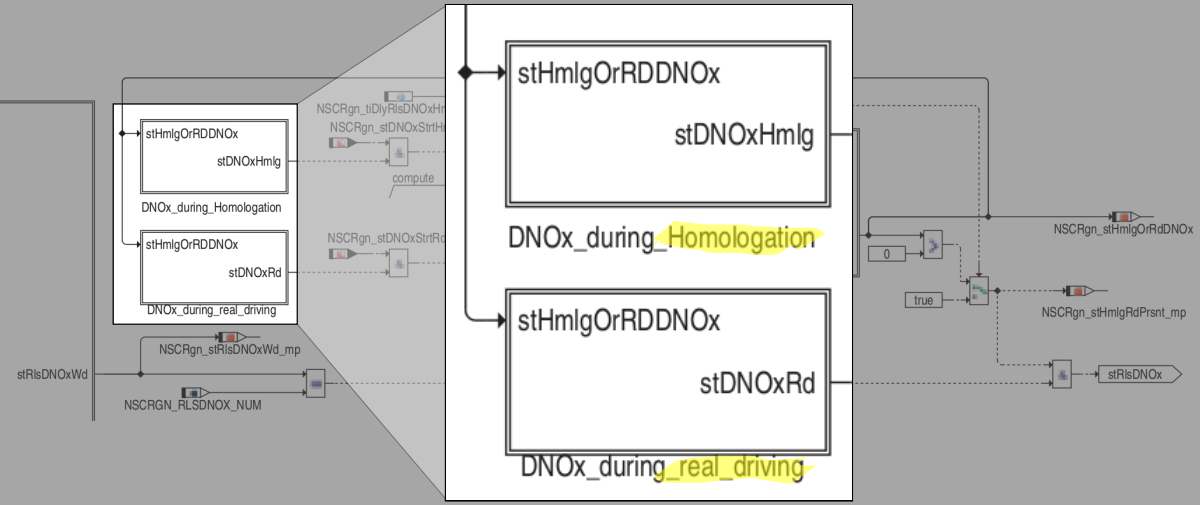
Potential Defeat Devices

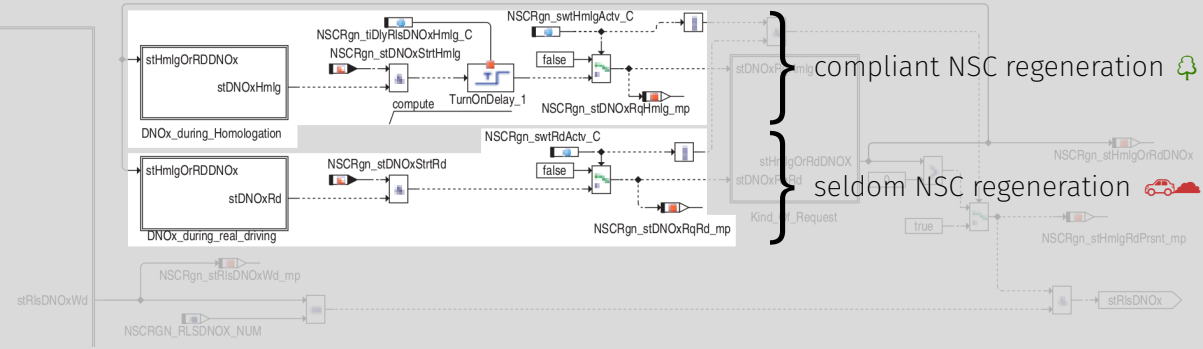
Analyzed **926** firmware images spanning **eight** years,
333 try to detect at least one emission test cycle.

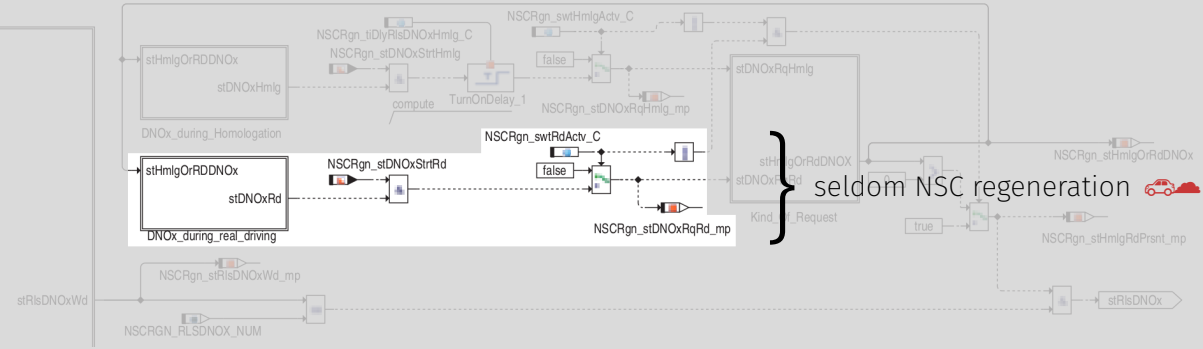
2009-01	Golf, Passat (2)
2009-07	A3
2009-08	Passat Blue Motion
2009-09	Golf (2), Passat (3)
2009-10	Golf+, Passat
2009-11	A3 (8), Golf Blue Motion, Golf (2), Passat
2009-12	A3 (5), Golf Variant (2), Golf+ (2), Golf (7), Jetta (3), Passat (4)
2010-01	Jetta, Passat (2)
2010-03	A3 (2), Golf (3), Jetta, 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

Fiat 500X Defeat Device





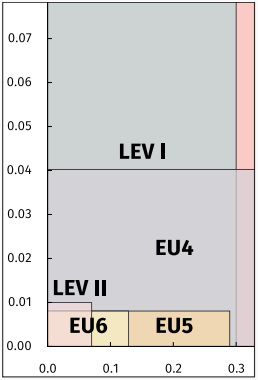




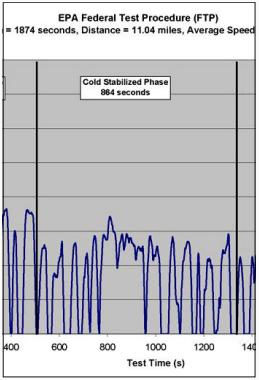
after 1600 seconds

Implications

State of Emissions Testing



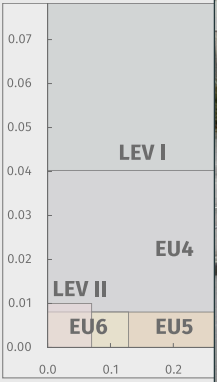
Strict Regulations



Public Test Cycles

Black Box Testing

State of Emissions Testing



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

Portable Emissions Measurement

Resulting Challenge

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

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

Conclusion

- 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.